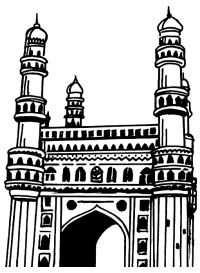
Rahul's ✔
Topper's Voice



B.Com.

III Year VI Semester

Latest 2022 Edition

CYBER SECURITY

- ☞ **Study Manual**
- ☞ **Important Questions**
- ☞ **Short Question & Answers**
- ☞ **Choose the Correct Answers**
- ☞ **Fill in the blanks**
- ☞ **Solved Model Papers**

- by -

WELL EXPERIENCED LECTURER

Rahul Publications™

Hyderabad. Ph : 66550071, 9391018098

All disputes are subjects to Hyderabad Jurisdiction only

B.Com.

III Year VI Semester

CYBER SECURITY

Inspite of many efforts taken to present this book without errors, some errors might have crept in. Therefore we do not take any legal responsibility for such errors and omissions. However, if they are brought to our notice, they will be corrected in the next edition.

© *No part of this publications should be reporduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording and/or otherwise without the prior written permission of the publisher*

Price ***`. 159/-***

Sole Distributors :

☎ : **66550071, Cell : 9391018098**

VASU BOOK CENTRE

Shop No. 2, Beside Gokul Chat, Koti, Hyderabad.

Maternity Hospital Opp. Lane, Narayan Naik Complex, Koti, Hyderabad.

Near Andhra Bank, Subway, Sultan Bazar, Koti, Hyderabad -195.

CYBER SECURITY

CONTENTS

STUDY MANUAL

SOLVED MODEL PAPERS

SYLLABUS

UNIT - I

Introduction to Cyber Security:

Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.

Cyber Security Vulnerabilities:

Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness.

Cyber Security Safeguards:

Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management.

UNIT - II

Securing Web Application, Services and Servers:

Introduction, Basic security for HTTP Applications and Services, Basic Security for SOAP Services, Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges.

UNIT - III

Intrusion Detection and Prevention:

Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection,Intrusion detection and Prevention Techniques, Anti-Malware software, Network based Intrusiondetection Systems, Network based Intrusion Prevention Systems, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation.

UNIT - IV

Cryptography and Network Security:

Introduction to Cryptography, Symmetric key Cryptography, Asymmetric key Cryptography, Message Authentication, Digital Signatures, Applications of Cryptography. Overview of Firewalls-Types of Firewalls, User Management, VPN Security Security Protocols: - security at the Application Layer- PGP and S/MIME, Security at Transport Layer- SSL and TLS, Security at Network Layer-IPSec.

UNIT - V

Cyberspace and The Law, Cyber Forensics:

Cyberspace and The Law: Introduction, Cyber Security Regulations, Roles of International Law, the state and Private Sector in Cyberspace, Cyber Security Standards. The INDIAN Cyberspace, NationalCyber Security Policy 2013.

Cyber Forensics: Introduction to Cyber Forensics, Handling Preliminary Investigations, Controlling anInvestigation, Conducting disk-based analysis, Investigating Information-hiding, Scrutinizing E-mail,Validating E-mail header information, Tracing Internet access, Tracing memory in real-time.

Contents

UNIT - I

Topic **Page No.**

UNIT - V

Important Questions

UNIT - I

1. What is cyber security? Why is cyber security important? Explain.

Ans :

Refer Unit-I, Q.No. 1

---

2. Define cyber crime? What are the various methods in cyber crime? How to prevent them.

Ans :

Refer Unit-I, Q.No. 7

---

3. What is the need for comprehensive cyber security policy?

Ans ;

Refer Unit-I, Q.No. 10

---

4. What is a software vulnerability? Explain about the most common security vulnerabilities.

Ans :

Refer Unit-I, Q.No. 14

---

5. What are the reasons for lack of cyber security awareness? Explain how to over come it.

Ans :

Refer Unit-I, Q.No. 20

---

6. What is a Cybersecurity Audit?Explain about it.

Ans :

Refer Unit-I, Q.No. 24

---

7. What is deception technology? Explain about it.

Ans :

Refer Unit-I, Q.No. 29

UNIT - II

1. What are the various issues in securing web applications.

Ans :

Refer Unit-II, Q.No. 1

---

2. Explain about the security protocols in HTTPS.

Ans :

Refer Unit-II, Q.No. 2

3. What is SOAP? Explain about SOAP protocol structure.

Ans :

Refer Unit-II, Q.No. 3

4. Explain various security considerations in web security.

Ans :

Refer Unit-II, Q.No. 6

5. Explain the challenges for web security.

Ans :

Refer Unit-II, Q.No. 7

UNIT - III

1. Explain what are Internal Data Security Threats and How to deal with them.

Ans :

Refer Unit-III, Q.No. 2

2. What is privilege abuse? Explain how to handle them

Ans :

Refer Unit-III, Q.No. 3

3. Explain various types of malware infection and attacks. Write about how to remove malware from the devices.

Ans :

Refer Unit-III, Q.No. 5

4. Explain about Intrusion detection and prevention techniques.

Ans :

Refer Unit-III, Q.No. 6

5. Explain about Network based Intrusion detection system.

Ans :

Refer Unit-III, Q.No. 8

6. What Is a Network Intrusion Prevention System and How Does it Work?

Ans :

Refer Unit-III, Q.No. 10

7. Write about system integrity validataion

Ans :

Refer Unit-III, Q.No. 14

UNIT - IV

1. What is Cryptography? Explain briefly.

Ans :

Refer Unit-IV, Q.No. 1

2. Explain Data Encryption Standard(DES) algorithm.

Ans :

Refer Unit-IV, Q.No. 4

3. What is a Firewall? Explain about the types of firewalls.

Ans :

Refer Unit-IV, Q.No. 10

4. What is VPN? Explain about VPN security.

Ans :

Refer Unit-IV, Q.No. 12

5. Write about security protocols at application layer.

Ans :

Refer Unit-IV, Q.No. 13

6. Explain working mechanism of PGP.

Ans :

Refer Unit-IV, Q.No. 14

7. Explain briefly about TLS Protocol.

Ans :

Refer Unit-IV, Q.No. 18

UNIT - V

1. Define Cyber space and cyber law? Explain the importance of cyber law.

Ans :

Refer Unit-V, Q.No. 1

2. Explain cyber security regulations.

Ans :

Refer Unit-V, Q.No. 2

3. Write about the roles of international cyber law.

Ans :

Refer Unit-V, Q.No. 3

4. Write about the roles of state and private sector in cyber space.

Ans :

Refer Unit-V, Q.No. 4

5. What are cyber security standards? Explain various cyber security stand ards.

Ans :

Refer Unit-V, Q.No. 5

6. What is the National Cyber Security Policy? Explain about it.

Ans :

Refer Unit-V, Q.No. 7

7. What is cyber forensics ? Explain computer forensic services?

Ans :

Refer Unit-V, Q.No. 8

8. Explain how to collect and control the investigation.

Ans :

Refer Unit-V, Q.No. 11

9. How data can be hidden in computer forensics and explain how hidden data can be investigated in cyber forensics.

Ans :

Refer Unit-V, Q.No. 13

10. How internet tracing can be done? Explain various methods to track internet access.

Ans :

Refer Unit-V, Q.No. 16

UNIT I

Introduction to Cyber Security: Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.
Cyber Security Vulnerabilities: Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness.
Cyber Security Safeguards: Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management.

1.1 Introduction to Cyber Security

1.1.1 Overview of Cyber Security

Q1. What is cyber security? Why is cyber security important? Explain.

Ans : **(Imp.)**

Meaning

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

- The term cyber security refers to techniques and practices designed to protect digital data.
- The data that is stored, transmitted or used on an information system.
- Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.

It is made up of two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

- Cyber attacks can be extremely expensive for businesses to endure.
- In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cyber criminals are using more sophisticated ways to initiate cyber attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.
- Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber attack.
- But, an organization or an individual can develop a proper response plan only when he has a good grip on cyber security fundamentals.

Cyber security Fundamentals

(i) Confidentiality

Confidentiality is about preventing the disclosure of data to unauthorized parties.

It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous.

Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

- Data encryption
- Two-factor authentication
- Biometric verification
- Security tokens

Rahul Publications

(ii) Integrity

Integrity refers to protecting information from being modified by unauthorized parties.

Standard measures to guarantee integrity include:

- Cryptographic check sums
- Using file permissions
- Uninterrupted power supplies
- Data backups

(iii) Availability

Availability is making sure that authorized parties are able to access the information when needed.

Standard measures to guarantee availability include:

- Backing up data to external drives
- Implementing firewalls
- Having backup power supplies
- Data redundancy

1.1.2 Internet Governance – Challenges and Constraints

Q2. What is internet governance? Explain the challenges of Internet Governance.

Ans :

Meaning

Internet governance is 'the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet'.

Challenges

1. The pace and changing nature of the internet

First, the internet today is simply bigger and more diverse than it used to be. Its range of services is far greater and continually growing. It's been transformed by massive growth in the capacity of networks and devices, mobility, the internet of things and cloud computing. All this continues and accelerates.

Governance mechanisms aren't always scalable. Ways of governing the internet that worked when it was smaller and less complex won't be sufficient now it's larger and more complex.

The internet began by radically disrupting governance and business models in communications. It's required other sectors to transform their models wholesale. The same logic of disruption applies to the internet's own governance arrangements.

2. The internet as part of digitalisation

Associated with this is the changing nature of the digital environment.

The internet's no longer at the cutting edge of this. The most important technological advances – the most important issues for digital governance emerging now – are not to do with the internet as a communications medium but with other digital developments – in data management, machine learning and artificial intelligence, algorithmic decision-making, robotics and autonomous vehicles, virtual reality, quantum computing.

Internet governance does not provide adequate models for governing those new digital phenomena, which is why there is so much discussion now, for instance, about the ethics of AI.

3. The concentration of digital power

Technologists stress the decentralising force they see inherent in the internet's packet-switched technology and protocols. Power on the internet, they tend to say, lies with end-users; there is no centre to it.

But economic logic differs from technology. Networks give powerful advantages to big players that can maximise numbers of users, achieve economies of scope and scale, and leverage data to maximise value to consumers and themselves.

The result has been the concentration of online power in a few large companies with global reach, that can act effectively

Rahul Publications

unchecked by the majority of governments. These have become the most powerful actors in internet governance today, and their decisions are decidedly not subject to the principles of multi stakeholderism.

4. Digital geopolitics (and the environment)

At the same time, there have been shifts in global geopolitics. Three things.

First, those dominant online businesses that I've just mentioned are almost all located in two countries. Twenty years ago, the fear in many countries was that the internet was dominated by America. Now China's as important, and leads in some new digital technologies. Between them, China and the United States have 90 per cent of market capitalisation in the 70 largest digital platforms. Africa and Latin America between them have just 1 per cent.

Second, the thirty years in which the internet's evolved have seen the world divided much more than it was. To a considerable degree, authoritarian nationalism has superseded liberal internationalism. Achieving digital cooperation a key aim for the UN Secretary-General is becoming harder. That really matters in areas like cyber security. And governments are much more capable of interfering with each other's internet environments for political and economic gain, and more inclined to do so. And the biggest challenge of all facing international governance is climate change. Like everything else, internet governance is going to evolve in a context redefined by climate change, by the success or failure of steps to mitigate it (not least this week and next), and by the conflicts that will follow likely failures.

5. Shaping the digital future

That means shaping the digital future in ways that work with other goals we have rather than letting technology shape the future for us.

There are three things:

- preserving what we value
- promoting what we want
- and preventing what we fear.

There'll be disagreements about what those mean. But achieving them requires governance that is consistent with other goals the international community's agreed. In particular, I'd cite the international human rights regime, the sustainable development agenda and the need to reverse climate change.

6. The future of regulation

The internet community and businesses have been keen to avoid regulation and sought what they've called 'permission less innovation' as distinct from the 'precautionary principle' that's generally applied in other economic sectors.

That's the principle that we should assess potential hazards before giving free rein to new inventions. It's the norm in industries like chemicals and pharmaceuticals and in other new technologies such as genetics. It's at the root of environmental audits and has been fundamental to building public trust in COVID vaccines.

These concerns are going to require rethinking the relationship between innovation which has been permissionless and the precautionary principle. Few people outside Facebook think the 'metaverse' should be unregulated.

7. Multilateralism and multi stakeholderism

Multi stakeholderism has been an important part of the way the internet's been governed, from its early days. But the model of it that emerged from the World Summit is looking tired and worn.

First, the standard stakeholder groupings are insufficiently disaggregated.

- There are huge differences between government departments that manage

Rahul Publications

communications and those that use them to deliver public services.

- Between businesses that supply the internet and those that use it.
- Between different groups of users, with different interests, different resources, different capabilities, not to mention those who aren't yet on the internet but whose lives are affected by the way it's changing their societies.

Representation in internet decision-making is skewed towards internet insiders; to the supply side of the internet rather than to the demand side.

Second, the stakeholders themselves have changed, and so have their resources. Global corporations can throw huge sums at influencing outcomes. Many decisions are made in boardrooms or through negotiations between businesses and governments.

8. Participation in decision-making

Countries in the North could put money, personnel and resources into attending meetings, planning initiatives, making deals and influencing outcomes. Most in the South could not. As a result, decisions reflected the interests of wealthy countries from the North, not those of developing countries in the South. Technical standards were affected by this, because they were set by what was possible in high-income countries rather than those with limited resources.

Q3. Explain the issues in Internet Governance.

Ans :

Issues

There have been debates globally on whether in its attempts to create new International Telecommunication Rules (ITRs), the ITU trying to control the Internet, and encourage censorship.

The issue of Internet governance (IG) was elevated at the global forum post the Snowden revelations. The multi-stakeholder model under unilateral control and oversight of the US government, over the Internet Corporation for Assigned Names and Numbers (ICANN), coupled with the bottom up approach in policy making and several other issues, echoed across major organizations that are part of IG community.

Resultantly, key players involved in various dimensions of Internet operations, namely ICANN, Internet Engineering Task Force (IETF), Internet Society (ISOC), Internet Architecture Board (IAB), World Wide Web Consortium (W3C), and Regional Internet Registries (RIRs), expressed intent to decouple themselves from the oversight of the US government and emphasized on multi-stakeholder model of IG. The National

Telecommunications and Information Administration (NTIA) of DoC of the US government in 2014 announced its intent of transition of oversight over Internet Assigned Numbers Authority (IANA) functions, which is managed by ICANN through a contract.

DSCI has been working as part of the deliberations with key stakeholders. We advocate a multi-stakeholder model for IG, which must be proportional to the Internet population of nations. Consultation and representation of the industry on its views on IG on various forums has been part of our work.

We strongly support the view that roles and responsibilities of all stakeholders must be clearly defined for various issues and our work focuses on reviving discussions on various platforms to establish global Internet principles, evolve global norms and treaties for complex subjects such as cyber crime, cyber security, privacy and intellectual property.

DSCI encourages participation of underdeveloped and developing countries on all platforms, by providing the required support, that can help build capacity and bridge the digital divide. We work with the Indian Industry for their active participation in various standard and protocol development organizations such as IEEE, IETF, W3C and ISO to establish thought leadership

Rahul Publications

1.1.3 Cyber Threats

Q4. What is a Threat in Cyber security? Explain the types of Cyber security threats.

Ans :

Meaning

A cyber security threat is a malicious and deliberate attack by an individual or organization to gain unauthorized access to another individual's or organization's network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data.

Types

While the types of cyber threats continue to grow, there are some of the most common and prevalent cyber threats that present-day organizations need to know about. The top 10 cyber security threats are as follows

1. Malware

Malware attacks are the most common cyber security threats. Malware is defined as malicious software, including spyware, ransomware, viruses, and worms, which gets installed into the system when the user clicks a dangerous link or email. Once inside the system, malware can block access to critical components of the network, damage the system, and gather confidential information, among others.

2. Phishing

Cyber criminals send malicious emails that seem to come from legitimate resources. The user is then tricked into clicking the malicious link in the email, leading to malware installation or disclosure of sensitive information like credit card details and login credentials.

3. Spear Phishing

Spear phishing is a more sophisticated form of a phishing attack in which cyber criminals target only privileged users such as system administrators and C-suite executives are than 71% of targeted attacks

4. Man in the Middle Attack

Man in the Middle (MitM) attack occurs when cyber criminals place themselves between a two-party communication. Once the attacker interprets the communication, they may filter and steal sensitive data and return different responses to the user.

5. Denial of Service Attack

Denial of Service attacks aims at flooding systems, networks, or servers with massive traffic, thereby making the system unable to fulfill legitimate requests. Attacks can also use several infected devices to launch an attack on the target system. This is known as a Distributed Denial of Service (DDoS) attack.

The year 2019 saw a staggering 8.4 million DDoS attacks.

6. SQL Injection

A Structured Query Language (SQL) injection attack occurs when cyber criminals attempt to access the database by uploading malicious SQL scripts. Once successful, the malicious actor can view, change, or delete data stored in the SQL database.

SL injection accounts for nearly 65.1% of all web application attacks.

7. Zero-day Exploit

A zero-day attack occurs when software or hardware vulnerability is announced, and the cyber criminals exploit the vulnerability before a patch or solution is implemented. t zero-day attacks will rise to one per day by 2021.

8. Advanced Persistent Threats (APT)

An advanced persistent threat occurs when a malicious actor gains unauthorized access to a system or network and remains undetected for an extended time.

9. Ransomware

Ransomware is a type of malware attack in which the attacker locks or encrypts the victim's data and threatens to publish or block access to data unless a ransom is paid. Learning more about ransomware threats can help companies prevent and cope with them better.

Rahul Publications

10. DNS Attack

A DNS attack is a cyberattack in which cyber criminals exploit vulnerabilities in the Domain Name System (DNS). The attackers leverage the DNS vulnerabilities to divert site visitors to malicious pages (DNS Hijacking) and remove data from compromised systems (DNS Tunneling).

1.1.3.1 Cyber Warfare

Q5. What is Cyber Warfare? Explain the types of Cyber Warfare.

Ans :

Meaning

Cyber Warfare is typically defined as a set of actions by a nation or organization to attack countries or institutions' computer network systems with the intention of disrupting, damaging, or destroying infrastructure by computer viruses or denial-of-service attacks.

Cyber warfare can take many forms, but all of them involve either the destabilization or destruction of critical systems. The objective is to weaken the target country by compromising its core systems.

This means cyber warfare may take several different shapes:

1. Attacks on financial infrastructure
2. Attacks on public infrastructure like dams or electrical systems
3. Attacks on safety infrastructure like traffic signals or early warning systems
4. Attacks against military resources or organizations

Types

1. Espionage

Espionage refers to spying on another country to steal secrets. In cyber warfare, this may involve using a botnet or spear-fishing attack to gain a foothold in a computer before extracting sensitive information.

2. Sabotage

With sensitive information identified, organizations then need to determine the potential threats presented to this data. This includes third parties that may want to steal the data, competitors that could gain an advantage by stealing information, and insider threats or malicious insiders like disgruntled workers or negligent employees

3. Denial-of-Service Attack

A denial-of-service (DoS) attack involves flooding a website with fake requests, forcing the site to process those requests, thereby making it unavailable for legitimate users. This kind of attack could be used to cripple a critical website used by citizens, military personnel, safety personnel, scientists, or others to disrupt critical operations or systems.

4. Electrical Power Grid

Hacking the electrical power grid could give an attacker the ability to disable critical systems, crippling infrastructure and causing the deaths of thousands. Further, an attack on the electrical power grid could disrupt communications, making it impossible to use services like text messaging or telecommunication.

5. Propaganda

Propaganda attacks involve trying to control the minds or hearts of the people living in or fighting for the targeted country. Propaganda can be used to expose embarrassing truths or to spread lies that cause people to lose faith in their country or even sympathize with the enemy.

6. Economic Disruption

Most modern economic systems depend on computers to function. Attacking the

Rahul Publications

computer networks of economic facilities like stock markets, payment systems, or banks can give hackers access to funds or prevent their targets from getting the money they need to live or engage in cyber or other warfare.

7. Surprise Cyberattack

These refer to the kinds of cyberattacks that would have an effect similar to Pearl Harbor or 9/11 massive strikes that catch the enemy off guard, weakening their defenses. They could be used to weaken the opponent in preparation for a physical attack as a form of hybrid warfare.

Q6. What are the reasons and motivations for cyber warfare?

Ans :

Reasons and Motivations for Cyber Warfare

1. Military

It is in the military's best interests to gain control of key elements of an enemy nation's cyberspace. An effective cyberattack could bring an enemy country's military to its knees and secure what would have been an otherwise costly victory.

2. Civil

Attacking the civil infrastructure of a nation directly impacts the people living and working in the country. This could be used to inspire fear or cause them to revolt against the government in protest, weakening the opponent from a political standpoint.

3. Hacktavism

Hacktivism involves hackers using cyber attacks to promote an ideology. Hacktivists can engage in cyber warfare by spreading propaganda or going after secrets and then exposing them to the rest of the world. In these ways, hacktivists can weaken an opponent's standing on the world stage, precluding support from other countries.

4. Income Generation

Cyber warfare "soldiers" can engage in these kinds of attacks for their own financial benefit. If they are employed by the government, they can earn a fee for their services. Further, they could break the defenses of a financial institution and steal money for themselves.

4. Nonprofit Research

Nonprofit research often reveals very valuable information that a country can use to solve a critical problem. For example, if a country is trying to develop a vaccine and another one already has it, cyber warfare could be used to steal information pertaining to their solution.

1.1.3.2 Cyber Crime

Q7. Define cyber crime? What are the various methods in cyber crime? How to prevent them.

Ans : **(Imp.)**

Cyber crime or computer-oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of a crime or it may be the target.

Cyber crime is the use of a computer as a weapon for committing crimes such as committing fraud, identities theft or breaching privacy. Cyber crime, especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment and government. Cyber crime may endanger a person or a nation's security and financial health.

Cyber crime encloses a wide range of activities, but these can generally be divided into two categories:

1. Crimes that aim computer networks or devices. These types of crimes involve different threats (like virus, bugs etc.) and denial-of-service (DoS) attacks.
2. Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

Rahul Publications

Classification

1. Cyber Terrorism

Cyber terrorism is the use of the computer and internet to perform violent acts that result in loss of life. This may include different type of activities either by software or hardware for threatening life of citizens.

In general, Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources.

2. Cyber Extortion

Cyber extortion occurs when a website, e-mail server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand huge money in return for assurance to stop the attacks and to offer protection.

3. Cyber Warfare

Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations concerning to the threat of cyber attacks, espionage and sabotage.

4. Internet Fraud

Internet fraud is a type of fraud or deceit which makes use of the Internet and could include hiding of information or providing incorrect information for the purpose of deceiving victims for money or property. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace.

5. Cyber Stalking

This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. In this case, these stalkers know their victims and instead of offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Prevention

Below are some points by means of which we can prevent cyber crime:

1. Use strong password

Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc, So make them complex. That means combination of letters, numbers and special characters.

2. Use trusted antivirus in devices

Always use trustworthy and highly advanced antivirus software in mobile and personal computers. This leads to the prevention of different virus attack on devices.

3. Keep social media private

Always keep your social media accounts data privacy only to your friends. Also make sure only to make friend who are known to you.

4. Keep your device software updated

Whenever your get the updates of the system software update it at the same time because sometimes the previous version can be easily attacked.

5. Use secure network

Public Wi-Fi are vulnerable. Avoid conducting financial or corporate transactions on these networks.

6. Never open attachments in spam emails

A computer get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

Rahul Publications

1.1.3.3 Cyber terrorism

Q8. What is cyber terrorism? Explain various types of cyber terrorism.

Ans :

Cyber terrorism is often defined as any premeditated, politically motivated attack against information systems, programs and data that threatens violence or results in violence. The definition is sometimes expanded to include any cyber attack that intimidates or generates fear in the target population. Attackers often do this by damaging or disrupting critical infrastructure.

Methods used for cyberterrorism

The intention of cyberterrorist groups is to cause mass chaos, disrupt critical infrastructure, support political activism or hacktivism, or inflict physical damage and even loss of life. Cyberterrorism actors use various methods. These include the following types of attacks:

(i) Advanced persistent threat (APT)

Advanced persistent threat (APT) attacks use sophisticated and concentrated penetration methods to gain network access. Once inside the network, the attackers stay undetected for a period of time with the intention of stealing data. Organizations with high-value information, such as national defense, manufacturing and the financial industry, are typical targets for APT attacks.

(ii) Computer viruses

Computer viruses, worms and malware target IT control systems. They are used to attack utilities, transportation systems, power grids, critical infrastructure and military systems.

(iii) DoS

DoS attacks attempt to prevent legitimate users from accessing targeted computer systems, devices or other computer network These attackers often go after critical infrastructure and governments.

(iv) Hacking

Hacking, or gaining unauthorized access, seeks to steal critical data from institutions, governments and businesses.

(v) Ransomware

Ransomware, a type of malware, holds data or information systems hostage until the victim pays the ransom. Some ransomware attacks also exfiltrate data.

(vi) Phishing

Phishing attacks attempt to collect information through a target's email, using that information to access systems or steal the victim's identity.

1.1.4 Cyber Espionage

Q9. What is Cyber Espionage? Explain about it.

Ans ;

Cyber espionage, or cyber spying, is a type of cyber attack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

Cyber espionage is primarily used as a means to gather sensitive or classified data, trade secrets or other forms of IP that can be used by the aggressor to create a competitive advantage or sold for financial gain. In some cases, the breach is simply intended to cause reputational harm to the victim by exposing private information or questionable business practices.

Cyber espionage attacks can be motivated by monetary gain; they may also be deployed in conjunction with military operations or as an act of cyber terrorism or cyber warfare. The impact of cyber espionage, particularly when it is part of a broader military or political campaign, can lead to disruption of public services and infrastructure, as well as loss of life.

Cyber Espionage Targets

The most common targets of cyber espionage include large corporations, government agencies, academic institutions, think tanks or other

Rahul Publications

organizations that possess valuable IP and technical data that can create a competitive advantage for another organization or government. Targeted campaigns can also be waged against individuals, such as prominent political leaders and government officials, business executives and even celebrities.

Cyber spies most commonly attempt to access the following assets:

- Research & Development data and activity
- Academic research data
- IP, such as product formulas or blueprints
- Salaries, bonus structures and other sensitive information regarding organizational finances and expenditures
- Client or customer lists and payment structures
- Business goals, strategic plans and marketing tactics
- Political strategies, affiliations and communications
- Military intelligence

Common Cyber Espionage Tactics

Most cyber espionage activity is categorized as an advanced persistent threat (APT). An APT is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization and evade existing security measures for long periods of time.

Executing an APT attack requires a higher degree of customization and sophistication than a traditional attack. Adversaries are typically well-funded, experienced teams of cybercriminals that target high-value organizations. They've spent significant time and resources researching and identifying vulnerabilities within the organization.

Most cyber espionage attacks also involve some form of social engineering to spur activity or gather needed information from the target in order to advance the attack. These methods often exploit human emotions such as excitement, curiosity, empathy or fear to act quickly or rashly. In doing so, cybercriminals trick their victims into giving up personal information, clicking malicious links, downloading malware or paying a ransom.

Other common attack techniques include:

- **Watering hole:** Malicious actors are able to infect legitimate websites commonly visited by the victim or people associated with the target with malware for the explicit purpose of compromising the user.
- **Spear-phishing:** A hacker targets specific individuals with fraudulent emails, texts and phone calls in order to steal login credentials or other sensitive information.
- **Zero-day exploits:** Cybercriminals leverage an unknown security vulnerability or software flaw prior to discovery and patching by the software developer or the customer's IT team.
- **Inside actors or insider threat:** A threat actor convinces an employee or a contractor to share or sell information or access to the system to unauthorized users.

1.1.5 Need for a Comprehensive Cyber Security Policy

Q10. What is the need for comprehensive cyber security policy?

Ans ; **(Imp.)**

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information. It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when they will occur. A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Rahul Publications

Need of Security policies

1. It increases efficiency

The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

2. It upholds discipline and accountability

When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law. The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

3. It can make or break a business deal

It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.

4. It helps to educate employees on security literacy

A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization sensitive data. It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.

We use security policies to manage our network security. Most types of security policies are automatically created during the installation. We can also customize policies to suit our specific environment. There are some important cybersecurity policies recommendations describe below

1. Virus and Spyware Protection policy

This policy provides the following protection:

- It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
- It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.
- It helps to detect the applications that exhibit suspicious behaviour by using SONAR heuristics and reputation data.

2. Firewall Policy

This policy provides the following protection:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals.
- It removes the unwanted sources of network traffic.

3. Intrusion Prevention policy

This policy automatically detects and blocks the network attacks and browser attacks. It also protects applications from vulnerabilities. It checks the contents of one or more data packages and detects malware which is coming through legal ways.

4. LiveUpdate policy

This policy can be categorized into two types one is LiveUpdate Content policy, and another is LiveUpdate Setting Policy. The LiveUpdate policy contains the setting which determines when and how client computers download the content updates from LiveUpdate. We can define the computer that clients contact to check for updates and schedule when and how often clients computer check for updates.

Rahul Publications

5. Application and Device Control

This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system. The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

6. Exceptions policy

This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.

7. Host Integrity policy

This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. We use this policy to ensure that the client's computers who access our network are protected and compliant with companies? securities policies. This policy requires that the client system must have installed antivirus

1.1.6 Need for a Nodal Authority

Q11. What is the use of Nodal Authority in cyber security?

Ans :

The Indian Computer Emergency Response Team (CERT-IN or ICERT) is an office within the Ministry of Electronics and Information Technology of the Government of India. It is the nodal agency to deal with cyber security threats like hacking and phishing. It strengthens security-related defence of the Indian Internet domain.

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

1.1.7 Need for an International convention on Cyberspace

Q12. What is the use of cyber space and explain about the necessity of international convention on cyberspace.

Ans :

- Over the past three decades, a convergence of information and communication technologies (ICTs), together with various governance policies, have created what we now call "cyberspace."
- Today cyberspace is a living reality, influencing all aspects of human behavior.
- The need to create a universal and transparent global framework to ensure the effective security and utilization of cyberspace "for the economic and social advancement of all peoples" has become paramount.
- Governments addressed this issue more than two decades ago, when the UN General Assembly (UNGA) adopted its first resolution on ICTs in December 1998.
- Other stakeholders including businesses, academia, and civil society have become more articulate in seeking a supportive international framework for their activities in cyberspace.

1. Cyberspace and its Stakeholders

- Emerging concepts related to the application of cyber technologies are propelling the world into the Fourth Industrial Revolution.

Rahul Publications

- The Internet of Things (IoT), artificial intelligence (AI), and robotics are expected to dominate cyberspace and redefine the role of human beings in this domain within just a few short years.
- A broad understanding of the internet incorporates cyber technologies such as wireless and fixed broadband, smartphones, the mobile internet, and cloud computing. Critical national infrastructures as well as social media platforms enable the flow of data across cyberspace, using a global network of fiber-optic cables and 13 primary root-servers that direct this data to its destination. The potential of cyberspace for the progress of mankind is immeasurable when it functions in a holistic manner. On the other hand, any fragmentation of this domain could have unfathomable ramifications.
- The four main stakeholders in cyberspace acknowledged by the UNGA are governments, businesses, academia, and civil society. These stakeholders are active in varying degrees within most UN member states.
- Of these four, governments have the primary responsibility for cyberspace policies, including cyber-security, and the application of cyber technologies for national governance objectives.
- All four stakeholders—governments, businesses, academia, and civil society—play a critical role in identifying the strengths and vulnerabilities of cyberspace. In varying degrees around the world, all four have expressed interest in creating the building blocks for a multi-stakeholder international framework for cyberspace.

2. Securing Cyberspace

- Within the United Nations, governments have taken the initiative to address the potential and also the dangers of cyberspace. In 1998, they adopted a resolution in the UNGA that noted the use of ICTs for both civilian and military purposes and prioritized "civilian applications." The resolution mandated the definition of "basic notions related to information security," while "developing international principles" to enhance cyber-security.
- The three broad areas that governments have taken up since 1998 to develop international cooperation in cyberspace relate to norms for cyber-security, measures to counter cybercrime, and agreeing on cyber policies for accelerating effective governance.
- In 2002 the UNGA adopted a resolution to create a regulatory framework for securing cyberspace. Dealing with the "global culture of cyber-security," this resolution highlighted nine elements that could contribute to such a global culture. These elements included awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment.
- To overcome the deadlock, the UNGA adopted a resolution in December 2018 to enhance "broad international cooperation." It decided to convene another GGE to focus on how international law applies to cyberspace and mandated the GGE to engage in multi-stakeholder consultations to generate greater acceptability for its eventual recommendations.
- the UNGA also adopted a resolution in December 2018 establishing an Open-Ended Working Group (OEWG) to make the discussions "more democratic, inclusive, and transparent.

3. Countering Cybercrime

- The first major legal impetus for seeking inter-governmental cooperation in countering cybercrime came in November 2001 from the Council of Europe, which is comprised of 47 states and includes Russia but not the United States, China, and other non-European countries. The Council of Europe adopted the Budapest Convention on Cybercrime, emphasizing that an "effective fight against cybercrime requires increased, rapid, and well-functioning international cooperation in criminal matters."

Rahul Publications

- The Budapest Convention has issued guidance notes on countering 11 specific threats. These included threats to computer systems, botnets, trans-border access, identity theft, DDOS attacks, critical infrastructure attacks, malware, spam, subscriber information, terrorism, and election interference. The relevance of these issues for broadening universal international cooperation on countering cybercrime through the UNGA is obvious.

4. Businesses and Cyberspace

- While governments have identified the key components for building a resilient international framework for cyberspace, major businesses have also realized the importance of such an international framework for their activities in cyberspace.
- The objective of the Charter is for the creation of "binding rules and standards to build trust in cyber-security and further advance digitalization," including for "the protection of data of individuals and businesses."
- Such rules and standards would need to be integrated into an international framework applicable to businesses in cyberspace

5. Towards an International Convention on Cyberspace

- In November 1967, the UNGA had responded to a call for "an effective international regime over the seabed and the ocean floor beyond a clearly defined national jurisdiction." The outcome of that response was the discussion of "the freedom-of-the-seas doctrine with technological changes that had altered man's relationship with the ocean."
- This led to the Third UN Conference on the Law of the Sea in 1973, with the objective to negotiate a comprehensive treaty for the maritime domain. The outcome was achieved nine years later (in 1982) with the adoption of the United Nations Convention on the Law of the Sea (UNCLOS).
- At its Seventy-fifth anniversary summit in September 2020, the UNGA will be faced with a similar choice. Taking into account the progress made in crystallizing international cooperation to secure cyberspace, counter cybercrime, maximize the use of cyber technologies for accelerating the objectives of sustainable development, and put people at the center of cyberspace, the UNGA must respond by convening a Conference on Cyberspace to negotiate and adopt an international multi-stakeholder framework for this unique domain.

1.2 Cyber Security Vulnerabilities

1.2.1 Overview

Q13. What is Vulnerability in Cyber Security? Explain about it.

Ans :

A vulnerability in cyber security refers to any weakness in an information system, system processes, or internal controls of an organization. These vulnerabilities are targets for lurking cybercrimes and open to exploitation through the points of vulnerability.

These hackers are able to gain illegal access to the systems and data and cause severe damage. Therefore, cybersecurity vulnerabilities are extremely important to monitor for the overall security posture as gaps in a network can result in a full-scale breach of systems in an organization.

Examples of Vulnerabilities

- A weakness in a firewall that can lead to malicious hackers getting into a computer network
- Lack of security cameras
- Unlocked doors at businesses

All of these are weaknesses that can be used by others to hurt a business or its assets.

There are many causes of Vulnerabilities like:

1. **Complex Systems:** Complex systems increase the probability of misconfigurations, flaws, or unintended access.

Rahul Publications

2. **Familiarity :** Attackers may be familiar with common code, operating systems, hardware, and software that lead to known vulnerabilities.
3. **Connectivity :** Onnected devices are more prone to have vulnerabilities.
4. **Poor Password Management :** and reused passwords can lead from one data breach to several.
5. **OS Flaws :** systems can have flaws too. Unsecured operating systems by default can give users full access and become a target for viruses and malware.
6. **Internet :** Internet is full of spyware and adware that can be installed automatically on computers.
7. **Software Bugs :** Programmers can sometimes accidentally, leave an exploitable bug in the software.
8. **Unchecked user input :** Software or a website assumes that all input is safe, it may run unintended SQL injection.
9. **People :** Social engineering is the biggest threat to the majority of organizations. So, humans can be one of the biggest causes of vulnerability.

Types

(i) System Misconfigurations

Network assets that have disparate security controls or vulnerable settings can result in system misconfigurations. Cybercriminals commonly probe networks for system misconfigurations and gaps that look exploitable. Due to the rapid digital transformation, network misconfigurations are on the rise. Therefore, it is important to work with experienced security experts during the implementation of new technologies.

(ii) Out-of-date or Unpatched Software

Similar to system misconfigurations, hackers tend to probe networks for unpatched systems that are easy targets. These unpatched vulnerabilities can be exploited by attackers to steal sensitive information. To minimize these kinds of risks, it is essential to establish a patch management schedule so that all the latest system patches are implemented as soon as they are released.

(iii) Missing or Weak Authorization Credentials

A common tactic that attackers use is to gain access to systems and networks through brute force like guessing employee credentials. That is why it is crucial that employees be educated on the best practices of cybersecurity so that their login credentials are not easily exploited.

(iv) Malicious Insider Threats

Whether it's with malicious intent or unintentionally, employees with access to critical systems sometimes end up sharing information that helps cyber criminals breach the network. Insider threats can be really difficult to trace as all actions will appear legitimate. To help fight against these types of threats, one should invest in network access control solutions, and segment the network according to employee seniority and expertise.

(v) Missing or Poor Data Encryption

It's easier for attackers to intercept communication between systems and breach a network if it has poor or missing encryption. When there is poor or unencrypted information, cyber adversaries can extract critical information and inject false information onto a server. This can seriously undermine an organization's efforts towards cyber security compliance and lead to fines from regulatory bodies.

(vi) Zero-day Vulnerabilities

Zero-day vulnerabilities are specific software vulnerabilities that the attackers have caught wind of but have not yet been discovered by an organization or user.

Rahul Publications

In these cases, there are no available fixes or solutions since the vulnerability is not yet detected or notified by the system vendor. These are especially dangerous as there is no defense against such vulnerabilities until after the attack has happened. Hence, it is important to remain cautious and continuously monitor systems for vulnerabilities to minimize zero-day attacks.

1.2.2 Vulnerabilities in software

Q14. What is a software vulnerability? Explain about the most common security vulnerabilities.

Ans : **(Imp.)**

A software vulnerability is a security flaw, glitch, or weakness found in software or in an operating system (OS) that can lead to security concerns. An example of a software flaw is a buffer overflow. This is when software becomes unresponsive or crashes when users open a file that may be "too heavy" for the program to read.

However, this commonly encountered error becomes a security concern when attackers uncover the vulnerability, conduct research about it, and create a malicious code or exploit that targets this glitch to launch their schemes. Some schemes may include gaining administrator privileges which gives attackers control over the vulnerable system or infecting it with malware.

The most common security vulnerabilities are as follows:

1. Broken Access Control

User restrictions must be properly enforced. If they are broken, it can create a software vulnerability. Untrustworthy agents can exploit that vulnerability.

2. Cryptographic Failures

Sensitive data such as addresses, passwords, and account numbers must be properly protected. If it isn't, untrustworthy agents take advantage of the vulnerabilities to gain access.

3. Injection

Injection flaws occur when untrusted data is sent as part of a command or query. The attack can then trick the targeted system into executing unintended commands. An attack can also provide untrustworthy agents access to protected data.

4. Insecure Design

Insecure design refers to risks related to design flaws, which often includes the lack of at least one of the following:

- Threat modeling
- Secure design patterns
- Secure design principles
- Reference architecture

5. Security Misconfiguration

Security misconfigurations are often the result of:

- Insecure default configurations.
- Incomplete or impromptu configurations.
- Open Cloud storage.
- Misconfigured HTTP headers.
- Wordy error messages that contain sensitive information.

6. Vulnerable and Outdated Components

Components are made up of libraries, frameworks, and other software modules. Often, the components run on the same privileges as your application. If a component is vulnerable, it can be exploited by an untrustworthy agent. This causes serious data loss or server takeover.

7. Identification and Authentication Failures

Authentication and session management application functions need to be implemented correctly. If they aren't, it creates a software vulnerability that can be exploited by

Rahul Publications

untrustworthy agents to gain access to personal information.

8. Software and Data Integrity Failures

Software and data integrity failures refer to assumptions made about software updates, critical data, and CI/CD pipelines without verifying integrity. In addition, deserialization flaws often result in remote code execution. This enables untrustworthy agents to perform replay, injection, and privilege escalation attacks.

9. Security Logging and Monitoring Failures

Insufficient logging and monitoring processes are dangerous. This leaves your data vulnerable to tampering, extraction, or even destruction.

10. Server-Side Request Forgery

Server-side request forgery refers to data that shows a relatively low incidence rate with above average testing coverage, and an above-average rating for Exploit and Impact potential.

Here are the three most efficient and effective practices to prevent software vulnerabilities.

1. Establish Software Design Requirements

Establish software design requirements. Define and enforce secure coding principles. This should include using a secure coding standard. This will also inform how to effectively write, test, inspect, analyze, and demonstrate your code.

2. Use a Coding Standard

Coding standards such as OWASP, CWE, and CERT enable you to better prevent, detect, and eliminate vulnerabilities. Enforcing a coding standard is easy when you use a SAST tool like Klocwork. Klocwork identifies security defects and vulnerabilities while the code is being written.

3. Test Your Software

It is essential that you test your software as early and often as possible. This helps to ensure that vulnerabilities are found and eliminated as soon as possible. One of the most effective ways to do this is by using a static code analyzer like Klocwork as part of your software testing process.

As part of your development pipeline, static analysis complements your testing efforts. Tests can be run during CI/CD integration as well as nightly integration testing.

Static code analyzers automatically inspect your code as it's being written to identify any errors, weaknesses, or bugs. You can even apply any software vulnerability definition that would be applicable.

1.2.3 System administration

Q15. What is system administration? Explain the roles and responsibilities of system administrator.

Ans :

System administration is the field of work in which someone manages one or more systems, be they software, hardware, servers or workstations. Its goal is ensuring the systems are running efficiently and effectively.

System administration is typically done by information technology experts for or within an organization. Their job is to ensure that all related computer systems and services keep working .

A system administrator, or sysadmin, is a person responsible to maintain and operate a computer system or network for a company or other organization. System administrators are often members of an information technology department.

Types of adminstration roles

For each delegate user domain (including the enterprise domain), predefined administrator types can be assigned in that domain. The following are the various administrator types and the set of administrative functions that can be performed by administrators assigned to each of these types:

Rahul Publications

- **Tivoli Access Manager Administrator:** The Tivoli Access Manager administrator is a member of the iv-admin group. The Tivoli Access Manager administrator can perform all delegate administration functions.
- **Domain Administrator:** The domain administrator can perform administrative functions for the users in their domain. Domain administrators can create new users and administrators in their own domain, and assign an existing domain user to be an administrator (of any type except domain administrator) for the domain.
- **Senior Administrator:** A senior administrator has the same authority as a domain administrator, except that a senior administrator cannot assign additional administrators.
- **Administrator:** An administrator has the same authority as a senior administrator, except that an administrator cannot create new domain users. An administrator can modify an existing user's properties.
- **Support Administrator:** A support administrator serves the user in a help desk role and is able to view users' properties, change users' passwords, and modify the Is Password Valid? flags for users.

Roles & Responsibilities

Where a system administrator knows a lot about many sectors of IT, a security administrator specializes in the security of the computers and networks.

In general, computer security, also known as IT security or cyber security, includes protecting computer systems and networks from the theft and/or damage to hardware, software, or information. It also includes preventing disruption or misdirection of these services. This should include knowledge of specific security devices, like firewalls, Bluetooth, Wi-Fi, and the IoT. This also includes general security measures and an ability to stay abreast of new security sector developments.

Specific roles and responsibilities of a security administrator may include:

- Monitoring networks for security breaches, investing violations as occurs
- Developing and supporting organizational security standards, best practices, preventative measures, and disaster recovery plans
- Conducting penetration tests (simulating cyberattacks to find vulnerabilities before others can find them)
- Reporting on security breaches to users, as necessary, and to upper management
- Implementing and updating software to protect information
- Staying up to date on IT security trends and information
- Recommending security enhancements to management and C-suite executives

1.2.4 Complex Network Architectures

Q16. What is Cybersecurity Architecture? Explain the features and components of it.

Ans :

- Cybersecurity architecture, also known as "network security architecture", is a frame work that specifies the organizational structure, standards, policies and functional behavior of a computer network, including both security and network features.
- Cybersecurity architecture is also the manner in which various components of your cyber or computer system are organized, synced and integrated.
- A cybersecurity architecture framework is one component of a system's overall architecture. It's designed and built to provide guidance during the design of an entire product/system.
- Security architecture helps to position security controls and breach countermeasures and how they relate to the overall systems framework of your company. The main purpose of these controls is to maintain your critical system's quality attributes such as confidentiality, integrity and availability.

Rahul Publications

- This framework unifies various methods, processes and tools in order to protect an organization's resources, data and other vital information. The success of a cybersecurity architecture relies heavily on the continuous flow of information throughout the entire organization. Everyone must work according to the framework and processes of your company's security architecture.

Security

The components listed below are part of an effective and carefully planned security architecture:

1. Direction in the area of incident response to threats, disaster recovery, systems configuration, account creation and management, and cybersecurity monitoring.
2. Identity management.
3. Decided inclusion and exclusion of those subject to the domain of the security architecture.
4. Access and border control.
5. Validation and adjustment of the architecture.
6. Training.

Features

The following are some of the features of cybersecurity architecture:

- **Network Elements**
  1. Network nodes like computers, NICs, repeaters, hubs, bridges, switches, routers, modems, gateways.
  2. Network communication protocols (TCP/IP, DHCP, DNS, FTP, HTTP, HTTPS, IMAP)
  3. Network connections between nodes using specific protocols
  4. Network topologies among nodes such as point-to-point, circular, chain, and hybrid
- **Security Elements**
  1. Cybersecurity devices like firewalls, Intrusion Detection/Protection Systems [IDS/IPS], encryption/decryption devices.
  2. Cybersecurity software (anti-virus software, spyware software, anti-malware software)
  3. Secure network communication protocols (TCP/IP, DHCP, DNS, FTP, HTTP, HTTPS, IMAP).
  4. Strong encryption techniques like end-to-end encryption, zero-knowledge privacy, blockchain.
- **Security Frameworks & Standards**
  1. Cybersecurity framework architecture standards like NIST Risk Management Framework (RMF) SP 800-37 and ISO IEC 27000-Series.
  2. Technology standards for cybersecurity software choices.
- **Security Procedures & Policies**

  These are security procedures and policies directed towards your organization and enforced. According to Cybersecurity Forum, a cybersecurity architecture should ideally be definable and simulatable using an industry-standard architecture modeling language (e.g., SysML, UML2).

Key Phases in Security Architecture

These are the key phases in the security architecture framework and process:

1. **Architecture Risk Assessment:** Here, you evaluate the influence of vital business assets, the risks, and the effects of vulnerabilities and security threats to your organization.
2. **Security Architecture and Design:** At this phase, the design and architecture of security services are structured to aid the protection of your organization's assets in order to facilitate business risk exposure objectives and goals.

Rahul Publications

3. **Implementation:** Cybersecurity services and processes are operated, implemented, monitored and controlled. The architecture is designed to ensure that the security policy and standards, security architecture decisions, and risk management are fully implemented and effective for a long period.

4. **Operations and Monitoring:** Here, measures like threat and vulnerability management and threat management are taken to monitor, supervise and handle the operational state in addition to examining the impact of the system's security.

1.2.5 Open Access to Organizational Data

Q17. What is open data? Explain how can we openly access to organizational data.

Ans : **(Imp.)**

Open data is research data that is freely available on the Internet for anyone to download, modify, and distribute without any legal or financial restrictions.

Open data is:

- **Available:** the data should be in whole, downloadable from the Internet, with no costs apart from reproduction fees
- **Accessible:** the data should be provided in a convenient form that can be modified
- **Reusable:** this should be expressed under terms provided with the data
- **Redistributable:** the data can be combined with data from other research
- **Unrestricted:** everyone can use, modify, and share the data, regardless of how they use the data (e.g. for commercial, non-commercial, or educational purposes)

A number of benefits can be realized through the open sharing of data:

- Increases reproducibility of research
- Promotes future research growth
- Supports research integrity
- Prevents duplication and loss of research
- Provides opportunities for collaboration
- Strengthens the economy
- Is recognized as an important aspect of research across many research communities.

Challenges

Challenges to making data openly available include:

1. **Labelling:** Open data is only useful if it is clearly identified as open. Improper labelling limits its benefits. Labelling of data ensures that researchers are acknowledged when their data is reused and distributed.

2. **Licensing:** Data on publisher's websites and in data repositories should be clearly defined as available for free and unrestricted access, redistribution and reuse. A publisher or researcher may state that the publisher or researcher reserves rights to all data, or that there is an open knowledge license to the data. See Open Definition for a list of licences.

3. **Research ethics restrictions:** When making data openly available one must consider the safeguarding of information, obtaining consent and the secondary use of identifiable information, and how identifiable information is handled during data linkage.

How does one make open data available?

There are two steps to making one's data open:

(i) Make the data publicly available through a data repository or publisher's website.

Open data can be made available by posting it to a data repository. York University Libraries makes available two repositories for data deposit: Scholars Portal Dataverse and YorkSpace. Additional options for multi-disciplinary data repositories include Figshare, and re3data.org where searches can be filtered by a number of dimensions, including Country and Subject area.

Rahul Publications

(ii) Assigning an open data license. This is required even if the data is for 'Public Domain'

To make data open, the data must be licensed. There are two types of license:

- **Public Domain Dedication and License (PDDL):** all data is put in the Public Domain.
- **Open Database Licenses: reusers of data are required to attribute and share back changes with the original researcher:** Licenses include the Database Contents License (DbCL) and Open Data Commons Open Database License (ODbL).

1.2.6 Weak Authentication

Q18. What is weak authentication? Explain various weak authentication sources.

Ans :

Weak Authentication describes any scenario in which the strength of the authentication mechanism is relatively weak compared to the value of the assets being protected. It also describes scenarios in which the authentication mechanism is flawed or vulnerable.

Password Strength

The "strength" of a password is related to the potential set of combinations that would need to be searched in order to guess it. For example, a password scheme with a length of two characters and consisting only of digits would represent a a search space of 100 possible passwords (10 x 10), whereas a 12 digit password would represent 10^{12} possible combinations. The larger the set of possible combinations, the harder it is to guess and the stronger the password.

Thus, the following factors influence password strength:

- **Length:** The number of characters in the password. The greater the length, the greater the strength.
- **Character Set:** The range of possible characters that can be used in the password. The broader the range of characters, the greater the strength. It is typical for strong password schemes to require upper and lower case letters, digits, and punctuation characters.

Password Policy

Password Policy describes the rules that are enforced regarding password strength, changes, and re-use. An effective password policy supports strong authentication. It is generally accepted that the each of the following will increase the integrity of the authentication process:

- Periodically changing the password for an account makes it less likely that a password will be compromised, or that a compromised password will be used. This is termed password expiration.
- Prohibiting the re-use of the same (or similar) password to the one being changed will prevent password expiration from being circumvented by users.
- Enforcing minimum strength rules for passwords will guarantee application compliance with Password Policy.
- Prohibiting dictionary words and/or popular passwords will make password cracking less likely.
- The use of secret questions to further demonstrate identity.

The more of these rules that are enforced, the stronger will be the authentication mechanism,

1. Password Cracking

There are countless hacking tools and frameworks available to help an attacker guess a password through an automated sequence of attempts. This is called "brute forcing" because such tools will attempt all possible password combinations given a set of constraints in an attempt to authenticate. An application that does not protect itself against password cracking in some manner may be considered as having a Weak Authentication vulnerability depending the requirements and risk-level.

Rahul Publications

2. Dictionary Attacks

In addition to brute force attacks, password cracking tools also typically have the ability to test a file of candidate passwords. This is called a dictionary attack because the file used may actually be a dictionary of words. Passwords that can be found in a dictionary are considered weak because they can eventually discovered using a dictionary attack. An application that allows dictionary words as passwords may be considered as having a Weak Authentication vulnerability depending the application requirements and risk-level.

3. Popular Passwords

Since passwords are usually freely chosen and must be remembered, and given that humans are lazy, passwords that are easy to remember tend to be more popular than those that are not. In fact, some passwords become very popular and are used far more frequently that might be expected. Although the most popular entries change over time, you can always find a "top-N" list somewhere, like here, or here, or here. Clearly it is in the user's best interest to avoid the most popular passwords.

An application that allows popular passwords may be considered as having a Weak Authentication vulnerability depending the application requirements and risk-level.

4. Authentication Bypass

The whole purpose of authentication is to ensure that only authorized users gain access to the application capabilities and the information it contains. It is essential therefore that the system verifies the "authentication status" of the user for every user action or request before it is carried out. The ability of a user to access any application feature or resource without having first authenticated represents a Weak Authentication vulnerability.

1.2.7 Unprotected Broadband communications

Q19. What are the risks for using unprotected broadband communications? Explain how to use it safely.

Ans :

An unsecure wireless connection is one you can access without a password. Public networks offered in places like cafes are often open. Although these provide free wireless Internet access, using public Internet comes with dangers.

If your home Internet is open, you should consider securing wireless access to protect your data and avoid legal trouble.

The two types of public networks are ones that are left open by businesses and ones that are left open by individuals. An open network from a business allows customers to use the Internet in the establishment such as patrons of a coffee shop using the network to work. An open network in a home comes from a router that hasn't been secured. Sometimes this is unintentional, if the owner doesn't know that her network is open.

The Risks of Hosting Open Wi-Fi

Here are some other risks of using unprotected public networks:

1. As these networks do not require any authentication, the hackers receive unfettered access to unprotected gadgets within the same network.
2. The hackers may position between you and the hotspot, which leaves youvulnerable to attacks.
3. If a hacker gets access to your personal information, he may misuse the same at any point in time.
4. Unsecured Wi-Fi networks are also used by cyber criminals to distribute infected software like viruses and malware.
5. Intruders may not damage the public network but may use it for illegal purposes that may have severe repercussions.

Rahul Publications

Stay Protected While Using Public Wi-Fi network

Hackers target users who do not have the right knowledge to remain protected. Here are a few tips that ensure security while connecting to a public Wi-Fi network:

1. Use a Virtual Private Network (VPN)

When you use a VPN, the information is encrypted. Therefore, the hackers are unable to access your confidential information even if they position within the connection. Also, criminals often do not want to spend time decrypting the information as it is a long and tedious procedure.

2. Choose Secure Sockets Layer (SSL) connections

It is most likely that you may not have access to a VPN. Nonetheless, you may still encrypt your data while using the internet on a public network. It is recommended that you enable the "Always use HTTPS" setting on frequently used websites for more security.

3. Switch off Sharing

While connecting to the Internet on a public network, you may not share personal files and data. It is advisable to switch off sharing from the control panel or system preferences while using a laptop. It generally depends on the operating system. Alternatively, you may allow Windows to switch it off while opting for "Public" option when you connect to an unprotected network the first time.

4. Check the Terms and Conditions

Before connecting to a public Wi-Fi network, reading the terms and conditions may be beneficial. Although you may not understand all these, it is likely you will be able to comprehend the kind of data the network will collect and how it will be used. Moreover, it is important you do not install any browser extensions or additional software.

5. Security Protocols

Using a well-configured firewall mechanism to filter data transmission over the public network is recommended. In addition, having updated security software, such as anti-key-logger or anti-malware is also beneficial.

6. Use a Security Tool

Tools like Wi-Fi check helps to verify the download speed and the security of the network. It helps in identifying if the public network is secure or not. Such tools are highly beneficial while using a public Wi-Fi network.

1.2.8 Poor Cyber Security Awareness

Q20. What are the reasons for lack of cyber security awareness? Explain how to over come it.

Ans : **(Imp.)**

Companies collect and store enormous amounts of data. From billing invoices to customers' credit card information, so much of your business focuses on private data.

To succeed, you have to trust employees with this data. But, sometimes, even the most well-intentioned employee can make mistakes that leave your company vulnerable to cyberattacks.

Here's a list of the seven most common employee mistakes and what you can do to fix them.

1. Opening Emails from Unknown People

Email is the preferred form of business communication. The average person receives 235 emails every single day, according to The Radicati Group. With that many emails, it stands to reason that some are scams. Opening an unknown email, or an attachment inside an email, can release a virus that gives cybercriminals a backdoor into your company's digital home.

Solutions:

- Advise employees not to open emails from people they don't know.
- Advise employees to never open unknown attachments or links.

Rahul Publications

2. Having Weak Login Credentials

Mashable reported that 81% of adults use the same password for everything. Repetitive passwords that use personal information, such as a nickname or street address, are a problem. Cybercriminals have programs that mine public profiles for potential password combinations and plug in possibilities until one hits. They also use dictionary attacks that automatically try different words until they find a match.

Solutions:

- Require employees to use unique passwords
- Add numbers and symbols to a password for increased security. For example, change "Seattle" to "S3att!e."
- Take the headache out of this by using a password manager software to automatically generate strong individual passwords for multiple apps, websites and devices.

3. Leaving Passwords on Sticky Notes

Have you ever wandered through the office and spotted a sticky note on a screen with passwords written on it? It happens more often than you think. While you want a certain level of trust inside your organization, leaving passwords visible is too trusting.

Solutions:

- If employees must write down passwords, ask that the paper copies are kept inside locked drawers.

4. Having Access to Everything

In some cases, companies don't compartmentalize data. In other words, everyone from interns to board members can access the same company files. Giving everyone the same access to data increases the number of people who can leak, lose or mishandle information.

Solutions:

- Set up tiered levels of access, giving permission only to those who need it on each level.
- Limit the number of people who can change system configurations.
- Don't provide employees with admin privileges to their devices unless they really require such set up. Even employees with the admin rights should only use them as needed, not routinely.

5. Lacking Effective Employee Training

Research shows the majority of companies do offer cybersecurity training. However, only 25% of business executives believe the training is effective.

Solutions:

- Provide annual cybersecurity awareness training. Topics could include:
- Reasons for and importance of cybersecurity training
- Phishing and online scams
- Locking computers
- Password management
- How to manage mobile devices
- Relevant examples of situations

6. Not Updating Antivirus Software

Your company should deploy antivirus software as a protective measure, but it shouldn't be up to employees to update it. At some companies, employees are prompted to make updates and can decide whether or not the updates take place. Employees likely say no to updates when they're in the middle of a project, since many updates force them to close programs or restart computers.

Antivirus updates are important, should be handled promptly and shouldn't be left to employees.

Solutions:

- Set up all system updates to take place after work hours automatically.
- Don't let any employee, no matter what their title, opt out of this company policy.

Rahul Publications

7. Using Unsecured Mobile Devices

Do your employees have company cell phones, tablets or laptops? If so, do you have protocol in place to keep these devices secure? Many companies have a lax attitude toward mobile devices, but they present an easy target for cybercriminals.

Solutions:

- Every device should be password protected.
- If a device is lost or stolen, have a point of contact to report this to and steps taken to deactivate the device remotely.
- Use endpoint security solutions to manage mobile devices remotely.
- Don't conduct confidential transactions using untrusted public Wi-Fi.

Cyber security awareness best practices

An effective staff awareness programme should complement the way people work rather creating rules that hinder employees' ability to get their jobs done.

The objective is to support them in obtaining the skills and knowledge required to work, and knowing when to raise any concerns.

- **All employees at every level of the organization should receive training :** No one is immune from mistakes or from being targeted by scammers. In fact, senior employees are proportionally more likely to be targeted by scammers (with the likes of business email compromise schemes) because they represent higher-value targets.
- **Training should occur multiple times a year:** Staff awareness training must be performed regularly to ensure that the knowledge is embedded.

  To demonstrate the importance of this, a study presented at the USENIX SOUPS security conference last year found that employees who went six months or more without phishing awareness training become increasingly likely to fall victim to scams.
- **Consider how your employees work:** What are your employees' workflows? What obstacles do they face when performing certain activities?

  Knowing the answers to these will help you understand the types of awareness training they need.
- **Don't be overly critical when employees make mistakes:** It's tempting to strongly reprimand anyone who makes an error despite receiving awareness training. However, experts warn against this; employees are rarely motivated by fear, and it will make them less likely to report mistakes when they occur.

  So although you should be strict about employees taking awareness training – and ideally these courses should come with tests to ensure that staff have understood the content – you should use errors as a learning experience.
- **Look for ways to complement staff awareness training:** There are also things you can do in addition to training courses to boost your staff's understanding of cyber security.

  You might consider placing posters around the office (if you are still office-based) or creating email signatures containing security tips.

Implementing cyber security awareness training

Here are seven tips to help you get your cyber security awareness programme started:

1. Consider your requirements

When it comes to staff awareness, the 'one-size-fits-all' approach isn't appropriate for all organisations.For your staff awareness training programme to succeed, you'll need to first consider the diverse needs and culture of your business and tailor the training accordingly.

2. Set metrics for success

Before you implement a staff awareness programme, you need to ensure it can

Rahul Publications

succeed and decide how to measure that success. This means you must decide on the metrics you will use and take measurements to determine a benchmark before you start.

3. Be thorough

Staff awareness training for the GDPR does not mean simply briefing your employees about the Regulation. Instead, it should comprise a thorough programme that ensures all employees underst and your organization's practices and procedures for processing personal data.

4. Engage your staff

Engaging staff training is critical to your programme's success. Incorporating thought-provoking activities will give your staff a clear understanding of the key changes introduced by the GDPR and the requirements that will affect their day-to-day work.

A common technique to make security awareness programmes more engaging for participants is 'gamification', which uses behavioural motivators taken from games such as rewards, competition and loss aversion.

5. Focus on behaviour, not knowledge

To change their behaviour, employees need to understand how the content applies to them in their everyday roles.

To bridge the gap between knowing and doing, it's essential to provide your staff with context for what they are learning and realistic examples they can follow. Doing so will help foster a much-needed cultural shift in which security becomes a part of everyday operations.

6. Time it right

There may be an urgent need to train your workforce, but this doesn't mean your awareness programme should be deployed in haste. Instead, consider a phased rollout, allowing you to meet some immediate requirements, after which you can refine and improve the programme.

7. Play the long game

For long-term success, your staff awareness programme should be an ongoing process that begins at induction and is reinforced by regular updates throughout the year and/or whenever staff-related security incidents occur.

1.3 Cyber Security Safeguards

1.3.1 Overview

Q21. What are cyber security safe guards? Explain various types of safe gaurds.

Ans :

Cybersecurity safeguards are the fundamental part of a cybersecurity investment. They are the expected outcomes of a cybersecurity investment and must be understood sufficiently so that they can be analyzed and evaluated within a systematic decision making process.

A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

The protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Examples of Commonly Used Security Safeguards

1. Administrative Safeguards

- Access to personal health information and access to any place or system where personal health information is kept must be restricted to individuals who are authorized to use, modify, transform, disclose, dispose or destroy personal health information to perform their assigned duties..
- Security checks may need to be employed to ensure that individuals in key employee positions are screened. This includes background checks and taking oaths of

Rahul Publications

confidentiality, where necessary. Screening of personnel should be done on a regular basis, and criminal record checks may be appropriate and required in some cases. For example, health care providers like hospitals and nursing homes should require every successful applicant for employment and every new volunteer to provide a criminal records check.

- All systems programmers, network/LAN technical staff, ID administrators, file and mailroom staff that have privileged access to the work environment and have to be "trusted".
- Information access privileges should be reviewed, modified or revoked as necessary when: an employee is transferred by appointment, assignment or secondment;
  - an employee commences an extended period of absence, including maternity, medical, military or community service;
  - access privileges have not been exercised for a period of time; or
  - the employment or contract of the individual has been terminated. Upon termination:
- the individual should be debriefed with respect to ongoing responsibilities for the confidentiality of Trustee information;
- access privileges (system passwords, user ID's, combinations, etc.) to systems, restricted access zones, and IT facilities should be revoked; and
- all security related items (badges, keys, documents, etc.) issued to the individual should be retrieved.
- To ensure that parties accessing information are who they say they are, the identity of any individual who accesses, uses, modifies, transforms, discloses or disposes of health information must be verified and authenticated prior to access to information being granted. The most common form of this safeguard in an electronic environment is the use of passwords. However, it could also include requiring proof of identification using tokens, biometrics, challenge/response scenarios, one-time passwords, digital signatures and certification authorities.

  Authentication passwords or codes must be:
  - generated, controlled and distributed in a manner which maintains the confidentiality and integrity of the code or password;
  - known only to the user of the identifier;
  - either pseudo-random in nature or verified by an automated process designed to counter triviality and repetition;
  - at least 7 characters in length;
  - one-way encrypted for storage in the computer system subject to a history check to preclude reuse;
  - prompted for manual user entry when using automatic or scripted log-on processes;
  - changed at least every 90 days; and
  - a mixture of characters, both upper and lower case, numbers, punctuation and special symbols.
- Records should be kept identifying all instances of access, use, modification, transformation, disclosure or disposal of individually identifying diagnostic, treatment and care information.
- Records must be kept of all instances of unauthorized access, use, change, deletion/ disposition or disclosure of personal health information.
- Procedures, policies and practices must be implemented to restore, replace or re-create personal health information that has been damaged, lost or destroyed either accidentally or deliberately.
- Policies, procedures, practices and other safeguards must be implemented to minimize the risk from unauthorized access to, or unauthorized use, modification, transformation, disclosure, disposal or destruction of

Rahul Publications

personal health information, and also to ensure accuracy and completeness of personal health information.

2. Physical Safeguards

- In addition to restrictions on who can access personal health information, access to the facility, offices, information retrieval equipment and systems and information stores must be controlled to ensure that access is granted only to individuals with authorization for such access. These controls relate to mechanisms in a computer operating system, hardware unit, software package, file room or mailroom. This is typically a password for systems access but may include card locks and physical security access systems such as keys, digital card keys and cipher lock barriers.
- Physical security safeguards to maintain access control can range from anti-theft systems such as bolting equipment to the floor in secure rooms, locked desks and cabinets.
- Smaller Trustees with little personal health information in electronic form should concentrate on physical security measures (locked rooms or cabinets, adequate access controls for employees and the public and sound disposition measures for the information). Larger Trustees with sensitive personal health information in a variety of forms and formats will have to take a wider range of security measures based upon the threat and risk analysis conducted.
- Stringent protection measures should be applied to personal health information with a high level of sensitivity and with a greater possibility of causing damage to an individual if it is accidentally disclosed, stolen or finds its way into unauthorized hands.
- For less sensitive personal health information where the risk of compromise or unauthorized access is low, a Trustee may only need to put in place lower grade security measures. Examples of these would be unlocked cabinets in a controlled area that are locked at night; computers being kept behind service counters, with screens not visible to patients/ clients other than the subjects of the information; and co mputers accessed through restricted authorization codes.

3. Technical Safeguards

- All methods of communication of personal health information must be secure from unauthorized access, including eavesdropping, interception and diversion.
- "All methods of communication" includes verbal communication, transmission of written documentation, telephone, cellular phone, fax, e-mail, video and audio communication or any other form of electronic communication.
- "Eavesdropping" occurs when unauthorized individuals inadvertently or through the use of deceptive techniques such as remote monitoring of conventional telephone or cellular phone conversations, voice mail or text messaging, gain access to personal health information.
- "Interception" occurs when unauthorized individuals inadvertently or through the use of deceptive techniques gain access to health information ex: by interrupting the flow of information over a transmission line, through the use of electronic or other means.
- "Diversion" occurs when the direction of the flow of personal health information is changed inadvertently or through the use of deceptive techniques so that an unauthorized recipient can gain access to it.
- Identification and authentication safeguards to monitor security systems and procedures may be needed. These include virus scanners, firewalls, monitoring operating system logs, software logs, version control and document disposition certification.
- Encrypted storage and transmission is necessary for particularly sensitive personal health information.

Anonymous identifiers allow processing of discrete person level records to analyze information across time, data sources or geographical areas for such purposes as measuring utilization, health system performance, and health outcomes or

Rahul Publications

program evaluation. Encryption may be hardware or software based and is usually "key" based

- All systems hardware and software must be secure from inappropriate access, accident, misappropriation, viruses and systems failure.
- Put in place disaster recovery safeguards. These can range from the use of on-site diskettes/tapes to replication with an external system and duplication (ex: photocopiers) on other media forms with possible off-site storage facilities.
- Other related safeguards include the use of redundant or fault tolerant equipment such as disk shadowing/mirroring, dual systems, hot backups and alternate routing. These safeguards are typically hardware based but require software/procedures to manage the environment.
- Personal or health information should not be stored on mobile computing devices unless absolutely necessary. Consideration should be given to other technologies that allow secure, remote access to the required network and data instead.

1.3.2 Access control

Q22. What is access control? Explain the components of access control

Ans :

Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources. Secure access control uses policies that verify users are who they claim to be and ensures appropriate control access levels are granted to users.

Implementing access control is a crucial component of web application security, ensuring only the right users have the right level of access to the right resources. The process is critical to helping organizations avoid data breaches and fighting attack vectors, such as a buffer overflow attack, KRACK attack, on-path attack, or phishing attack.

Access control is managed through several components:

(i) Authentication

Authentication is the initial process of establishing the identity of a user. For example, when a user signs in to their email service or online banking account with a username and password combination, their identity has been authenticated. However, authentication alone is not sufficient to protect organizations' data.

(ii) Authorization

Authorization adds an extra layer of security to the authentication process. It specifies access rights and privileges to resources to determine whether the user should be granted access to data or make a specific transaction.

For example, an email service or online bank account can require users to provide two-factor authentication (2FA), which is typically a combination of something they know (such as a password), something they possess (such as a token), or something they are (like a biometric verification). This information can also be verified through a 2FA mobile app or a thumbprint scan on a smartphone.

(iii) Access

Once a user has completed the authentication and authorization steps, their identity will be verified. This grants them access to the resource they are attempting to log in to.

(iv) Manage

Organizations can manage their access control system by adding and removing the authentication and authorization of their users and systems. Managing these systems can become complex in modern IT environments that comprise cloud services and on-premises systems.

(v) Audit

Organizations can enforce the principle of least privilege through the access control audit process. This enables them to gather data around user activity and analyze that information to discover potential access violations.

Rahul Publications

Q23. Explain about types and challenges of access control.

Ans :

The main models of access control are the following:

- **Mandatory access control (MAC):** This is a security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system (OS) or security kernel. It grants or denies access to those resource objects based on the information security clearance of the user or device. For example, Security Enhanced Linux (SELinux) is an implementation of MAC on the Linux OS.
- **Discretionary access control (DAC):** This is an access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.
- **Role-based access control (RBAC):** This is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions e.g., executive level, engineer level 1, etc. rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks.
- **Rule-based access control:** This is a security model in which the system administrator defines the rules that govern access to resource objects. Often, these rules are based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and RBAC to enforce access policies and procedures.
- **Attribute-based access control (ABAC):** This is a methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.

Implementing access control

Access control is a process that is integrated into an organization's IT environment. It can involve identity management and access management systems. These systems provide access control software, a user database, and management tools for access control policies, auditing and enforcement.

When a user is added to an access management system, system administrators use an automated provisioning system to set up permissions based on access control frameworks, job responsibilities and workflows.

The best practice of least privilege restricts access to only resources that employees require to perform their immediate job functions.

Challenges of access control

Many of the challenges of access control stem from the highly distributed nature of modern IT. It is difficult to keep track of constantly evolving assets as they are spread out both physically and logically. Some specific examples include the following:

- dynamically managing distributed IT environments;
- password fatigue;
- compliance visibility through consistent reporting;
- centralizing user directories and avoiding application-specific silos; and
- data governance and visibility through consistent reporting.

Rahul Publications

1.3.3 Audit

Q24. What is a Cybersecurity Audit? Explain about it.

Ans : **(Imp)**

A cybersecurity audit involves a comprehensive analysis and review of the IT infrastructure of your business. It detects vulnerabilities and threats, displaying weak links, and high-risk practices. It is a primary method for examining compliance. It is designed to evaluate something (a company, system, product, etc.) against a specific standard to validate that the exact needs are met.

Cybesecurity is not just about technical resilience or IT security; it is about Information and Data security. Misguided assurances from the internal team or a cybersecurity company and a false sense of security are the major reasons why hackers are succeeding in their attempts. They target your processes, people, procedures, and weakest links.

The Scope of a Cybersecurity Audit

Cybersecurity audits ensure a 360-degree in-depth audit of your organization's security postures. It detects vulnerabilities, risks, and threats that organizations face and the influence of such risks causing across these areas.

- **Data Security:** involves a review of network access control, encryption use, data security at rest, and transmissions
- **Operational Security:** involves a review of security policies, procedures, and controls
- **Network Security:** a review of network & security controls, SOC, anti-virus configurations, security monitoring capabilities, etc.
- **System Security:** This review covers hardening processes, patching processes, privileged account management, role-based access, etc.
- **Physical Security:** a review that covers disk encryption, role-based access controls, biometric data, multifactor authentication, etc.

Beyond these, a Cybersecurity audit can also cover cybersecurity risk management, cyber risk governance, training & awareness, legal, regulatory & contractual requirements, technical security controls, business continuity & incident management, and third-party management.

How Cybersecurity Audit will be helpful for your Business?

A cybersecurity audit offers the highest level of assurance for your cyber risk management process in place. It adds a line of sight to evaluate as well as enhance your security management. Significant benefits of IT security audits are:

- Highlight and address weak spots
- Delivers in-depth analysis of internal and external security practices
- Identify gaps in your defense
- Determines whether you must enhance your security posture or not
- Recommends how to leverage technology in business security
- Testing controls
- Staying ahead of cybercriminals
- Reputational value
- Assurance to employees, clients, and vendors
- Increased technology and security performance

1.3.4 Authentication

Q25. What is authentication? Explain various types of authentication systems.

Ans :

Authentication is the process of verifying the identity of user or information. User authentication is the process of verifying the identity of user when that user logs into a computer system.

There are different types of authentication systems which are:

1. Single-Factor authentication

This was the first method of security that was developed. On this authentication system, the user has to enter the username and the password to

Rahul Publications

confirm whether that user is logging in or not. Now if the username or password is wrong, then the user will not be allowed to log in or access the system.

Advantage

- It is a very simple to use and straightfor-ward system.
- it is not at all costly.
- The user does not need any huge technical skills.

Disadvantage

- It is not at all password secure. It will depend on the strength of the password entered by the user.
- The protection level in Single-Factor Authentication is much low.

2. Two-factor Authentication

n this authentication system, the user has to give a username, password, and other information. There are various types of authentication systems that are used by the user for securing the system. Some of them are: wireless tokens, virtual tokens, otp and more.

Advantage

- The Two-Factor Authentication System provides better security than the Single-factor Authentication system.
- The productivity and flexibility increase in the two-factor authentication system.
- The Two-Factor Authentication prevents the loss of trust.

Disadvantages

- It is time-consuming.

3. Multi-Factor authentication system

In this type of authentication, more than one factor of authentication is needed. This gives better security to the user. Any type of keylogger or phishing attack will not be possible in a Multi-Factor Authentication system. This assures the user, that the information will not get stolen from them.

Advantage

- No risk of security.
- No information could get stolen.
- No risk of any key-logger activity.
- No risk of any data getting captured.

Disadvantages

- It is time-consuming.
- it can rely on third parties.

The main objective of authentication is to allow authorized users to access the computer and to deny access to the unauthorized users. Operating Systems generally identifies/authenticates users using following 3 ways : Passwords, Physical identification, and Biometrics. These are explained as following below.

1. Passwords

Passwords verification is the most popular and commonly used authentication technique. A password is a secret text that is supposed to be known only to a user. In password based system, each user is assigned a valid username and password by the system administrator.

System stores all username and Passwords. When a user logs in, its user name and password is verified by comparing it with stored login name and password. If the contents are same then the user is allowed to access the system otherwise it is rejected.

2. Physical Identification

This technique include machine readable badges(symbols), card or smart cards. In some companies, badges are required for employees to gain access to the organization's gate. In many system, identification is combined with the use of password i.e the user must insert the card and then supply his /her password. This kind of authentication is commonly used with ATM. Smart card can enhance this scheme by keeping the user password within the card itself. This allow the authentication without storage of password in the computer system. The loss of such card can be dangerous.

Rahul Publications

3. Biometrics

This method of authentication is based on the unique biological characteristics of each user such as finger prints, voice or face recognition, signatures and eyes.

Biometric

- A scanner or other devices to gather the necessary data about user.
- Software to convert the data into a form that can be compared and stored.
- A database that stores information for all authorized users.

Characteristics

- **Facial Characteristics**

  Humans are differentiated on the basis of facial characteristics such as eyes, nose, lips, eyebrows and chin shape.

- **Fingerprints**

  Fingerprints are believed to he unique across the entire human population.

- **Hand Geometry**

  Hand geometry systems identify features of hand that includes shape, length and width of fingers.

- **Retinal pattern**

  It is concerned with the detailed structure of the eye.

- **Signature**

  Every individual has a unique style of handwriting, and this feature is reflected in the signatures of a person.

- **Voice**

  This method records the frequency pattern of the voice of an individual speaker.

One Time passwords :

One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password are implemented in various ways. Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

1.3.5 Biometrics

Q26. What is Biometrics in Cybersecurity? How do Biometric Security Systems Work?

Ans :

Biometric security is a type of security that uses the verification of people's behavioral and physical characteristics to identify them. It is the most accurate and strongest physical security technique currently in use for identity verification.

Biometric authentication indicates that each individual can be accurately identified based on his or her intrinsic behavioral or physical characteristics.

Security systems mostly use biometrics in environments where physical security is crucial and theft is a concern.

These biometric security systems store and use physical characteristics that remain constant over time such as hand patterns, facial recognition, retinal patterns, and fingerprints.

The system stores these characteristics as "templates."

If someone tries to get access to the biometric security system, the system scans them, analyzes their characteristics, and compares them to previously saved records. The person is then granted access to the facility or device if a match is found.

Because of the lower cost, fingerprint sensors have become the most widely used biometric security system. But, iris recognition systems are mostly used in high-security environments for the best accuracy.

Biometric authentication is becoming more popular in public and corporate security systems, as well as point-of-sale applications and consumer electronics.

Biometric verification provides both convenience and security, as there are no security tokens to carry or passwords to remember.

Rahul Publications

Some biometric technologies, such as gait analysis, can work without requiring physical contact with the individual being authenticated.

Biometrics scanners are hardware elements that collect physical characteristics for authentication and identity verification.

The following are components of biometric devices:

- A scanning device or reader to capture the biometric factor to be authenticated.
- A database for storing and comparing biometric data in a secure manner.
- And software that converts scanned biometric data into a digital format and compares observed and recorded data match points.

The system saves a person's biometric data when it is collected and matched, so it can be matched with subsequent access attempts.

Biometric data is usually encrypted before being saved on a remote server or device.

Scanned biometric data are compared to the saved database, and access is restricted or granted depending on whether a match is detected.

Q27. What are the types of Biometrics? Explain.

Ans :

Behavioral characteristics and physical characteristics are the two main types of biometrics used for security.

1. Physical biometrics

Physical biometrics analyze your hand shape, eye structures, facial features, and other physical characteristics. Physical biometrics include the following:

- DNA Matching
- Finger or Palm Veins Recognition
- Hand Geometry
- Iris Recognition
- Retina Scanning
- Skull Shape
- Fingerprints
- Facial Geometry

2. Finger or Palm Veins Recognition

In vein recognition, a person's finger's (or hand's) unique pattern of blood veins is used to identify them. It maps the veins beneath the skin of your fingerprints or hands using infrared light.

3. Iris/Retina Recognition

The unique pattern of someone's retina or iris is used to identify them in iris or retina recognition.

Because an iris scan requires minimum light pollution, a camera that can see IR, an infrared light source, to ensure accuracy, this method of biometric verification is more difficult to implement.

4. Face Recognition

A person's unique facial anatomy is used by face recognition systems to identify them. It can be used in many areas, including law enforcement, credit card payments, smartphones, and even fried chicken purchases in China.

5. Fingerprint Recognition

Fingerprint authentication verifies a person's identity by using their unique fingerprint.

It's one of the most widely utilized biometric verification methods, with applications ranging from mobile phones to vehicles to even buildings.

6. Behavioral biometrics

Behavioral biometrics, on the other hand, evaluates individuals' unique ways of acting or any pattern of behavior that is linked to a certain person.

Behavioral biometrics include the following:

- Walking Gait
- Keystroke Dynamics
- Finger and Mouse Movements
- Signature
- Typing Patterns
- Speaker Recognition
- Walking Gait Recognition

Rahul Publications

Gait recognition uses a person's walking style to identify them. Because everyone walks a little differently, observing how they place one foot in front of the other is a good approach to confirm their identification.

7. Speaker Recognition

To verify someone, voice recognition (or voice biometry for cybersecurity purposes) uses the unique frequencies, pitch, and tone of their voice.

This is now most widely used to validate users when they call a call center for customer service assistance such as online banking.

Instead of a single one-time authentication check, some of these behavioral biometrics offer continuous authentication.

- **Applications of biometrics:** Let's take a closer look at the organizations and fields where biometrics are currently being used to enhance security.
- **Home Security:** Biometric security systems are used to verify an individual who wants to enter a home.

  They also grant access to particular rooms, entire houses, and office buildings. So, keys are no longer needed and you can grant access to buildings with the swipe of a fingerprint.
- **Airport Security:** Biometrics are commonly used for airport security. Many airports use iris recognition to verify the identity of an individual.
- **Money Security:** One of the financial applications of biometrics is biometric payment security. This technology is used to authorize transaction processes and fingerprint scans are widely used for this.
- **Healthcare:** Biometric security is also used in the health care sector for health insurance programs and identity cards. Fingerprints are the most common type of biometrics used in the healthcare field for identification.
- **Security of Mobile Devices:** Biometric authentication has been integrated into Android and iOS smartphones over the last decade and now you can experience fingerprint scanning in any modern smartphone.

  The good news is device biometrics has now progressed beyond mere fingerprints. For example, Intelligent Scan is a Samsung-developed biometric security function. It provides biometric multi-factor authentication by combining facial recognition with an iris scan.

  Take, for another example, Apple's Face ID, which projects over 30,000 infrared dots onto a user's face, analyzes the pattern, and creates a "facial map." Later login attempts are then authenticated using that map.
- **Law Enforcement:** Criminal identification systems also use biometric security. For example, palm print or fingerprint authentication are widely used in criminal IDs.
- **Banking:** In the banking sector, many customers have grown tired of having to prove their identification regularly, yet without it, the risk of identity theft will continue to increase.

So, bank biometric security systems are in high demand. Biometrics such as fingerprint scanning, facial recognition, and voice verification are used by many banks in their mobile apps.

Some banks also utilize a combination of biometrics.

That means when multi-factor authentication is combined with biometrics, a nearly impenetrable layer of protection is created.

1.3.6 Cryptography

Q28. What is cryptography? Write about it.

Ans :

Cryptography is technique of securing information and communications through use of

Rahul Publications

codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Features

1. Confidentiality

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

2. Integrity

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

3. Non-repudiation:

The creator/sender of information cannot deny his or her intention to send information at later stage.

4. Authentication:

The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types

In general there are three types Of cryptography:

1. Symmetric Key Cryptography

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

2. Hash Functions

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3. Asymmetric Key Cryptography

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

1.3.7 Deception

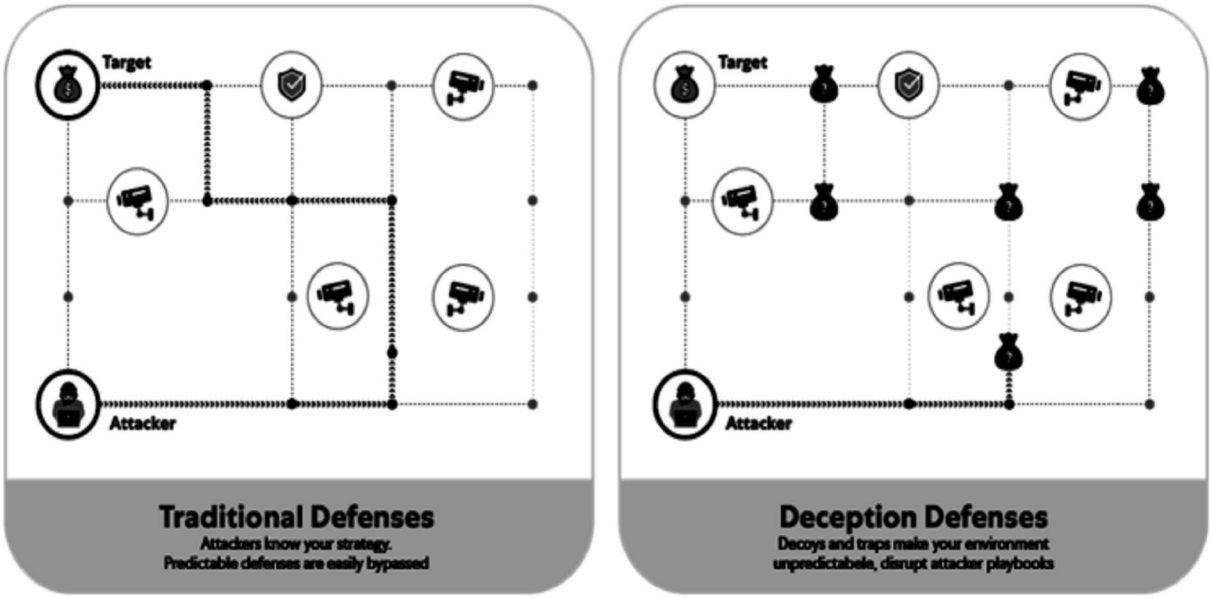
Q29. What is deception technology? Explain about it.

Ans : **(Imp.)**

Deception technology is a category of simple, effective cybersecurity defenses that detect threats early with low false positives and minimal network performance impact. The technology creates realistic decoy assets (e.g., domains, databases, active directories, servers, applications, files, credentials, breadcrumbs, sessions) to be deployed in your network alongside real assets to act as lures for cybercriminals. Attackers who breach your network have no way to differentiate the fake from the real, and the moment they interact with a decoy, a silent alarm is raised—your systems begin collecting information on the attacker's actions and intent, and then use that intel to generate high-fidelity alerts that decrease dwell time and speed up incident response.

No matter how good your perimeter defenses are, there is always a chance cybercriminals will infiltrate your network. Deception technology will make them waste their time exploring worthless planted assets while you bait them into a trap. Once they reveal their presence, you get an early indicator of their behavior and can gain intelligence to use against them.

Rahul Publications



Modern-day deception technology defenses borrow heavily from military deception principles employed by the likes of Chanakya, Sun Tzu, Napoleon, and Genghis Khan to conquer continents through deceit, camouflage, and subterfuge. In the context of cybersecurity, defenders use decoys and lures to mislead attackers into believing they have a foothold in the network and revealing themselves.

Benefits of deception technology

Overall, the biggest benefit of deception is that it puts the burden of success on the attacker instead of the defender. Once you've populated your network with decoys, adversaries need to carry out a flawless attack, without falling for a single fake asset, misdirect, or trap, to succeed. You win if they make any mistakes.

Let's look at five concrete benefits of deception that make this possible.

1. Improved threat detection

If you place detection classes on a scale of accuracy, there are two extremes:

- **Signature-based detection**, which is highly accurate but very threat-specific
- **Behavior analysis/heuristics**, which have broad threat coverage, but are prone to false positives

Deception alerts are the best of both worlds: highly accurate with broad threat coverage.

2. Business risk awareness

Most security controls don't account for current business risks—your antivirus doesn't know you're going through a merger. Deception, however, can be intrinsically aligned with them. For example, if you're launching a new product, you can create deception measures around that launch, aligning security controls tightly to areas where you perceive risk.

Rahul Publication

3. Greater coverage

Deception can be applied broadly across your organization, including in environments that are often blind spots. Deception can detect threats at the perimeter, on endpoints, in the network, in Active Directory, and throughout application layers, as well as cover often neglected environments like SCADA/ICS, IoT, and the cloud.

Unlike point solutions, deception also covers the entire kill chain, from pre-attack reconnaissance to exploitation, privilege escalation, lateral movement, and data loss.

4. Extremely low false positives

False positives can leave any security team exhausted. Deception inherently produces very few—nobody but an attacker should have any reason to interact with a decoy. Beyond that, the alerts provide context around an attacker's intent.

Most behavior analysis uses machine learning to flag anomalies from a baseline, which tends to create false positives. Deception establishes a zero-activity baseline (so any activity at all warrants investigation) and gives detailed indicators of compromise.

5. Orchestrated response

Orchestrated/Automated response is most useful when the trigger event is 100% certain. Even then, such alerts don't usually need orchestration because the products that generate them already handle remediation (e.g., antivirus quarantine).

Deception alerts are highly certain and contextual, so you can orchestrate more complex scenarios (e.g., decoy credentials redirect to a decoy environment and are blocked in the real environment) or target specific applications (e.g., an account accessing a decoy SWIFT banking server gets blocked in the real SWIFT server).

Rahul Publications

1.3.8 Denial of Service Filters

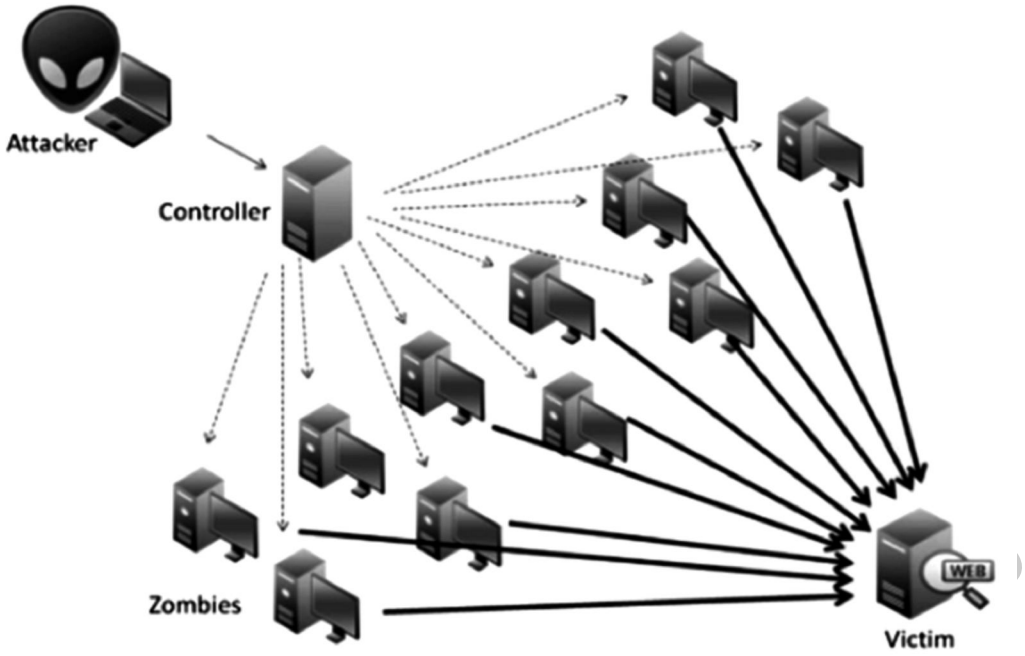
Q30. Explain about denial of service attacks and its types.

Ans :

Denial of service attack (DOS) is an attack against computer or network which reduces, restricts or prevents accessibility of its system resources to authorized users.

Distributed Denial of Service (DDoS) attack is an attack where multiple compromised systems simultaneously attack a single system; thereby, causing a DOS attack for the users of the target.

An attacker can select the Zombies randomly or topologically and once compromised, he sets up a command and controller to control the zombies that attack the target. A bot is a malicious software installed on compromised machines, this gives the attacker control over the zombies. The network of Bots is called botnet.

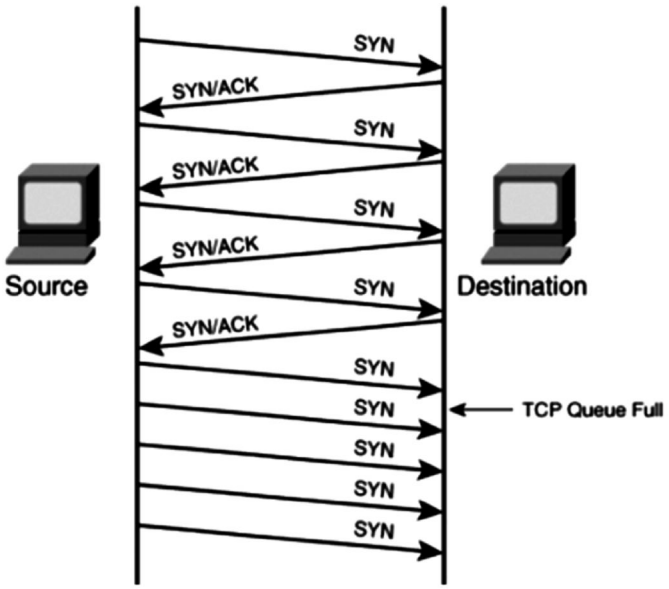


1. Volumetric attacks

This is an Attack where the entire bandwidth of a network is consumed so the authorized clients will not be able to get the resources. This is achieved BY flooding the network devices like hubs or switches with numerous ICMP echo request/reply packets so the entire bandwidth is consumed, and no other clients are able to connect with the target network.

2. Syn flooding

Is another attack where an attacker compromises multiple zombies and simultaneously floods the target with multiple SYN packets. The target will be overwhelmed by the SYN requests, either it goes down or its performance is reduced drastically.



Rahul Publications

3. Fragmentation attacks

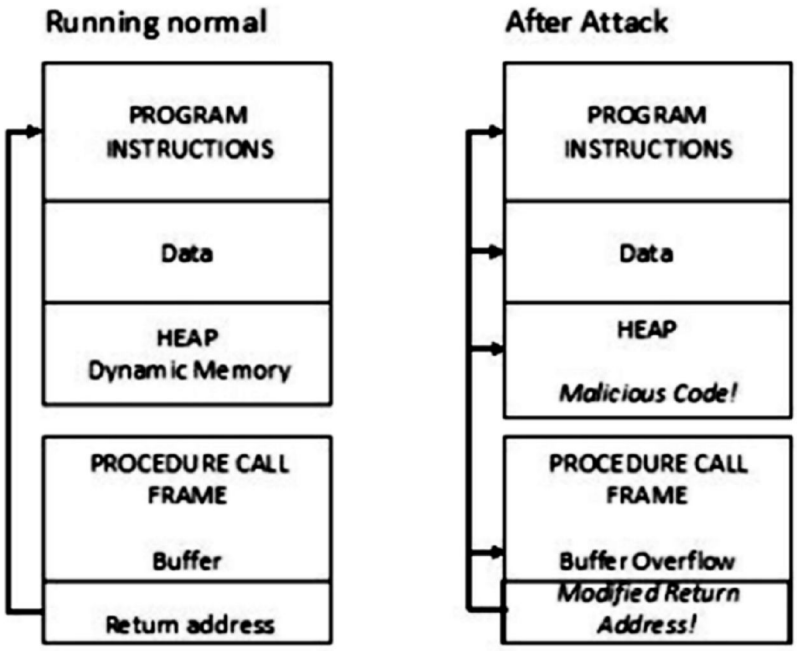
This is an attack that fights against the reassembling ability of the target. Numerous fragmented packets are sent to the target, making it difficult for the target to reassemble them; thereby, denying access to the valid clients.

4. TCP-State exhaustion attack:

The attacker sets up and tears down TCP connections and overwhelms the stable tables; thereby, causing a DOS attack.

5. Application Layer Attacks:

The attacker takes advantage of the programming errors in the application to cause the denial of service attack. It is achieved by sending numerous application requests to the target to exhaust the target's resources so it will not be able to service any valid clients. A programming error in the case of buffer overflow attack- if the memory allocated to a variable is smaller than the requested, then it may lead to memory leakage or crashing the entire application.



Attacker plants code that overflows buffer and corrupts the return address. Instead of returning to the appropriate calling procedure, the modified return address returns control to malicious code, located elsewhere in process memory.

E.g., Buffer overflow attack, Account lockout, Request flooding, etc.

6. Plashing

This is done by causing a permanent damage to the system hardware by sending fraudulent updates to the hardware thereby making them completely unusable. The only solution is to re-install the hardware.

7. Counter Measures

- Use up-to-date anti-virus and IDS tools.
- Perform network analysis to find out the possibility of DOS attack.
- Shut down unnecessary services in the target network.

- Find and neutralize handlers. Protect secondary victims.
- Perform proper activity profiling and ingress/ egress filtering to filter out unwanted traffic.
- Enforce in-depth packet Analysis.
- Use Defense-in–depth approach.
- Add additional load balancers to absorb traffic and set up a throttle logic to control traffic.
- Correct program errors.
- Use Strong encryption mechanisms.

1.3.9 Ethical Hacking

Q31. What is Ethical Hacking? Explain the phases of ethical hacking.

Ans :

Meaning

Ethical hacking is a part of cyber security and can be defined as the process of testing the system against all possible security breaches and solving any vulnerabilities in the system before any malicious attack even happens. Hacking is illegal but ethical hacking is the authorized practice of bypassing system security to identify any potential data threat. Ethical hackers try to examine the systems to pinpoint the weak points in that system that malicious hackers can exploit.

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization. They use this process to prevent cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points. An ethical hacker follows the steps and thought process of a malicious attacker to gain authorized access and test the organization's strategies and network.

Phases

The five phases of ethical hacking are:

1. Reconnaissance

First in the ethical hacking methodology steps is reconnaissance, also known as the footprint or information gathering phase. The goal of this preparatory phase is to collect as much information as possible. Before launching an attack, the attacker collects all the necessary information about the target. The data is likely to contain passwords, essential details of employees, etc. An attacker can collect the information by using tools such as HTTPTrack to download an entire website to gather information about an individual or using search engines such as Maltego to research about an individual through various links, job profile, news, etc.

Reconnaissance is an essential phase of ethical hacking. It helps identify which attacks can be launched and how likely the organization's systems fall vulnerable to those attacks.

Footprinting collects data from areas such as:

- TCP and UDP services
- Vulnerabilities
- Through specific IP addresses
- Host of a network

In ethical hacking, footprinting is of two types:

- **Active**: This footprinting method involves gathering information from the target directly using Nmap tools to scan the target's network.
- **Passive**: The second footprinting method is collecting information without directly accessing the target in any way. Attackers or ethical hackers can collect the report through social media accounts, public websites, etc.

2. Scanning

The second step in the hacking methodology is scanning, where attackers try to find different ways to gain the target's information. The attacker looks for information such as user accounts, credentials, IP addresses, etc. This step of ethical hacking involves finding easy and quick ways to access the network and skim for information. Tools such as dialers, port scanners, network mappers, sweepers, and vulnerability scanners are used in the scanning phase to scan data and records. In ethical hacking methodology, four different types of scanning practices are used, they are as follows:

Rahul Publications

(i) **Vulnerability Scanning**: This scanning practice targets the vulnerabilities and weak points of a target and tries various ways to exploit those weaknesses. It is conducted using automated tools such as Netsparker, OpenVAS, Nmap, etc.

(ii) **Port Scanning**: This involves using port scanners, dialers, and other data-gathering tools or software to listen to open TCP and UDP ports, running services, live systems on the target host. Penetration testers or attackers use this scanning to find open doors to access an organization's systems.

(iii) **Network Scanning**: This practice is used to detect active devices on a network and find ways to exploit a network. It could be an organizational network where all employee systems are connected to a single network. Ethical hackers use network scanning to strengthen a company's network by identifying vulnerabilities and open doors.

3. Gaining Access

The next step in hacking is where an attacker uses all means to get unauthorized access to the target's systems, applications, or networks. An attacker can use various tools and methods to gain access and enter a system. This hacking phase attempts to get into the system and exploit the system by downloading malicious software or application, stealing sensitive information, getting unauthorized access, asking for ransom, etc. Metasploit is one of the most common tools used to gain access, and social engineering is a widely used attack to exploit a target.

Ethical hackers and penetration testers can secure potential entry points, ensure all systems and applications are password-protected, and secure the network infrastructure using a firewall. They can send fake social engineering emails to the employees and identify which employee is likely to fall victim to cyberattacks.

4. Maintaining Access

Once the attacker manages to access the target's system, they try their best to maintain that access. In this stage, the hacker continuously exploits the system, launches DDoS attacks, uses the hijacked system as a launching pad, or steals the entire database. A backdoor and Trojan are tools used to exploit a vulnerable system and steal credentials, essential records, and more. In this phase, the attacker aims to maintain their unauthorized access until they complete their malicious activities without the user finding out.

Ethical hackers or penetration testers can utilize this phase by scanning the entire organization's infrastructure to get hold of malicious activities and find their root cause to avoid the systems from being exploited.

5. Clearing Track

The last phase of ethical hacking requires hackers to clear their track as no attacker wants to get caught. This step ensures that the attackers leave no clues or evidence behind that could be traced back. It is crucial as ethical hackers need to maintain their connection in the system without getting identified by incident response or the forensics team. It includes editing, corrupting, or deleting logs or registry values. The attacker also deletes or uninstalls folders, applications, and software or ensures that the changed files are traced back to their original value.

1.3.10 Firewalls

Q32. What is a Firewall? Explain about it.

Ans :

A cybersecurity firewall is a network security system which can either be a hardware or software that protects the trusted network from unauthorized access from external networks and external threats.

- It uses the mechanism of filtering of data by using a defined set of policies rules, that help restrict access to the applications and systems
- It acts like a gatekeeper and monitors and

Rahul Publications

control incoming and outgoing network traffic

- Any specific traffic, in the form of requests for access, requests for data, to a resource behind the firewall and inside the trusted network, will be inspected, analyzed and is allowed to pass or blocked based on pre-defined security rules
- The security rules are configured into the firewall and are customizable

Various Implementations of Firewalls

- They are hardware firewalls, ranging from entry levels, mid-range to high end depending on
- A load of simultaneous hits on the entity we are protecting
- The expected user base
- There are software-based firewalls
- Some implementations work with a combination of software and a hardware firewall
- Large organizations install high end dedicated hardware firewalls
- Small app vendors and Individuals can setup basic software firewalls on their personal devices

Expectations of a Firewall Implementation

Implementing a firewall does the following things:

- Ensure that all traffic from the external world onto the system or application is mandatorily routed through the firewall
- The rules defined ensure isolation and detection of all possibilities of unauthorized incoming traffic
- Denial of unauthorized traffic
- Passing of all authorized traffic
- Learning and improvisation of rules
- Identification of a right fit firewall for the expected load is imperative to ensure performance is not impacted

Advantages and Disadvantages of Firewall

- Advantage is an outcome of the effectiveness of the implementation of rules and controls on the firewall. The firewall is effective when it can handle all possible external threats.
- A disadvantage is that firewalls cannot prevent internal threats, virus attacks and authentic mechanisms used by hackers (like username password).

Organizations have to implement other mechanisms and controls to circumvent these threats. Threats like, intrusion detection systems and intrusion prevention systems. Attacks from the internet of virus, trojans, spyware, ransomware, denial of service, malware, can be foiled by implementing an antivirus and other prevention and detection systems alongside firewalls.

Types of Firewalls

- Any access that happens to the application inside a trusted network is broken down to multiple packets. To recognize the authenticity of a packet there are packet filtering firewalls. These are very popular and are used to block packets from a specific source or another network. Hence, when the network is attacked by unknown packets, the firewall recognizes it as a threat and raises an alarm and blocks it.
- A firewall can work to mask or hide the internet address of the trusted private trusted network from the external public network hence unwarranted access cannot happen.
- Application-level gateways or proxy-based firewalls are becoming the need of the hour.
- Today the dependencies and advent of cloud-based applications have diverted focus to control applications access. Hence one may want to block complete application services (like FTP, telnet, Http).
- Eg. FTP access allows a user to copy files from one network to another. By blocking FTP service it is unavailable to a malicious user who tries to connect to this network and to copy content.

Rahul Publications

There are multiple solutions to detect and prevent malicious behavior and attacks. Because there are many ways to avoid attacks a need is felt to find integrated solutions for firewalls, antivirus, anti-spam, and intrusion detection and intrusion prevention. Such solutions will be the next-generation innovation in the field of Cyber Security.

1.3.11 Intrusion Detection Systems

Q33. Explain about Intrusion Detection Systems.

Ans :

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat.

Classification of Intrusion Detection Systems

Intrusion detection systems are designed to be deployed in different environments. And like many cybersecurity solutions, an IDS can either be host-based or network-based.

- **Host-Based IDS (HIDS):** A host-based IDS is deployed on a particular endpoint and designed to protect it against internal and external threats. Such an IDS may have the ability to monitor network traffic to and from the machine, observe running processes, and inspect the system's logs. A host-based IDS's visibility is limited to its host machine, decreasing the available context for decision-making, but has deep visibility into the host computer's internals.
- **Network-Based IDS (NIDS):** A network-based IDS solution is designed to monitor an entire protected network. It has visibility into all traffic flowing through the network and makes determinations based upon packet metadata and contents. This wider viewpoint provides more context and the ability to detect widespread threats; however, these systems lack visibility into the internals of the endpoints that they protect.

Due to the different levels of visibility, deploying a HIDS or NIDS in isolation provides incomplete protection to an organization's system. A unified threat management solution, which integrates multiple technologies in one system, can provide more comprehensive security.

Detection Method of IDS Deployment

Beyond their deployment location, IDS solutions also differ in how they identify potential intrusions:

- **Signature Detection:** Signature-based IDS solutions use fingerprints of known threats to identify them. Once malware or other malicious content has been identified, a signature is generated and added to the list used by the IDS solution to test incoming content. This enables an IDS to achieve a high threat detection rate with no false positives because all alerts are generated based upon detection of known-malicious content. However, a signature-based IDS is limited to detecting known threats and is blind to zero-day vulnerabilities.
- **Anomaly Detection:** Anomaly-based IDS solutions build a model of the "normal" behavior of the protected system. All future behavior is compared to this model, and any anomalies are labeled as potential threats and generate alerts. While this approach can detect novel or zero-day threats, the difficulty of building an accurate model of "normal" behavior means that these systems must balance false positives (incorrect alerts) with false negatives (missed detections).
- **Hybrid Detection:** A hybrid IDS uses both signature-based and anomaly-based detection. This enables it to detect more potential attacks with a lower error rate than using either system in isolation.

1.3.12 Response

Q34. What is incident response in cyber security? Explain

Ans :

Incident response is a term used to describe the process by which an organization handles a data

Rahul Publications

breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the "incident"). Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

Organizations should, at minimum, have a clear incident response plan in place. This plan should define what constitutes an incident for the company and provide a clear, guided process to be followed when an incident occurs.

There are six steps to incident response. These six steps occur in a cycle each time an incident occurs. The steps are:

Incident Response Plan – Six Steps

1. Preparation

Developing policies and procedures to follow in the event of a cyber breach. This will include determining the exact composition of the response team and the triggers to alert internal partners. Key to this process is effective training to respond to a breach and documentation to record actions taken for later review.

2. Identification

This is the process of detecting a breach and enabling a quick, focused response. IT security teams identify breaches using various threat intelligence streams, intrusion detection systems, and firewalls. Some people don't understand what threat intelligence is but it's critical to protecting your company. Threat intelligence professionals analyze current cyber threat trends, common tactics used by specific groups, and keep your company one step ahead.

3. Containment

One of the first steps after identification is to contain the damage and prevent further penetration. This can be accomplished by taking specific sub-networks offline and relying on system backups to maintain operations. Your company will likely remain in a state of emergency until the breach is contained.

4. Eradication

This stage involves neutralizing the threat and restoring internal systems to as close to their previous state as possible. This can involve secondary monitoring to ensure that affected systems are no longer vulnerable to subsequent attack.

5. Recovery

Security teams need to validate that all affected systems are no longer compromised and can be returned to working condition. This also requires setting timelines to fully restore operations and continued monitoring for any abnormal network activity. At this stage, it becomes possible to calculate the cost of the breach and subsequent damage.

6. Lessons Learned

One of the most important and often overlooked stages. During this stage, the incident response team and partners meet to determine how to improve future efforts. This can involve evaluating current policies and procedures, as well specific decisions the team made during the incident. Final analysis should be condensed into a report and used for future training. Forcepoint can help your team analyze previous incidents and help improve your response procedures. Protecting your organization requires a determined effort to constantly learn and harden your network against malicious actors.

1.3.13 Scanning

Q35. What is scanning in cyber security? Explain the types of scanning.

Ans :

Scanning is another essential step, which is necessary, and it refers to the package of techniques and procedures used to identify hosts, ports, and various services within a network. Network scanning is one of the components of intelligence gathering and information retrieving mechanism an attacker used to create an overview scenario of the target organization (target organization: means the group of people or organization which falls in the prey of

Rahul Publications

the Hacker). Vulnerability scanning is performed by pen-testers to detect the possibility of network security attacks. This technique led hackers to identify vulnerabilities such as missing patches, unnecessary services, weak authentication, or weak encryption algorithms. So a pen-tester and ethical hacker list down all such vulnerabilities found in an organization's network.

Scanning is of three types:

- Network Scanning
- Port Scanning
- Vulnerability Scanning

Objectives of Network Scanning

1. To discover live hosts/computer, IP address, and open ports of the victim.
2. To discover services that are running on a host computer.
3. To discover the Operating System and system architecture of the target.
4. To discover and deal with vulnerabilities in Live hosts.

Scanning Methodologies

1. Hackers and Pen-testers check for Live systems.
2. Check for open ports (The technique is called Port Scanning, which will be discussed below)
3. Scanning beyond IDS (Intrusion Detection System)
4. Banner Grabbing: is the method for obtaining information regarding the targeted system on a network and services running on its open ports. Telnet and ID Serve are the tools used mainly to perform a Banner-grabbing attack. This information may be used by intruders/ hackers to portray the lists of applicable exploits.
5. Scan for vulnerability
6. Prepare Proxies

Port Scanning

It is a conventional technique used by penetration testers and hackers to search for open doors from which hackers can access any organization's system. During this scan, hackers need to find out those live hosts, firewalls installed, operating systems used, different devices attached to the system, and the targeted organization's topology. Once the Hacker fetches the victim organization's IP address by scanning TCP and UDP ports, the Hacker maps this organization's network under his/her grab. Amap is a tool to perform port scanning.

TCP/IP Handshake

Before moving to the scanning techniques, we have to understand the 3-way TCP/IP handshaking process. In computer terms, handshaking means the automated process used to set dynamic parameters of a communication channel between two entities using some protocols. Here, TCP (Transmission Control Protocol) and IP (Internet Protocol) are the two protocols used for handshaking between a client and a server. Here first, the client sends a synchronization packet for establishing a connection, and the server listens to and responds with a syn/ack packet to the client. The client again responds to the server by sending an ack packet. Here SYN denotes synchronization, which is used to initialize connections between the client and the server in packets. ACK denotes acknowledgment, which is used to establish a connection between two hosts.

Scanning techniques mainly used:

1. **SYNScan**: SYN scan or stealth doesn't complete the TCP three-way handshake technique. A hacker sends an SYN packet to the victim, and if an SYN/ACK frame is received back, then the target would complete the connection, and the port is in a position to listen. If an RST is retrieved from the target, it is assumed that the port is closed or not activated. SYN stealth scan is advantageous because a few IDS systems log this as an attack or connection attempt.
2. **XMASScan**: XMAS scan send a packet which contains URG (urgent), FIN (finish) and PSH (push) flags. If there is an open port, there will be no response; but the target responds with an RST/ACK packet if the port is closed. (RST = reset).

Rahul Publications

3. **FINScan:** A FIN scan is similar to an XMAS scan except that it sends a packet with just the FIN (finish) flag and no URG or PSH flags. FIN scan receives the same response and has the same limitations as XMAS scans.
4. **IDLEScan:** An IDLE scan uses a spoofed/ hoax IP to send the SYN packet to the target by determining the port scan response and IP header sequence number. Depending on the response of the scan, the port is determined, whether open or closed.
5. **Inverse TCP Flag Scan:** Here, the attacker sends TCP probe packets with a TCP flag (FIN, URG PSH) or no flags. If there is no response, it indicates that the port is open, and RST means it is closed.
6. **ACK Flag Probe Scan:** Here, the attacker sends TCP probe packets where an ACK flag is set to a remote device, analyzing the header information (TTL and WINDOW field). The RST packet signifies whether the port is open or closed. This scan is also used to check the target's/victim's filtering system.

Vulnerability Scanning

It is the proactive identification of the system's vulnerabilities within a network in an automated manner to determine whether the system can be exploited or threatened. I this case, the computer should have to be connected to the internet.

1.3.14 Security policy

Q36. Explain about the need of security policy in cyber security.

Ans :

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information. It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when they will occur. A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Need of Security policies

1. It increases efficiency

The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

2. It upholds discipline and accountability

When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law. The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

3. It can make or break a business deal

It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place

4. It helps to educate employees on security literacy

A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization sensitive data. It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.

Rahul Publications

We use security policies to manage our network security. Most types of security policies are automatically created during the installation. We can also customize policies to suit our specific environment. There are some important cybersecurity policies recommendations describe below-

1. Virus and Spyware Protection policy

This policy provides the following protection:

- It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
- It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.
- It helps to detect the applications that exhibit suspicious behaviour by using SONAR heuristics and reputation data.

2. Firewall Policy

This policy provides the following protection:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals.
- It removes the unwanted sources of network traffic.

3. Intrusion Prevention policy

This policy automatically detects and blocks the network attacks and browser attacks. It also protects applications from vulnerabilities. It checks the contents of one or more data packages and detects malware which is coming through legal ways.

4. LiveUpdate policy

This policy can be categorized into two types one is LiveUpdate Content policy, and another is LiveUpdate Setting Policy. The LiveUpdate policy contains the setting which determines when and how client computers download the content updates from LiveUpdate. We can define the computer that clients contact to check for updates and schedule when and how often clients computer check for updates.

5. Application and Device Control

This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system. The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

6. Exceptions policy

This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.

7. Host Integrity policy

This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. We use this policy to ensure that the client's computers who access our network are protected and compliant with companies? securities policies. This policy requires that the client system must have installed antivirus.

1.3.15 Threat Management

Q37. Explain about threat management.

Ans :

Threat management is an exercise of using a combination of the detection system, like intrusion detection system (IDS), event management (SIEM) and security information system, etc. The security tool is to proactively monitor and counter-threat to the business network.

The unified risk management is a specified system that collects all of threat management tools into one single solution. The UTM allows you to deal only with a single technology dealer for all the threat management needs. The UTM minimize the complexity of your business network security, also help management efforts and time.

Benefits

- 24/7 cyber risk services and monitoring to ensure better incident reporting and deal with advanced cyber incidents and cyber-attacks.
- Adds huge value to the cyber security defense solution and provides you access to trained experts to help you out in detection and

Rahul Publications

monitoring of threats, retaining an internal team and removes the hiring difficulty.

- Provides your cyber security threat management to ensure the safety and protects you from cyber-attacks.
- Expert analysis by the expert SOC team to make sure that all alarms are trigged, while the endpoint event and deep dive network packets analysis completed, escalating genuine and false positive threats. The alerts are not reliant solely on traditional signature detections we utilize the technical threat intelligence to make detailed illegal insights.
- We always carry analyst-led threats hunting, iteratively and proactively searching through the datasets and networks to identify threats that could evade technologies.
- Our authentic services monitor various organizations and sectors, which allow us to collect relevant intelligence data and later on apply to exact sector intelligence.
- Our proactive platform allows you to see the analysts sees, access to incident and cases, packet data, sensor alert, management, and endpoint alerts information in the real time.

Common Attacks Detected

- Data Breaches
- Botnet communication traffic
- Ransomware
- Success instruction attempts
- Drive-by downloads
- Suspicious traffic patterns
- Malware distribution
- Malware distribution
- Remote access tools
- Clouds storage policy violations

Best practices for cyber threat management

Some experts believe that the key to effective cyber threat management is technology. Tools such as automation and AI and help organizations counter sophisticated cyber attacks and give security teams insights into the threat landscape.

However, technology is only one part of the equation. Organizations must look at the ways they can use people and processes to address the full threat lifecycle – from identifying threats to responding to breaches.

1. Insight

Organizations must have a complete understanding of their sensitive assets and resources. This is where a data flow map can help; it enables organizations to identify and visualise the ways that information moves through their systems.

The data flow map is often a valuable tool when conducting a risk assessment, as it provides further insight into the way an organization could be compromised.

2. Detection

Threat detection ensures that the organization is promptly alerted to suspicious activity.

There are a variety of threat detection tools that organizations can use. Additionally, security teams should log suspicious activity and investigate signs of a data breach.

3. Response

When a security incident occurs, organizations must act quickly. They can do this by implementing an incident response plan that includes a framework for threat analysis, mitigation and continual improvement.

4. Recovery

Finally, organizations must consider recovery activities that ensure the organization can continue functioning during disruption. This includes cyber resilience and business continuity planning.

Rahul Publications

Short Question and Answers

1. What is cyber security?

Ans

Meaning

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

- The term cyber security refers to techniques and practices designed to protect digital data.
- The data that is stored, transmitted or used on an information system.
- Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.

It is made up of two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.

2. What is internet governance?

Ans

Meaning

Internet governance is 'the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet'.

3. Cyber Warfare.

Ans

Meaning

Cyber Warfare is typically defined as a set of actions by a nation or organization to attack countries or institutions' computer network systems with the intention of disrupting, damaging, or destroying infrastructure by computer viruses or denial-of-service attacks.

Cyber warfare can take many forms, but all of them involve either the destabilization or destruction of critical systems. The objective is to weaken the target country by compromising its core systems.

This means cyber warfare may take several different shapes:

1. Attacks on financial infrastructure
2. Attacks on public infrastructure like dams or electrical systems
3. Attacks on safety infrastructure like traffic signals or early warning systems
4. Attacks against military resources or organizations

4. Cyber crime.

Ans

Cyber crime or computer-oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of a crime or it may be the target.

Cyber crime is the use of a computer as a weapon for committing crimes such as committing fraud, identities theft or breaching privacy. Cyber crime, especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment and government. Cyber crime may endanger a person or a nation's security and financial health.

5. What is cyber terrorism?

Ans

Cyber terrorism is often defined as any premeditated, politically motivated attack against information systems, programs and data that threatens violence or results in violence. The definition is sometimes expanded to include any cyber attack that intimidates or generates fear in the target population. Attackers often do this by damaging or disrupting critical infrastructure.

6. Cyber Espionage.

Ans

Cyber espionage, or cyber spying, is a type of cyber attack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

Rahul Publications

Cyber espionage is primarily used as a means to gather sensitive or classified data, trade secrets or other forms of IP that can be used by the aggressor to create a competitive advantage or sold for financial gain. In some cases, the breach is simply intended to cause reputational harm to the victim by exposing private information or questionable business practices.

Cyber espionage attacks can be motivated by monetary gain; they may also be deployed in conjunction with military operations or as an act of cyber terrorism or cyber warfare. The impact of cyber espionage, particularly when it is part of a broader military or political campaign, can lead to disruption of public services and infrastructure, as well as loss of life.

7. What is Vulnerability in Cyber Security?

Ans

A vulnerability in cyber security refers to any weakness in an information system, system processes, or internal controls of an organization. These vulnerabilities are targets for lurking cybercrimes and open to exploitation through the points of vulnerability.

These hackers are able to gain illegal access to the systems and data and cause severe damage. Therefore, cybersecurity vulnerabilities are extremely important to monitor for the overall security posture as gaps in a network can result in a full-scale breach of systems in an organization.

Examples of Vulnerabilities

- A weakness in a firewall that can lead to malicious hackers getting into a computer network
- Lack of security cameras
- Unlocked doors at businesses

All of these are weaknesses that can be used by others to hurt a business or its assets.

8. System administration.

Ans

System administration is the field of work in which someone manages one or more systems, be they software, hardware, servers or workstations. Its goal is ensuring the systems are running efficiently and effectively.

System administration is typically done by information technology experts for or within an organization. Their job is to ensure that all related computer systems and services keep working .

A system administrator, or sysadmin, is a person responsible to maintain and operate a computer system or network for a company or other organization. System administrators are often members of an information technology department.

9. What are cyber security safe guards?

Ans

Cybersecurity safeguards are the fundamental part of a cybersecurity investment. They are the expected outcomes of a cybersecurity investment and must be understood sufficiently so that they can be analyzed and evaluated within a systematic decision making process.

A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

The protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

10. What is access control?

Ans

Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources. Secure access control uses policies that verify users are who they claim to be and ensures appropriate control access levels are granted to users.

Implementing access control is a crucial component of web application security, ensuring only the right users have the right level of access to the right resources. The process is critical to helping organizations avoid data breaches and fighting attack vectors, such as a buffer overflow attack, KRACK attack, on-path attack, or phishing attack.

11. What is a Cybersecurity Audit?

Ans

A cybersecurity audit involves a comprehensive analysis and review of the IT infrastructure of your business. It detects vulnerabilities and threats, displaying weak links, and high-risk practices. It is a primary method for examining compliance. It is designed to evaluate something (a company, system, product, etc.) against a specific standard to validate that the exact needs are met.

Rahul Publications

Cybesecurity is not just about technical resilience or IT security; it is about Information and Data security. Misguided assurances from the internal team or a cybersecurity company and a false sense of security are the major reasons why hackers are succeeding in their attempts. They target your processes, people, procedures, and weakest links.

12. What is authentication?

Ans :

Authentication is the process of verifying the identity of user or information. User authentication is the process of verifying the identity of user when that user logs into a computer system.

13. What is Biometrics in Cybersecurity?

Ans :

Biometric security is a type of security that uses the verification of people's behavioral and physical characteristics to identify them. It is the most accurate and strongest physical security technique currently in use for identity verification.

Biometric authentication indicates that each individual can be accurately identified based on his or her intrinsic behavioral or physical characteristics.

Security systems mostly use biometrics in environments where physical security is crucial and theft is a concern.

These biometric security systems store and use physical characteristics that remain constant over time such as hand patterns, facial recognition, retinal patterns, and fingerprints.

14. What is cryptography?

Ans :

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

15. Ethical Hacking.

Ans :

Meaning

Ethical hacking is a part of cyber security and can be defined as the process of testing the system against all possible security breaches and solving any vulnerabilities in the system before any malicious attack even happens. Hacking is illegal but ethical hacking is the authorized practice of bypassing system security to identify any potential data threat. Ethical hackers try to examine the systems to pinpoint the weak points in that system that malicious hackers can exploit.

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization. They use this process to prevent cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points. An ethical hacker follows the steps and thought process of a malicious attacker to gain authorized access and test the organization's strategies and network.

16. Scanning

Ans :

Scanning is another essential step, which is necessary, and it refers to the package of techniques and procedures used to identify hosts, ports, and various services within a network. Network scanning is one of the components of intelligence gathering and information retrieving mechanism an attacker used to create an overview scenario of the target organization (target organization: means the group of people or organization which falls in the prey of the Hacker). Vulnerability scanning is performed by pen-testers to detect the possibility of network security attacks. This technique led hackers to identify vulnerabilities such as missing patches, unnecessary services, weak authentication, or weak encryption algorithms. So a pen-tester and ethical hacker list down all such vulnerabilities found in an organization's network.

Rahul Publications

Choose the Correct Answers

1. Which one of the following can be considered as the class of computer threats? [a]

   (a) Dos Attack (b) Phishing

   (c) Soliciting (d) Both A and C

2. Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else? [b]

   (a) Malware (b) Spyware

   (c) Adware (d) All of the above

3. Which of the following malware types does not clone or replicate itself through infection? [c]

   (a) Viruses (b) Worms

   (c) Trojans (d) Rootkits

4. Which of these is a sort of independent type of malicious program that would not require any host program? [c]

   (a) Virus (b) Trap Door

   (c) Worm (d) Trojan Horse

5. _____ are the special type of programs used for recording and tracking user's keystroke. [a]

   (a) Keylogger (b) Trojans

   (c) Virus (d) Worms

6. _____ is a violent act done using the Internet, which either threatens any technology user or leads to loss of life or otherwise harms anyone in order to accomplish political gain. [c]

   (a) Cyber-warfare (b) Cyber campaign

   (c) Cyber-terrorism (d) Cyber attack

7. Which of them does not comes under scanning methodologies? [b]

   (a) Vulnerability scanning (b) Sweeping

   (c) Port Scanning (d) Google Dorks

8. _____ is a weakness that can be exploited by attackers. [c]

   (a) System with Virus (b) System without firewall

   (c) System with vulnerabilities (d) System with a strong password

9. In a phishing, attackers target the _____ technology to so social engineering. [a]

   (a) Emails (b) WI-FI network

   (c) Operating systems (d) Surveillance camera

10. Which of the following is not a type of virus? [d]

    (a) Boot sector (b) Polymorphic

    (c) Multipartite (d) Trojans

Rahul Publications

Fill in the blanks

1. _____ is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
2. Cybercriminals send malicious emails that seem to come from legitimate resources is called _____.
3. _____ refers to spying on another country to steal secrets.
4. A computer _____ is a malicious code which self-replicates by copying itself to other programs.
5. _____ are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.
6. _____ describes any scenario in which the strength of the authentication mechanism is relatively weak compared to the value of the assets being protected.
7. _____ is a data security process that enables organizations to manage who is authorized to access corporate data and resources
8. _____ detects vulnerabilities and threats, displaying weak links, and high-risk practices.
9. _____ authentication indicates that each individual can be accurately identified based on his or her intrinsic behavioral or physical characteristics.
10. _____ attack is an attack where multiple compromised systems simultaneously attack a single system.

Rahul Publications

ANSWERS

1. Cyber security
2. phishing
3. Espionage
4. virus
5. Security Policies.
6. Weak Authentication
7. Access control
8. cyber security audit
9. Biometric
10. Distributed Denial of Service (DDoS)

UNIT II

Securing Web Application, Services and Servers:

Introduction, Basic security for HTTP Applications and Services, Basic Security for SOAP Services, Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges.

2.1 Securing Web Application, Services and Servers

2.1.1 Introduction

Q1. What are the various issues in securing web applications?

Ans : **(Imp.)**

Security is critical to web services. However, neither XML-RPC nor SOAP specifications make any explicit security or authentication requirements.

There are three specific security issues with web services "

1. Confidentiality
2. Authentication
3. Network Security

1. Confidentiality

If a client sends an XML request to a server, can we ensure that the communication remains confidential?

Answer lies here -

- XML-RPC and SOAP run primarily on top of HTTP.
- HTTP has support for Secure Sockets Layer (SSL).
- Communication can be encrypted via SSL.
- SSL is a proven technology and widely deployed.

A single web service may consist of a chain of applications. For example, one large service might tie together the services of three other applications. In this case, SSL is not adequate; the messages need to be encrypted at each node along the service path, and each node represents a potential weak link in the chain. Currently, there is no agreed-upon solution to this issue, but one promising solution is the W3C XML Encryption Standard. This standard provides a framework for encrypting and decrypting entire XML documents or just portions of an XML document.

2. Authentication

If a client connects to a web service, how do we identify the user? Is the user authorized to use the service?

The following options can be considered but there is no clear consensus on a strong authentication scheme.

- HTTP includes built-in support for Basic and Digest authentication, and services can therefore be protected in much the same manner as HTML documents are currently protected.
- SOAP Digital Signature (SOAP-DSIG) leverages public key cryptography to digitally sign SOAP messages. It enables the client or server to validate the identity of the other party. Check it at www.w3.org/TR/SOAP-dsig.
- The Organization for the Advancement of Structured Information Standards (OASIS) is working on the Security Assertion Markup Language (SAML).

Rahul Publications

3. Network Security

There is currently no easy answer to this problem, and it has been the subject of much debate. For now, if you are truly intent on filtering out SOAP or XML-RPC messages, one possibility is to filter out all HTTP POST requests that set their content type to text/xml.

Another alternative is to filter the SOAPAction HTTP header attribute. Firewall vendors are also currently developing tools explicitly designed to filter web service traffic.

2.2 Basic security for HTTP Applications and Services

Q2. Explain about the security protocols in HTTPS.

Ans : **(Imp.)**

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communi-cation over a computer network, and is widely used on the Internet. The principal motivations for HTTPS are authentication of the accessed website, and protection of the privacy and integrity of the exchanged data while in transit. It protects against man-in-the-middle attacks, and the bidirectional encryption of communications between a client and server protects the communications against eavesdropping and tampering. he security of HTTPS is that of the underlying TLS, which typically uses long-term public and private keys to generate a short-term session key, which is then used to encrypt the data flow between the client and the server. X.509 certificates are used to authenticate the server.

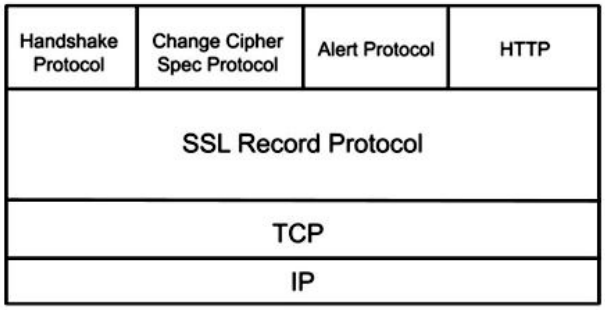
Secure Socket Layer (SSL)

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

1. SSL record protocol
2. Handshake protocol
3. Change-cipher spec protocol
4. Alert protocol

SSL Protocol Stack



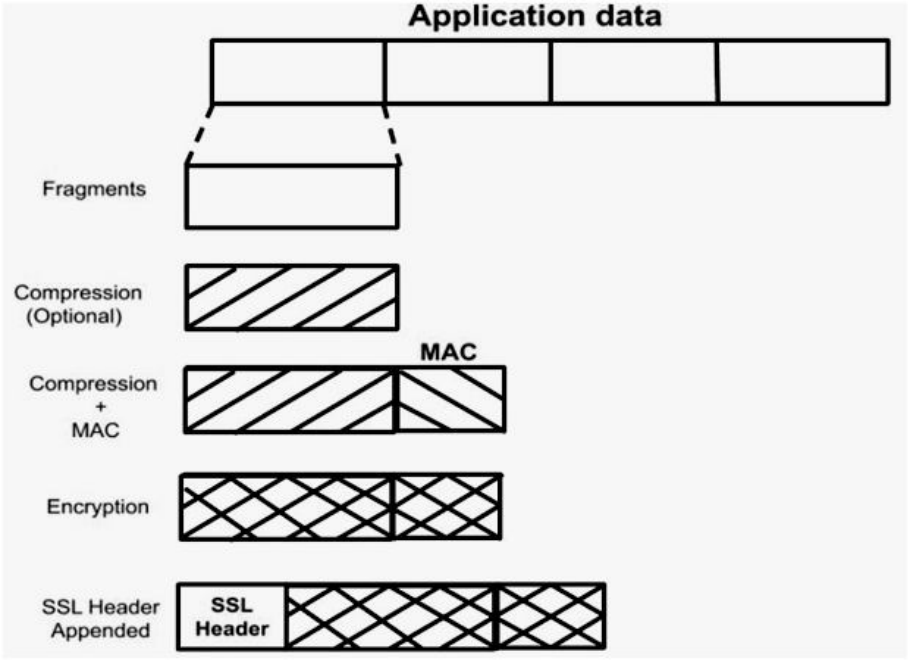
Rahul Publications

1. SSL Record Protocol

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



2. Handshake Protocol

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2:** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3:** In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- **Phase-4:** In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.

3. Change-cipher Protocol

This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After handshake protocol, the Pending state is converted into the current state.

Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copied into the current state.

1 byte

4. Alert Protocol

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.

Level (1 byte)	Alert (1 byte)

The level is further classified into two parts:

Warning (level = 1)

This Alert has no impact on the connection between sender and receiver. Some of them are:

(i) **Bad certificate:** When the received certificate is corrupt.

(ii) **No certificate:** When an appropriate certificate is not available.

(iii) **Certificate expired:** When a certificate has expired.

(iv) **Certificate unknown:** When some other unspecified issue arose in processing the certificate, rendering it unacceptable.

(v) **Close notify**: It notifies that the sender will no longer send any messages in the connection.

Fatal Error (level = 2)

This Alert breaks the connection between sender and receiver. Some of them are :

(i) **Handshake failure:** When the sender is unable to negotiate an acceptable set of security parameters given the options available.

(ii) **Decompression failure:** When the decompression function receives improper input.

(iii) **Illegal parameters:** When a field is out of range or inconsistent with other fields.

(iv) **Bad record MAC:** When an incorrect MAC was received.

(v) **Unexpected message:** When an inappro-priate message is received.

The second byte in the Alert protocol describes the error.

Silent Features of Secure Socket Layer

- The advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is a two-layered protocol.

Transport Layer Security (TLS)

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Socket Layer (SSL). TLS ensures that no third party may eavesdrop or tampers with any message.

There are several benefits of TLS:

- **Encryption**

  TLS/SSL can help to secure transmitted data using encryption.

- **Interoperability**

  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.

- **Algorithm flexibility**

  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.

- **Ease of Deployment**

  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.

- **Ease of Use**

  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

Rahul Publications

Working of TLS

The client connect to server (using TCP), the client will be something. The client sends number of specification:

1. Version of SSL/TLS.
2. Which cipher suites, compression method it wants to use.

The server checks what the highest SSL/TLS version is that is supported by them both, picks a cipher suite from one of the clients option (if it supports one) and optionally picks a compression method. After this the basic setup is done, the server provides its certificate. This certificate must be trusted either by the client itself or a party that the client trusts. Having verified the certificate and being certain this server really is who he claims to be (and not a man in the middle), a key is exchanged. This can be a public key, "PreMasterSecret" or simply nothing depending upon cipher suite.

Both the server and client can now compute the key for symmetric encryption. The handshake is finished and the two hosts can communicate securely. To close a connection by finishing. TCP connection both sides will know the connection was improperly terminated. The connection cannot be compromised by this through, merely interrupted.

2.3 Basic Security for SOAP Services

Q3. What is SOAP? Explain about SOAP protocol structure.

Ans : **(Imp.)**

SOAP is an XML-based protocol for accessing web services over HTTP. It has some specification which could be used across all applications.

SOAP is known as the Simple Object Access Protocol, but in later times was just shortened to SOAP v1.2. SOAP is a protocol or in other words is a definition of how web services talk to each other or talk to client applications that invoke them.

SOAP was developed as an intermediate language so that applications built on various programming languages could talk easily to each other and avoid the extreme development effort.

One of the methods used to combat this complexity is to use XML (Extensible Markup Language) as the intermediate language for exchanging data between applications.

Every programming language can understand the XML markup language. Hence, XML was used as the underlying medium for data exchange.

But there are no standard specifications on use of XML across all programming languages for data exchange. That is where SOAP software comes in.

SOAP was designed to work with XML over HTTP and have some sort of specification which could be used across all applications. We will look into further details on the SOAP protocol in the subsequent chapters.

Reasons of SOAP

SOAP is the protocol used for data interchange between applications. Below are some of the reasons as to why SOAP is used.

- When developing SOAP based Web services, you need to have some of language which can be used for web services to talk with client applications. SOAP is the perfect medium which was developed in order to achieve this purpose. This protocol is also recommended by the W3C consortium which is the governing body for all web standards.
- SOAP is a light-weight protocol that is used for data interchange between applications. Note the keyword 'light.' Since SOAP programming is based on the XML language, which itself is a light weight data interchange language, hence SOAP as a protocol that also falls in the same category.
- SOAP is designed to be platform independent and is also designed to be operating system independent. So the SOAP protocol can work any programming language based applications on both Windows and Linux platform.

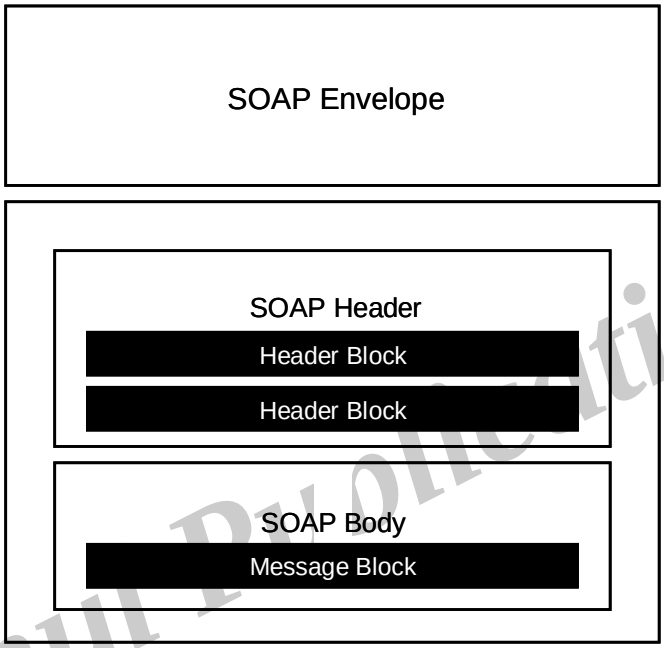
Rahul Publications

- It works on the HTTP protocol –SOAP works on the HTTP protocol, which is the default protocol used by all web applications. Hence, there is no sort of customization which is required to run the web services built on the SOAP protocol to work on the World Wide Web.

SOAP Building Blocks

The SOAP specification defines something known as a "**SOAP message**" which is what is sent to the web service and the client application.

The below diagram of SOAP architecture shows the various building blocks of a SOAP Message.



Rahul Publications

SOAP Message Building Blocks

The SOAP message is nothing but a mere XML document which has the below components.

- An Envelope element that identifies the XML document as a SOAP message – This is the containing part of the SOAP message and is used to encapsulate all the details in the SOAP message. This is the root element in the SOAP message.
- A Header element that contains header information – The header element can contain information such as authentication credentials which can be used by the calling application. It can also contain the definition of complex types which could be used in the SOAP message. By default, the SOAP message can contain parameters which could be of simple types such as strings and numbers, but can also be a complex object type.

A simple SOAP service example of a complex type is shown below.

Suppose we wanted to send a structured data type which had a combination of a "Tutorial Name" and a "Tutorial Description," then we would define the complex type as shown below.

The complex type is defined by the element tag <xsd:complexType>. All of the required elements of the structure along with their respective data types are then defined in the complex type collection.

```
<xsd:complexType>
<xsd:sequence>
    <xsd:element name="Tutorial Name" type="string"/>
    <xsd:element name="Tutorial Description"  type="string"/>
</xsd:sequence>
</xsd:complexType>
```

- A Body element that contains call and response information – This element is what contains the actual data which needs to be sent between the web service and the calling application. Below is an SOAP web service example of the SOAP body which actually works on the complex type defined in the header section. Here is the response of the Tutorial Name and Tutorial Description that is sent to the calling application which calls this web service.

```
<soap:Body>
<GetTutorialInfo>
        <TutorialName>Web Services</TutorialName>
        <TutorialDescription>All about web services</TutorialDescription>
</GetTutorialInfo>
</soap:Body>
```

SOAP Message Structure

One thing to note is that SOAP messages are normally auto-generated by the web service when it is called.

Whenever a client application calls a method in the web service, the web service will automatically generate a SOAP message which will have the necessary details of the data which will be sent from the web service to the client application.

As discussed in the previous topic of this SOAP tutorial, a simple SOAP Message has the following elements –

- The Envelope element
- The header element and
- The body element
- The Fault element (Optional)

Let's look at an example below of a simple SOAP message and see what element actually does.

1. As seen from the above SOAP message, the first part of the SOAP message is the envelope element which is used to encapsulate the entire SOAP message.
2. The next element is the SOAP body which contains the details of the actual message.
3. Our message contains a web service which has the name of "Guru99WebService".
4. The "Guru99Webservice" accepts a parameter of the type 'int' and has the name of TutorialID.

Now, the above SOAP message will be passed between the web service and the client application.

You can see how useful the above information is to the client application. The SOAP message tells the client application what is the name of the Web service, and also what parameters it expects and also what is the type of each parameter which is taken by the web service.

Rahul Publications

SOAP Envelope Element

The first bit of the building block is the SOAP Envelope.

The SOAP Envelope is used to encapsulate all of the necessary details of the SOAP messages, which are exchanged between the web service and the client application.

The SOAP envelope element is used to indicate the beginning and end of a SOAP message. This enables the client application which calls the web service to know when the SOAP message ends.

The following points can be noted on the SOAP envelope element.

- Every SOAP message needs to have a root Envelope element. It is absolutely mandatory for SOAP message to have an envelope element.
- Every Envelope element needs to have at least one soap body element.
- If an Envelope element contains a header element, it must contain no more than one, and it must appear as the first child of the Envelope, before the body element.
- The envelope changes when SOAP versions change.
- A v1.1-compliant SOAP processor generates a fault upon receiving a message containing the v1.2 envelope namespace.
- A v1.2-compliant SOAP processor generates a Version Mismatch fault if it receives a message that does not include the v1.2 envelope namespace.

The Fault Message

When a request is made to a SOAP web service, the response returned can be of either 2 forms which are a successful response or an error response. When a success is generated, the response from the server will always be a SOAP message. But if SOAP faults are generated, they are returned as "HTTP 500" errors.

The SOAP Fault message consists of the following elements.

1. **<faultCode>**– This is the code that designates the code of the error. The fault code can be either of any below values
   (i) SOAP-ENV:VersionMismatch – This is when an invalid namespace for the SOAP Envelope element is encountered.
   (ii) SOAP-ENV:MustUnderstand – An immediate child element of the Header element, with the mustUnderstand attribute set to "1", was not understood.
   (iii) SOAP-ENV:Client – The message was incorrectly formed or contained incorrect information.
   (iv) SOAP-ENV:Server – There was a problem with the server, so the message could not proceed.
2. **<faultString>** – This is the text message which gives a detailed description of the error.
3. **<faultActor> (Optional)**– This is a text string which indicates who caused the fault.
4. **<detail>(Optional)** – This is the element for application-specific error messages. So the application could have a specific error message for different business logic scenarios.

OAP Communication Model

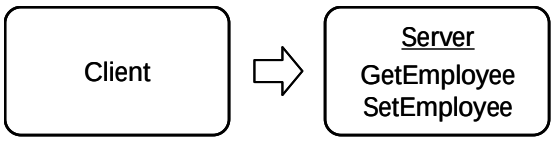
All communication by SOAP is done via the HTTP protocol. Prior to SOAP, a lot of web services used the standard RPC (Remote Procedure Call) style for communication. This was the simplest type of communication, but it had a lot of limitations.

Now in this SOAP API tutorial, let's consider the below diagram to see how this communication works. In this example, let's assume the server hosts a web service which provided 2 methods as

- **GetEmployee** – This would get all Employee details
- **SetEmployee** – This would set the value of the details like employees dept, salary, etc. accordingly.

In the normal RPC style communication, the client would just call the methods in its request and send the required parameters to the server, and the server would then send the desired response.

Rahul Publications



The above communication model has the below serious limitations

1. Not Language Independent

The server hosting the methods would be in a particular programming language and normally the calls to the server would be in that programming language only.

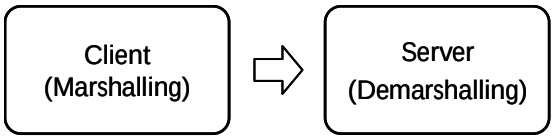
2. Not the standard protocol

When a call is made to the remote procedure, the call is not carried out via the standard protocol. This was an issue since mostly all communication over the web had to be done via the HTTP protocol.

3. Firewalls

Since RPC calls do not go via the normal protocol, separate ports need to be open on the server to allow the client to communicate with the server. Normally all firewalls would block this sort of traffic, and a lot of configuration was generally required to ensure that this sort of communication between the client and the server would work.

To overcome all of the limitations cited above, SOAP would then use the below communication model.



1. The client would format the information regarding the procedure call and any arguments into a SOAP message and sends it to the server as part of an HTTP request. This process of encapsulating the data into a SOAP message was known as Marshalling.
2. The server would then unwrap the message sent by the client, see what the client requested for and then send the appropriate response back to the client as a SOAP message. The practice of unwrapping a request sent by the client is known as Demarshalling.

2.4 IDENTITY MANAGEMENT AND WEB SERVICES

Q4. Explain about Identity Management web service.

Ans :

Web Services technology is a collection of standards and protocols designed to

- reduce the amount of work it takes to accomplish integration (and thereby reduce cost and schedule), and
- provide flexible interfaces between systems that won't "break" when one system or the other is updated or revised.

IT departments are already using the Web services approach to integration because it has many advantages over previous approaches, and now physical security systems are beginning to use Web services to connect to other systems as well.

This is creating an interesting circular relationship between Web services and identity management systems. As companies integrate more business applications using Web services, they find that establishing identity management is a critical prerequisite. And if they decide to implement a fully integrated, central identity management system, they find that Web services is the best way to integrate it with their various business applications and systems.

Need

The implementation of an enterprise-wide identity management system is of great interest to corporate security for several reasons.

- An IDMS will close IT security gaps related to enrolling and terminating employees.
- The deployment of an IDMS is typically accompanied by a role-based access control (RBAC) scheme for the information systems.

Rahul Publications

Once roles are jointly defined by human resources and business managers, and once IT security privileges are assigned to the roles, security privileges can be automatically granted upon enrollment in the IDMS. Privileges are also automatically changed when an employee's position changes, and revoked automatically upon the employee's termination.

- Physical security can leverage the defined corporate roles by defining access control privileges to match, aligning physical security more tightly with the organization's job roles. This doesn't require the access control system to be integrated to any other system.
- Physical security can leverage the HR enrollment of employees by integrating the physical access control system (PACS) with the IDMS, so that access control privileges are managed automatically along with IT privileges as HR enrolls, re-assigns and terminates employees.

Using an IDMS as a common point of reference, physical and IT access control can be synchronized. And using role-based access control to establish privileges based upon job functions, both physical and IT access control can be policy-driven.

Even if no identity management system is used and the physical and IT access control systems are not integrated with each other, RBAC can be used in both physical and IT systems to provide a policy-driven access control approach that aligns with the organization. Maintaining this scheme requires more human attention than with integrated systems. On the other hand, it does strengthen security while making it very manageable and auditable.

2.5 Authorization Patterns

Q5. What is authorization process? Explain about various patterns of authorization process.

Ans :

- Authorization is a process by which a server determines if the client has permission to use a resource or access a file.
- Authorization is usually coupled with authentication so that the server has some concept of who the client is that is requesting access.
- The type of authentication required for authorization may vary; passwords may be required in some cases but not in others.
- In some cases, there is no authorization; any user may be use a resource or access a file simply by asking for it. Most of the web pages on the Internet require no authentication or authorization.

Pattern 1: Keep the data where it is

Often the simplest solution is to keep the data where it is and have the services ask for the data that they need, when they need it. You might see this as the most obvious solution given the problem outlined above.

You split up your data model and logic such that the documents service controls which document-related permissions are granted by which role (admins can edit, members can read, etc), and then the users service exposes an API to grab a user's role on an organization. With this API in place, the permission check can happen like so:

This pattern begins to show cracks when the numbers of services or teams grows, when authorization logic gets more complex, or when facing more strict performance requirement

Pattern 2: A Request Gateway

One clean solution to the authorization data problem is to include a user's roles in any request to all services that might need to make a decision. If the documents service gets information about the user's role as a part of the request, it can make its own authorization decisions based on that.

In this pattern, a "gateway" sits between an API and its end-user. The gateway has access to user information and role information, which it can attach to the request before it passes it on to the API itself. When the API receives the request, it can use the role data from the request (i.e. in its headers) to check that the user's action is allowed.

Rahul Publications

It is common for the gateway to be responsible for both authentication AND authorization. For example, the gateway might use an Authorization header to authenticate a particular user, and then additionally fetch that user's role information. The gateway then proxies the request with user ID and role information to a downstream service (the documents service in the example above).

The main benefit of the gateway pattern is its architectural simplicity. It allows developers of downstream services (like the documents service) not to care about where roles data is coming from. The authorization data is always available on the request — a permission check can be performed immediately without any additional round-trips.

Pattern 3: Centralize all authorization data

Another solution is to put all authorization data and logic into one place, separate from all the services that need to enforce authorization. The most common way to implement this pattern is to build a dedicated "authorization service." Then, when your other services need to perform permissions checks, they turn around and ask the authorization service:

In this model, the documents service doesn't care about the user's role at all: it just needs to ask the authorization service whether the user can edit a document, or whether a user can view a document. The authorization service itself contains everything it needs (including role data) to make that decision.

This can be quite appealing: you now have one system in charge of authorization, which fits with the philosophy of microservices. Separating concerns in this way has some advantages: other developers on your team don't need to care how authorization works. Because it stands alone, any optimizations you make to your authorization service help speed up the rest of your overall system.

2.6 SECURITY CONSIDERATIONS

Q6. Explain various security considerations in web security.

Ans : **(Imp.)**

Web Security is very important nowadays. Websites are always prone to security threats/risks. Web Security deals with the security of data over the internet/network or web or while it is being transferred to the internet. For e.g. when you are transferring data between client and server and you have to protect that data that security of data is your web security.

Hacking of Website may result in theft of Important Customer Data the important customer data maybe your credit card information the login details of the customer or it can be the destruction of one's business and propagation of illegal content to the users so while somebody hacks your website they can either steal the information the important information of the customers or they can even propagate the illegal content to your users through your website so, therefore, security considerations are needed in the context of web security.

Security Threats

A Threat is nothing but a possible event that can damage and harm an information system. Security Threat is defined as a risk that which, can potentially harm Computer systems & organizations. Whenever an Individual or an Organization creates a website, they are vulnerable to security attacks.

Rahul Publications

Security attacks are mainly aimed at stealing altering or destroying a piece of personal and confidential information, stealing the hard drive space, illegally accessing passwords. So whenever the website you created is vulnerable to security attacks then the attacks are going to steal your data alter your data destroy your personal information see your confidential information and also it accessing your password.

Top Web Security Threats

Web security threats are constantly emerging and evolving, but many threats consistently appear at the top of the list of web security threats. These include:

- Cross-site scripting (XSS)
- SQL Injection
- Phishing
- Ransomware
- Code Injection
- Viruses and worms
- Spyware
- Denial of Service

- **Updated Software:** You need to always update your software. Hackers may be aware of vulnerabilities in certain software, which are sometimes caused by bugs and can be used to damage your computer system and steal personal data. Older versions of software can become a gateway for hackers to enter your network. Software makers soon become aware of these vulnerabilities and will fix vulnerable or exposed areas. That's why It is mandatory to keep your software updated, It plays an important role in keeping your personal data secure.
- **Beware of SQL Injection:** SQL Injection is an attempt to manipulate your data or your database by inserting a rough code into your query. For e.g. somebody can send a query to your website and this query can be a rough code while it gets executed it can be used to manipulate your database such as change tables, modify or delete data or it can retrieve important information also so, one should be aware of the SQL injection attack.
- **Cross-Site Scripting (XSS):** XSS allows the attackers to insert client-side script into web pages. E.g. Submission of forms. It is a term used to describe a class of attacks that allow an attacker to inject client-side scripts into other users' browsers through a website. As the injected code enters the browser from the site, the code is reliable and can do things like sending the user's site authorization cookie to the attacker.
- **Error Messages:** You need to be very careful about error messages which are generated to give the information to the users while users access the website and some error messages are generated due to one or another reason and you should be very careful while providing the information to the users. For e.g. login attempt – If the user fails to login the error message should not let the user know which field is incorrect: Username or Password.

Rahul Publications

- **Data Validation:** Data validation is the proper testing of any input supplied by the user or application. It prevents improperly created data from entering the information system. Validation of data should be performed on both server-side and client-side. If we perform data validation on both sides that will give us the authentication. Data validation should occur when data is received from an outside party, especially if the data is from untrusted sources.
- **Password:** Password provides the first line of defense against unauthorized access to your device and personal information. It is necessary to use a strong password. Hackers in many cases use sophisticated software that uses brute force to crack passwords. Passwords must be complex to protect against brute force. It is good to enforce password requirements such as a minimum of eight characters long must including uppercase letters, lowercase letters, special characters, and numerals

2.7 CHALLENGES FOR WEB SECURITY

Q7. Explain the challenges for web security.

Ans : **(Imp.)**

1. Large-scale Automated Attacks

Distributed Denial of Service (DDoS) attacks aren't a new threat, but they're bigger and worse than ever. In the old days, DDoS attacks came from a single IP address. Today, hackers deploy networks made of thousands of devices from many locations, making the attacks harder to stop with traditional methods alone, such as a web application firewall or IP blocking.

2. Bad Bots and Fraud

Thirty-nine percent of bad bots can fool traditional security tools by mimicking human behaviors, such as mouse movement and website navigation. These sophisticated bad bots infiltrate websites to steal passwords, hold inventory, make fraudulent purchases, and carry out other forms of damage. That said, only about 20 percent of bots are "bad". Bots generate about 50 percent of internet traffic, so it's important to choose a bot management solution that can identify good bots from bad.

3. Third-party JavaScript Vulnerabilities

Modern websites and apps use third-party scripts to power advanced capabilities, such as dynamic content, live chat, analytics, and retargeting display ads. It's not uncommon for an eCommerce site to load 50 different scripts — each one has the potential to be a door for attackers to walk through.

Third-party JavaScript is an attractive target for cybercriminals, such as Magecart, because these scripts sidestep your internal security protocols and infrastructure while allowing access to the same data as first-party code. In other words, a compromised third-party script can access the same data as your own code — including credit card details and personally identifiable information (PII). British Airways, NewEgg, and Ticketmaster are just a few of the thousands of businesses compromised using this attack vector during the past 12 months.

4. Web Application Attacks

Web application attacks like SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) can also exfiltrate sensitive consumer information. There are attack-specific solutions, including:

Rahul Publications

- Employing bot detection and mitigation capabilities to prevent bad bots from accessing your application data.
- Use a Web Application Firewall (WAF) to monitor your network and block potential attacks.
- Using prepared statements with parameterized queries to ensure the SQL code is defined before queries are passed. This allows the database to differentiate between SQL code and SQL data and prevents injection attempts.

Rahul Publications

Short Questions and Answers

1. Authentication.

Ans :

If a client connects to a web service, how do we identify the user? Is the user authorized to use the service?

The following options can be considered but there is no clear consensus on a strong authentication scheme.

- HTTP includes built-in support for Basic and Digest authentication, and services can therefore be protected in much the same manner as HTML documents are currently protected.
- SOAP Digital Signature (SOAP-DSIG) leverages public key cryptography to digitally sign SOAP messages. It enables the client or server to validate the identity of the other party. Check it at www.w3.org/TR/SOAP-dsig.

2. Hypertext Transfer Protocol Secure (HTTPS).

Ans :

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communi-cation over a computer network, and is widely used on the Internet. The principal motivations for HTTPS are authentication of the accessed website, and protection of the privacy and integrity of the exchanged data while in transit. It protects against man-in-the-middle attacks, and the bidirectional encryption of communications between a client and server protects the communications against eavesdropping and tampering. he security of HTTPS is that of the underlying TLS, which typically uses long-term public and private keys to generate a short-term session key, which is then used to encrypt the data flow between the client and the server. X.509 certificates are used to authenticate the server.

3. What is SOAP?

Ans :

SOAP is an XML-based protocol for accessing web services over HTTP. It has some specification which could be used across all applications.

SOAP is known as the Simple Object Access Protocol, but in later times was just shortened to SOAP v1.2. SOAP is a protocol or in other words is a definition of how web services talk to each other or talk to client applications that invoke them.

SOAP was developed as an intermediate language so that applications built on various programming languages could talk easily to each other and avoid the extreme development effort.

One of the methods used to combat this complexity is to use XML (Extensible Markup Language) as the intermediate language for exchanging data between applications.

Every programming language can understand the XML markup language. Hence, XML was used as the underlying medium for data exchange.

4. Reasons of SOAP.

Ans :

- When developing SOAP based Web services, you need to have some of language which can be used for web services to talk with client applications. SOAP is the perfect medium which was developed in order to achieve this purpose. This protocol is also recommended by the W3C consortium which is the governing body for all web standards.
- SOAP is a light-weight protocol that is used for data interchange between applications. Note the keyword 'light.' Since SOAP programming is based on the XML language, which itself is a light weight data interchange language, hence SOAP as a protocol that also falls in the same category.
- SOAP is designed to be platform independent and is also designed to be operating system independent. So the SOAP protocol can work any programming language based applications on both Windows and Linux platform.

5. OAP Communication Model.

Ans :

All communication by SOAP is done via the HTTP protocol. Prior to SOAP, a lot of web services used the standard RPC (Remote Procedure Call) style for communication. This was the simplest type of communication, but it had a lot of limitations.

Rahul Publications

Now in this SOAP API tutorial, let's consider the below diagram to see how this communication works. In this example, let's assume the server hosts a web service which provided 2 methods as

- **GetEmployee** – This would get all Employee details
- **SetEmployee** – This would set the value of the details like employees dept, salary, etc. accordingly.

In the normal RPC style communication, the client would just call the methods in its request and send the required parameters to the server, and the server would then send the desired response.

6. What is authorization process?

Ans :

- Authorization is a process by which a server determines if the client has permission to use a resource or access a file.
- Authorization is usually coupled with authentication so that the server has some concept of who the client is that is requesting access.
- The type of authentication required for authorization may vary; passwords may be required in some cases but not in others.
- In some cases, there is no authorization; any user may be use a resource or access a file simply by asking for it. Most of the web pages on the Internet require no authentication or authorization.

7. Security Threats.

Ans :

A Threat is nothing but a possible event that can damage and harm an information system. Security Threat is defined as a risk that which, can potentially harm Computer systems & organizations. Whenever an Individual or an Organization creates a website, they are vulnerable to security attacks.

Security attacks are mainly aimed at stealing altering or destroying a piece of personal and confidential information, stealing the hard drive space, illegally accessing passwords. So whenever the website you created is vulnerable to security attacks then the attacks are going to steal your data alter your data destroy your personal information see your confidential information and also it accessing your password.

Rahul Publications

Choose the Correct Answers

1. Which of the following is not a security issue in securing web applications. [c]
   (a) Confidentiality (b) Authentication
   (c) Ethical hacking (d) Network Security
2. The Full form of HTTPS [b]
   (a) Hypertext Transfer Protocol Service (b) Hypertext Transfer Protocol Secure
   (c) Hypertext Transfer Protocol Suite (d) Hypertext Transfer Protocol System
3. Which one of the following is not a higher –layer SSL protocol? [c]
   (a) Alert Protocol (b) Handshake Protocol
   (c) Alarm Protocol (d) Change Cipher Spec Protocol
4. Number of phases in the handshaking protocol? [c]
   (a) 2 (b) 3
   (c) 4 (d) 5
5. In the Handshake protocol action, which is the last step of the Phase 2 : Server Authentication and Key Exchange? [a]
   (a) server_done (b) server_key_exchange
   (c) certificate_request (d) crtificate_verify
6. Which protocol consists of only 1 bit? [d]
   (a) Alert Protocol (b) Handshake Protocol
   (c) Upper-Layer Protocol (d) Change Cipher Spec Protocol
7. SOAP is a format for sending messages and is also called as _____. [b]
   (a) Data Transfer protocol (b) Communication protocol
   (c) Network protocol (d) None of these
8. Which element is used to encapsulate all of the necessary details of the SOAP messages, which are exchanged between the web service and the client application. [a]
   (a) The Envelope element (b) The header element and
   (c) The body element (d) The Fault element
9. In the computer system Authentication is the fundamental building block in _____ [a]
   (a) Security context (b) Control context
   (c) Execution context (d) Performance context
10. In processes access control implements [d]
   (a) check Policy (b) control Policy
   (c) access Policy (d) Security Policy

Rahul Publications

Fill in the blanks

1. Full form of SSL _____.
2. _____. provides security to the data that is transferred between web browser and server
3. In the handshake protocol _____ message type first sent between client and server ?
4. This _____ allows the client and server to authenticate each other by sending a series of messages to each other
5. _____ protocol is used to convey SSL-related alerts to the peer entity
6. Full form of TLS _____.
7. _____ protocol ensures that no third party may eavesdrop or tampers with any message.
8. SOAP is an _____ protocol for accessing web services over HTTP
9. All communication by SOAP is done via the _____ protocol.
10. _____ is a collection of standards and protocols designed to reduce the amount of work it takes to accomplish integration.

ANSWERS

1. Secure Socket Layer
2. Secure Socket Layer
3. certificate_request
4. hand shake
5. alter
6. Transport layer security.
7. Transport layer security.
8. XML-based
9. HTTP
10. Web Services technology

Rahul Publications

UNIT III

Intrusion Detection And Prevention:

Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection,Intrusion detection and Prevention Techniques, Anti-Malware software, Network based Intrusiondetection Systems, Network based Intrusion Prevention Systems, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation.

3.1 Intrusion

Q1. What is Intrusion? Write about it briefly.

Ans :

An intrusion is any activity that is designed to compromise your data security. This can be through more menacing and pervasive formats like ransomware or unintentional data breaches by employees or others connected to your network.

An intrusion may include any of the following:

- Malware or ransomware
- Attempts to gain unauthorized access to a system
- DDOS attacks
- Cyber-enabled equipment destruction
- Accidental employee security breaches (like moving a secure file into a shared folder)
- Untrustworthy users both team members and those outside of your organization
- Social engineering attacks such as phishing campaigns and other ways of tricking users with seemingly legitimate communication

There are hundreds of ways that your MSP clients can experience data insecurity through an intrusion. There are much fewer methods for ensuring data safety with confidence and dependability. One trusted data security solution for MSPs is using an intrusion detection system.

3.2 Physical Theft

Q2. Explain what are Internal Data Security Threats and How to deal with them.

(OR)

Explain various ways of physical theft .

Ans : **(Imp.)**

When considering cyber security strategies for data protection, guarding against external threats is usually the first on the list. However, headline grabbing cyber attacks account for only half of the root causes of data breaches according to the 2019 Cost of a Data Breach Report released by the Ponemon Institute and IBM Security. The rest are due to internal threats and system glitches.

The human factor is often hardest to control and predict when it comes to data protection. While some companies invest in employee training in hopes that a well-educated work force, aware of the financial and reputational consequences of data breaches, will be enough to increase vigilance and deter poor security practices. However, the truth is, in many case, organizations are only one careless employee away from a damaging security incident. There is also always the potential danger of malicious insiders, disgruntled employees that want to damage a company's reputation or steal data on their way out of an organization.

1. Social Engineering

Although technically an external threat, social engineering only works if someone inside a company can be tricked into revealing

Rahul Publications

information. It implies that employees are manipulated into giving up passwords or other confidential information. Social engineering can take the form of attackers impersonating friends or other trusted sources and requesting sensitive information or unexpected offers and prizes from sought-after brands that contain or link to malware.

While antimalware and antivirus software can help flag these kind of malicious emails, social engineering is best dealt with through training. Employees must be educated in the many ways they may be approached by outside attackers and how they need to react when they receive suspicious requests. An understanding of social engineering is essential in preventing it. Training should also be put to the test to identify any potential weaknesses among employees.

2. Data Sharing Outside the Company

Employees sharing sensitive data either publically or with third parties outside the company can spell disaster. This usually happens out of carelessness: a reply all button is hit instead of a simple reply, information is sent to the wrong email address, something is accidentally posted publically.

These kind of incidents are rarely helped by training as they represent human errors which we are all prone to. Specialized software like Data Loss Prevention (DLP) tools can help organizations keep track of sensitive data and ensure that its transfer, whether by email or other internet services, is limited or blocked all together.

3. Shadow IT

The use of unauthorized third party software, applications or internet services in the work place is often hard to trace by IT departments which is where the term shadow IT comes from. The reasons for the prevalence of shadow IT are fairly simple: employees use known applications out of habit, because they improve their efficiency and lighten their workload or are more user-friendly than company-authorized alternatives.

4. Use of unauthorized devices

A lot of data protection policies focus on data transfers outside the company network over the internet and fail to consider another often used method: portable devices. USBs in particular have long been the bane of data protection strategies. Easy to lose or steal, but convenient to use, USBs have led to some disastrous data breaches such as the by now infamous

5. Physical theft of company devices

In today's increasingly mobile work environment, employees often take their work computers and portable devices out of the office. Whether working remotely, visiting clients or attending industry events, work devices often leave the security of company networks and become more vulnerable to both physical theft and outside tampering.

Encryption is always a good solution to guard against physical theft. Whether it's laptops, mobile phones or USBs, encryption removes the possibility that anyone who steals them can access the information on them. Enabling remote wipe options can also help organizations erase all data on stolen devices from a distance

Prevention methods of physical theft

- **Don't leave your device alone, even for a minute!**

  If you're not using it, lock your device in a cabinet or drawer, use a security cable, or take it with you. It's not enough to simply ask the stranger next to you in a library or coffee shop to watch your laptop for a few minutes.

- **Differentiate your device**

  It's less likely that someone will steal your device and say they thought it belonged to them if your device looks unique. Sometimes these markings make the laptop harder to resell, so they're less likely to be stolen. Use a permanent marking, engraving, or tamper-resistant commercial asset tracking tag.

Rahul Publications

- **Delete sensitive information**

  Don't keep any restricted data on your laptop. We recommend searching your computer for restricted data and deleting it. Restricted data includes your Social Security number, credit card numbers, network IDs, passwords, and other personally identifiable information. You'd be surprised how easy it is to forget that this information is on your computer!

- **Back it up**

  Set a reminder to backup your data on a regular basis! Keep an external copy of important files stored on your laptop in a safe location in case it is lost or stolen. Your photos, papers, research, and other files are irreplaceable, and losing them may be worse than losing your device.

- **Encrypt information**

  Protect your personal data with the built-in disc encryption feature included with your computer's operating system (e.g., Bit Locker or FileVault).

- **Record the serial number**

  Jot down the serial number of your device and store it in a safe place. This information can be useful for verifying your device if it's found.

- **Install software**

  Install and use tracking and recovery software included with most devices (e.g., the "Find iDevice" feature in iOS) or invest in commercial products like LoJack or Prey. Some software includes remote-wipe capabilities. This feature allows you to log on to an online account and delete all of the information on your laptop. There are both paid and free versions of this type of software, and each provides different levels of features. Search online to find the best combination of cost and functions to meet your needs.

3.3 Abuse of Privileges

Q3. What is privilege abuse? Explain how to handle them

Ans : **(Imp.)**

Privileged account abuse occurs when the privileges associated with a particular user account are used inappropriately or fraudulently, either maliciously, accidentally or through willful ignorance of policie.

In a typical scenario, privilege abuse is the direct result of poor access control: Users have more access rights than they need to do their jobs, and the organization fails to properly monitor the activity of privileged accounts and establish appropriate controls.

These access control issues often stem from a lack of coordination between IT management and security teams. IT is in charge of user accounts, but its main goal is administration. Security teams, meanwhile, are responsible for monitoring privileged accounts to protect the company from insider and outsider threats and ensure compliance with regulatory requirements.

Consequences of privilege abuse

Privileged accounts are a gateway to critical systems and data. Abuse of these powerful accounts can lead to the loss of sensitive data and business intelligence, as well as downtime of systems and applications essential for business operations. In addition to the direct damage to the business, these issues can result in bad publicity and loss of customers and lawsuits that can last for years — as well as compliance failures and their related penalties, which can include both steep fines and imprisonment for top management.

proper privileged account management

Proper privileged account management is the key to minimizing the risk of privilege abuse. Here are some real cases that illustrate the benefits of privileged account security in different industries and in IT departments both large and small:

Rahul Publications

1. Protection against any unwanted activity.

A government agency stores a variety of personally identifiable information (PII) about citizens. To ensure the security of this sensitive data and comply with regulatory requirements, the IT team carefully performs user activity monitoring and reviews all suspicious actions and other anomalies with other IT staff to determine whether the action was authorized or needs to be investigated further.

2. Protection against third-party violations

A financial company also deals with a lot of sensitive data that must be stored securely to comply with regulations, maintain customer trust and loyalty and ensure ongoing business operations. But monitoring of employee activity is not enough, because vendors also access internal systems to perform maintenance tasks. By automatically video recording all vendor activity, the IT team stays aware of exactly what each account does, so they can quickly spot any misuse of permissions that could endanger sensitive data.

3. Protection against ex-employees or temporary workers

An educational institution has high turnover of staff and students, but HR doesn't always report these important changes to IT. To prevent security incidents, the IT team continuously apply user activity monitoring across its distributed IT infrastructure, including file manipulations, so they can quickly spot any unwanted activity and respond appropriately. One investigation led to the discovery of two ex-employees who still had access to their accounts and took advantage of it by deleting curriculum files.

4. Protection against low experienced employees

Another educational institution offers students the opportunity to work in the IT department, which requires giving them rights to critical systems to perform specific tasks. But they must not be allowed to read or delete files that contain sensitive information, such as grades and financial data on loans. While students are trusted to make appropriate IT changes, department heads track their activity to verify the changes have been made correctly and that no one accesses anything they shouldn't.

5. Protection against human mistakes

An energy company uses SQL databases to store extremely important data, such as sensitive customer information and usage data used for billing. Because this data is business-critical, the IT department pays special attention to monitoring all changes to it. One of the routine checks revealed an unauthorized change. Further investigation showed it was made by an employee who gained DBA rights by mistake. By removing those privileges right away, the company reduced the risk of data loss and operational downtime.

6. Protection against overexposure of data

A lottery company stores sensitive information about players and retailers. Employees need different level of access to this data, and as their roles change (for example, due to a promotion or internal transfer), their access permissions must be updated accordingly. To avoid overexposure of sensitive data and minimize the risk of privilege misuse, the company continuously reviews user access rights, access attempts, manipulations with files and other activity in the IT environment.

7. Self-protection in case of a security breach

What if you are the only IT person in your organization? If you follow all security policies and diligently perform your duties, then you can never be accused of privilege misuse, right? Well, no. There might be a situation when you need to prove that you did your best and a breach is not your fault.

Rahul Publications

Proper privileged account management will be your savior. As one IT administrator put it, "I'm the only person managing IT in our company. I keep track of my own activities not only for compliance reasons, but to save my hide as well. If anything happens, nobody can accuse me of doing something wrong. There is proof."

Three steps for reducing the risk of privileged account abuse

Is it possible to prevent all privilege abuse? No. Some insiders will misuse their privileges, either accidentally or maliciously, and your privileged accounts will always be a top target of outside attackers who want to take advantage of their powerful permissions. However, you can minimize these risks. Here are three key steps to get started:

Step 1. Continuously assess and properly manage assigned privileges

Ask your friends whether they have ever accessed information they shouldn't have seen. I'm sure you'll find that many of them have. This happens because privilege assignment is often seen as a one-time task, which it shouldn't be. Instead, on a regular basis, you make sure to:

- Review access rights and remove excessive permissions in accordance with the least-privilege principle.
- Review and update permissions whenever a user's role in the organization changes.
- Make sure your sensitive data is not overexposed by verifying that access to it is granted based strictly on a specific need.
- Pay special attention to your privileged accounts — who can use them and what permissions they grant.

Step 2. Gain visibility into your IT environment

Would you know if there was a suspiciously high number of failed attempts to access a critical file or database, or an unauthorized modification to your security groups? If not, this step is especially important to you. Without a thorough monitoring of all changes and user activity in the IT environment, it is impossible to detect threats, including privilege abuse, in their early stage.

Step 3. Analyze user behavior

It's one thing to collect data. It's totally another to get meaningful insights out of it. Can you tell when your users exercise their privileges outside of normal working hours? Do you know whether their current behavior deviates from the norm? User behavior analysis will show you anomalies that are not always obvious if you just look at event logs.

3.4 Unauthorized Access by Outsider

Q4. What is Unauthorized Access? Explain the methods to prevent it.

Ans :

Unauthorized access refers to individuals gaining access to an organization's data, networks, endpoints, applications or devices, without permission. It is closely related to authentication – a process that verifies a user's identity when they access a system. Broken, or misconfigured authentication mechanisms are a main cause of access by unauthorized parties.

Other common causes of unauthorized access

- Weak passwords selected by users, or passwords shared across services
- Social engineering attacks, primarily phishing, in which attackers send messages impersonating legitimate parties, often with the aim of stealing user credentials
- Compromised accounts – attackers often seek out a vulnerable system, compromise it, and use it to gain access to other, more secure systems
- Insider threats – a malicious insider can leverage their position to gain unauthorized access to company systems

Rahul Publications

- Zeus malware – uses botnets to gain unauthorized access to financial systems by stealing credentials, banking information and financial data
- Cobalt strike – a commercial penetration testing tool used to conduct spear-phishing and gain unauthorized access to systems

Security Breach or Data Breach

A security breach or data breach is a successful attempt by an attacker to gain unauthorized access to organizational systems

Blocking unauthorized access plays a central role in preventing data breaches. However, a robust security program uses "defense in depth" – several layers of security defenses, in an attempt to mitigate attacks long before attackers reach a sensitive system. Additional layers of security include network protection, endpoint protection, and data protection.

A typical security breach happens in three stages:

- **Research** — The attacker searches for weaknesses or vulnerabilities in organizational systems, people or processes.
- **Network/Social attack**

  The attacker attempts to penetrate the network perimeter, either by evading network defenses, or by using social engineering to trick individuals into providing access, data or credentials.
- **Exfiltration** — Once the attacker manages to gain access, they can steal valuable assets or cause damage at their entry point, and also perform lateral movement to gain access to additional, more valuable systems.

Best Practices to Prevent Unauthorized Access

Here are several ways your organization can improve the strength of authentication mechanisms and prevent access by unauthorized parties, whether internal or external.

Electronic Data Protection

- Monitoring should be in place to flag suspicious attempts to access sensitive information.
- Inventory of the devices on the network should be performed regularly to maintain comprehensive, up-to-date maps.
- Encryption should be used for viewing, exchanging, and storing sensitive information.
- Network drives should be used to store sensitive information to protect it from unauthorized access and for disaster recovery.
- Mobile devices and personal computing devices should not be used for storing sensitive information.
- Removable media and devices should not be used to store sensitive information.
- Access to systems and data should be limited on a need to use basis, also known as the principle of least privilege.
- Suspected security breaches should be reported immediately.

Backup and Disposal of Data

- Data should be backed up and stored according to data governance policies.
- Sensitive data backed up to cloud storage providers should be encrypted.
- Backups should be conducted on a regular basis.
- Data that is no longer needed should be permanently deleted.
- Professional computer recycling programs should be used for decommissioned computers and devices, with all data removed prior to the recycling process.
- Cross shedders should be used to dispose of paper documents.

Password Management and Protection

Organizational leaders should ensure strong password policies and effective compliance

Rahul Publications

programs are in place to prevent unauthorized access, as well as follow these guidelines themselves.

- Unique passwords should be used for each online account.
- Passwords should be changed for any account or device that has experienced an unauthorized access incident.
- Strong passwords should be used that include a combination of letters, numbers, and symbols. A password should not be a word, common phrase, or one that someone with a little personal knowledge might guess, such as the user's child's name, address, or phone number.
- Passwords should never be shared.
- Passwords should be changed periodically.
- Passwords should not be written down or stored in an unsecure location.

System and Device Protection

- Multifactor authentication should be used for all systems.
- Malware scans should be regularly run on all systems.
- Computers, laptops, and smart devices should have the lock screen enabled, and should be shut down when not in use for extended periods.
- Single sign-on (SSO) should be considered to centrally manage users' access to systems, applications, and networks.
- Operating systems and applications should be updated when patches and new versions are available.
- Anti-virus, anti-malware, and anti-ransomware software should be installed on all computers, laptops, and smart devices.

Electronic Communications Protection-Email, Instant Messaging, Text Messaging, and Social Media

- Sensitive data should only be encrypted or sent as a password-protected file.
- Attachments or links from untrusted sources should not be opened.
- Caution should be taken to avoid phishing scams.

Coach Employees to Avoid Risky Behaviors

- Screens should be positioned so they cannot be viewed by others.
- Special precautions should be taken when leaving devices unattended in work from home environments.
- Account recovery questions should not be easy to guess.
- Pop-ups and shortened URLs should not be clicked on unless from a trusted source.
- Sensitive information should not be accessed or discussed in public locations.

3.5 MALWARE INFECTION

Q5. Explain various types of malware infection and attacks. Write about how to remove malware from the devices.

Ans : **(Imp.)**

Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user's permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware and other malicious programs.

Types of Malware

- **Viruses**

  A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

- **Worms**

  Worms replicate themselves on the system, attaching themselves to different files and

Rahul Publications

looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.

- **Spyware**

  Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

- **Trojan horse**

  A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files.

- **Logic Bombs**

  A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cyber security specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.

- **Ransomware**

  Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key which is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.

- **Backdoors**

  A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant the cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.

- **Rootkits**

  A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.

- **Keyloggers**

  Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program

Types

Malware also uses a variety of methods to spread itself to other computer systems beyond an initial attack vector. Malware attack definitions can include:

- Email attachments containing malicious code can be opened, and therefore executed by unsuspecting users. If those emails are forwarded, the malware can spread even deeper into an organization, further compromising a network.
- File servers, such as those based on common Internet file system (SMB/CIFS) and network file system (NFS), can enable malware to spread quickly as users access and download infected files.
- File-sharing software can allow malware to replicate itself onto removable media and then on to computer systems and networks.
- Peer to peer (P2P) file sharing can introduce malware by sharing files as seemingly harmless as music or pictures.
- Remotely exploitable vulnerabilities can enable a hacker to access systems regardless of geographic location with little or no need for involvement by a computer user.

Rahul Publications

How To Remove Malware

1. Stop shopping, banking, and doing other things online that involve usernames, passwords, or other sensitive information — until you get your device cleared of any malware.
2. Check to see if you have security software on your device — if not, download it. Find recommendations from independent review sites by doing a search online. Also ask friends and family for recommendations. Some software that claims to be security software to protect you from malware is malware, so it's important to do your research.
3. Make sure your software is up to date. Check that all software - the operating system, security software, apps, and more - is up to date. Consider turning on automatic updates so your software always stays up to date.
4. Scan your device for malware. Run a malware or security Delete anything it identifies as a problem. You may have to restart your device for the changes to take effect. Run your scan again to make sure everything is clear. If the scan shows there are no more issues, you've likely removed the malware.

   If you're not able to fix your device with steps 1-4, steps 5 and 6 may resolve the issue. When using either of these options, you risk losing data. If you've backed up your data regularly, you'll minimize what you lose.
5. Recover your operating system. To find out how to recover your operating system (like Windows or Mac OS), visit your device manufacturer's website. Recovering your system typically means you'll get back a lot of the data stored on the device, so it's a good alternative to reinstalling your operating system (step 6). That is, if it clears the malware problem. After recovering your operating system, you'll want to go back to steps 2, 3 and 4 to ensure that you've removed the malware.
6. Reinstall your operating system. To find out how to reinstall your operating system (like Windows or Mac OS), visit your device manufacturer's website. Reinstalling your system is the safest way to clean an infected device, but you'll lose all of the data stored on the device that you haven't backed up.

3.6 Intrusion detection and Prevention Techniques

Q6. Explain about Intrusion detection and prevention techniques.

Ans : **(Imp.)**

Due to the internet being a vast place, it is very difficult to pinpoint a particular way in which Network Intrusion takes place. However, the following are some common techniques through which Network Intrusion has taken place:

1. Multi-Routing

This refers to when the intruders use multiple sources to intrude which helps them avoid detection. This is also known as asymmetric routing;

2. Buffer Overflow Attacks

The Buffer overflow attack refers to when certain sections of the computer's memory code is rewritten so that they can be used as a part of the intrusion later on;

3. Traffic Flooding

This type of attacks are when the intruders flood the victim's systems with traffic that they cannot handle in order to cause chaos and confusion. When the systems have too large traffic in order to screen, then they can easily get away undetected;

4. Trojan Horse Malware

Trojan Horse Malware gives provides a network backdoor to the attackers so that they get an unfettered access to the network;

5. Worms

This type of virus is most common and effective. Worms usually spread through email or instant messaging and can spread throughout the network.

Rahul Publications

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

Classification

IDS are classified into 5 types:

1. Network Intrusion Detection System (NIDS)

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

2. Host Intrusion Detection System (HIDS)

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

3. Protocol-based Intrusion Detection System (PIDS)

Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

4. Application Protocol-based Intrusion Detection System (APIDS)

Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

5. Hybrid Intrusion Detection System

Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent

Rahul Publications

or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS

1. Signature-based Method

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. Anomaly-based Method

Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

Intrusion Prevention System (IPS)

Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.

Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both IPS and IDS operate network traffic and system activities for malicious activity.

IPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment or changing the attack's content.

Classification of Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) is classified into 4 types:

1. Network-based intrusion prevention system (NIPS)

It monitors the entire network for suspicious traffic by analyzing protocol activity.

2. Wireless intrusion prevention system (WIPS)

It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

3. Network behavior analysis (NBA)

It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.

Rahul Publications

4. Host-based intrusion prevention system (HIPS)

It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

Detection Method of Intrusion Prevention System (IPS)

1. Signature-based detection

Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.

2. Statistical anomaly-based detection

Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.

3. Stateful protocol analysis detection

This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

Comparison of IPS with IDS

The main difference between Intrusion Prevention System (IPS) with Intrusion Detection Systems (IDS) are:

1. Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
2. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.

   IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

3.7 ANTI-MALWARE SOFTWARE

Q7. What is antimalware (anti-malware)? Explain how it works.

Ans :

Antimalware is a type of software program created to protect information technology (IT) systems and individual computers from malicious software, or malware. Antimalware programs scan a computer system to prevent, detect and remove malware.

The three most common types of malware mentioned above are viruses, worms and Trojan horses. A virus is a piece of software that duplicates itself and spreads from one computer to another. A worm is similar to a virus, except that it doesn't need to infect other programs on a computer to spread. A worm can spread on its own. A Trojan horse appears to be something benign, such as a game or a screen saver, but it actually contains code that causes damage to the computer or enables the author to access the user's data.

How antimalware works

Antimalware software uses three strategies to protect systems from malicious software: signature-based detection, behavior-based detection and sandboxing.

1. Signature-based malware detection

Signature-based malware detection uses a set of known software components and their digital signatures to identify new malicious software. Software vendors develop signatures to detect specific malicious software. The signatures are used to identify previously identified malicious software of the same type and to flag the new software as malware. This approach is useful for common types of malware, such as keyloggers and adware, which share many of the same characteristics.

2. Behavior-based malware detection

Behavior-based malware detection helps computer security professionals more quickly identify, block and eradicate malware by using an active approach to malware analysis.

Rahul Publications

Behavior-based malware detection works by identifying malicious software by examining how it behaves rather than what it looks like. Behavior-based malware detection is designed to replace signature-based malware detection. It is sometimes powered by machine learning algorithms.

3. Sandboxing

Sandboxing is a security feature that can be used in antimalware to isolate potentially malicious files from the rest of the system. Sandboxing is often used as a method to filter out potentially malicious files and remove them before they have had a chance to do damage.

For example, when opening a file from an unknown email attachment, the sandbox will run the file in a virtual environment and only grant it access to a limited set of resources, such as a temporary folder, the internet and a virtual keyboard. If the file tries to access other programs or settings, it will be blocked, and the sandbox has the ability to terminate it.

Uses of antimalware

The value of antimalware applications is recognized beyond simply scanning files for viruses. Antimalware can help prevent malware attacks by scanning all incoming data to prevent malware from being installed and infecting a computer. Antimalware programs can also detect advanced forms of malware and offer protection against ransomware attacks.

Antimalware programs can help in the following ways:

- prevent users of from visiting websites known for containing malware;
- prevent malware from spreading to other computers in a computer system;
- provide insight into the number of infections and the time required for their removal; and
- provide insight into how the malware compromised the device or network.

Antimalware is helpful to keep a computer malware-free, and running an anti-malware program regularly can help keep a personal computer (PC) running smoothly and safely. The best type of antimalware software catches the most threats and requires the fewest updates, meaning it can run in the background without slowing the computer down. There are many free antimalware programs that can protect a computer from becoming infected with malware.

3.8 NETWORK BASED INTRUSION DETECTION SYSTEMS

Q8. Explain about Network based Intrusion detection system.

Ans : **(Imp.)**

Network intrusion detection systems (NIDS) attempt to detect cyber attacks, malware, denial of service (DoS) attacks or port scans on a computer network or a computer itself. NIDS monitor network traffic and detect malicious activity by identifying suspicious patterns in incoming packets. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

Why are NIDS Needed?

Due to the sophistication of cyber threats and data breaches, implementing and maintaining network security, data security and information security requires a defense in depth approach. Organizations need to secure their networks with a combination of technologies and detection methods designed to combat multiple attack vectors, intrusion and compromise methods available to cyber criminals today.

It's no longer enough to rely on a simple security system and antivirus software that can protect against known attacks at the application layer.

A variety of tools and methodologies exist, however two common elements used to secure enterprise network configurations are the firewall and intrusion detection and intrusion prevention systems (IDS/IDPS). Firewalls control incoming and

Rahul Publications

outgoing traffic based on rules and policies, acting as a barrier between secure and untrusted networks.

Inside the secure network, an IDS/IDPS detects suspicious activity to and from hosts and within traffic itself, taking proactive measures to log and block attacks.

The main difference between intrusion detection systems and intrusion prevention systems are that intrusion prevention systems are placed inline. This means they can actively prevent or block intrusions that are detected. IPS can send an alarm, drop malicious packets, reset a connection, block traffic from an offending IP address, correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

This post will focus on NIDS rather than host intrusion detection systems (HIDS) and intrusion prevention systems.

Signature-Based NIDS and Anomaly-Based NIDS

NIDS can incorporate one or both types of intrusion detection: signature-based and anomaly-based.

A signature-based NIDS monitors network traffic for suspicious patterns in data packets, signatures of known network intrusions, to detect and remediate attacks and compromises.

This is achieved through the use of a database of known intrusion types and data patterns, allowing signature-based NIDS to quickly identify intrusions and initiate the appropriate course of action.

In contrast, anomaly-based NIDS use the baseline of the system in a normal state to track whether unusual or suspicious activity is occurring. This method takes time to set up, as baselining requires the NIDS to learn about your usage patterns, making it an organic, heuristic based approach to intrusion detection.

The benefit of anomaly-based NIDS is that it is more flexible and powerful than signature-based NIDS that require an intrusion type is on file to pattern match against.

For example, a newly discovered intrusion type or vulnerability may not yet to be listed on CVE, making it hard for the signature-based NIDS to detect it.

However, an anomaly-based NIDS could react immediately to the change in baseline.

In general, it's suggested to employ a defense in depth strategy because both have their pros and cons.

Signature-based approaches are faster, generate less false positives and don't require time for baselining. However, they are reactive in nature and are completely exposed to new cyber threats. as they rely on a database of preexisting intrusion signatures.

While anomaly-based NIDS are difficult to set up, configure and train, they can be effective against new and existing attack vectors because of their ability to baseline a system at each protocol stack.

Signature-based and anomaly-based NIDS have complementary strengths and should be used together.

Limitations

- Noise can limit a NIDS effectiveness. Bad packets generated from bugs, corrupt DNS data and local packets can create a high false-alarm rate.
- It's common for the number of real attacks to be far lower than the number of false-alarms.
- Many attacks take advantage of vulnerabilities in outdated software, so a constant feed of new signatures is needed to mitigate threats.
- Signature-based NIDS have a delay between a new threat discovery and its signature being applied to the NIDS. During this time, the NIDS will be unable to identify the threat.
- NIDS don't compensate for weak identification and authentication or weaknesses in network protocols.
- Encrypted packets aren't processed by most NIDS and can be used to allow intrusion to

Rahul Publications

the network that is undiscovered until further intrusion has occurred.

- NIDS provides information based on network address associated with the IP packet that is sent into the network. As we know, IP attribution is not perfect and can be faked or scrambled.
- NIDS are susceptible to protocol-based attacks and invalid data and TCP/IP stack attacks can cause NIDS to crash.

Q9. What is the Difference Between NIDS and HIDS?

Ans :

IDS/IDPS offerings can be split into two solutions: network intrusion detection systems (NIDS) and host intrusion detection systems (HIDS).

NIDS are strategically positioned at various points in the network to monitor incoming and outgoing traffic to and from networked devices. NIDS solutions offer sophisticated, real-time intrusion detection capabilities, consisting of an assembly of interoperating pieces: a standalone appliance, hardware sensors and software components are common. These work in concert to allow a wider range of network intrusion detection capabilities than HIDS solutions.

In contrast, HIDS solutions are installed on every computer's operating system to analyze and monitor traffic coming to and from the device in question. HIDS also track and monitor local file changes and potential alterations due to unauthorized access and/or compromise.

A comprehensive cyber security strategy will employ both NIDS and HIDS since each comes with distinct advantages and disadvantages.

For example, since HIDS are host-installed and have access to details such as registry settings, logs and other system information, they can make IP address attribution and digital forensics more accessible. However, resources are drawn from the host (e.g. the computer the HIDS is installed on) to power the HIDS and HIDS are reactive in nature and can only respond to an attack after it has occurred.

In contrast, NIDS are usually hardware installed on the network itself and don't tap into any underlying network devices for resources. The installation of NIDS tends to be simple too, simply drop them into the network to begin monitoring for suspicious traffic. However, NIDS are usually expensive and targeted at the enterprise user.

That said, there are a decent selection of free, open-source NIDS solutions available based on commodity hardware that offer comparable levels of security and protection as commercial NIDS offerings.

Before we can jump into what free NIDS offerings are available, another distinction must be made concerning how different types of NIDS detect intrusions.

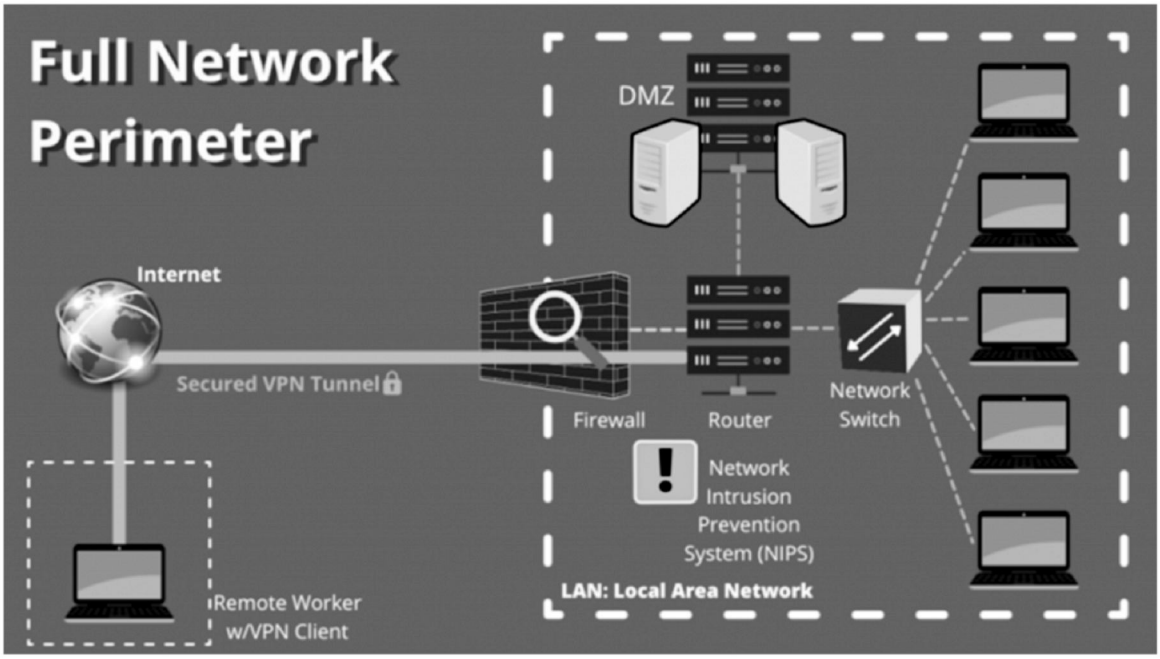
3.9 NETWORK BASED INTRUSION PREVENTION SYSTEMS

Q10. What Is a Network Intrusion Prevention System and How Does it Work?

Ans : **(Imp.)**

Starting off, a network intrusion prevention system (NIPS) is a type of network security software that detects malicious activity on a network, reports information about said activity, and takes steps to block or stop the activity from occurring automatically. This is an expansion of capabilities over an "intrusion detection system," which you can guess by the name only detects threats but doesn't take any active steps to prevent them. The NIPS lives within the network perimeter between the firewall and the router as a sort of checkpoint and enforcement point for network traffic passing through.

Rahul Publications



The network intrusion prevention system is one of the last lines of defense in the network perimeter before traffic hits the router and subsequently the switch.

A network intrusion prevention systems use three types of intrusion detection:

- **Signature**

  Detects attacks based on specific patterns, such as network traffic, number of bytes, and known previous attacks

- **Anomaly**

  Systems use machine learning to create a model of trustful activity and compare the current activity with it

- **Policy**

  Relies on predetermined network traffic baselines and activity outside of that baseline is seen as a potential threat to the network; requires a systems administrator to configure security policies manually

More advanced intrusion prevention systems can rely less and less on policy-based detections, and more on anomaly and signature-based detections. Once the intrusion prevention system has detected a threat, it takes steps to alert administrators of the issue, then acts to drop packets from the offending source or reset the connection between the network and the source.

Sometimes an intrusion prevention system can work in conjunction with a honeypot within the demilitarized zone (DMZ) of a network to detect malicious traffic and send them to a fake source of seemingly valuable data separate from the actual network. This allows network security personnel to observe and learn more about continuous threats to the network and build new signature-based security policies.

Rahul Publications

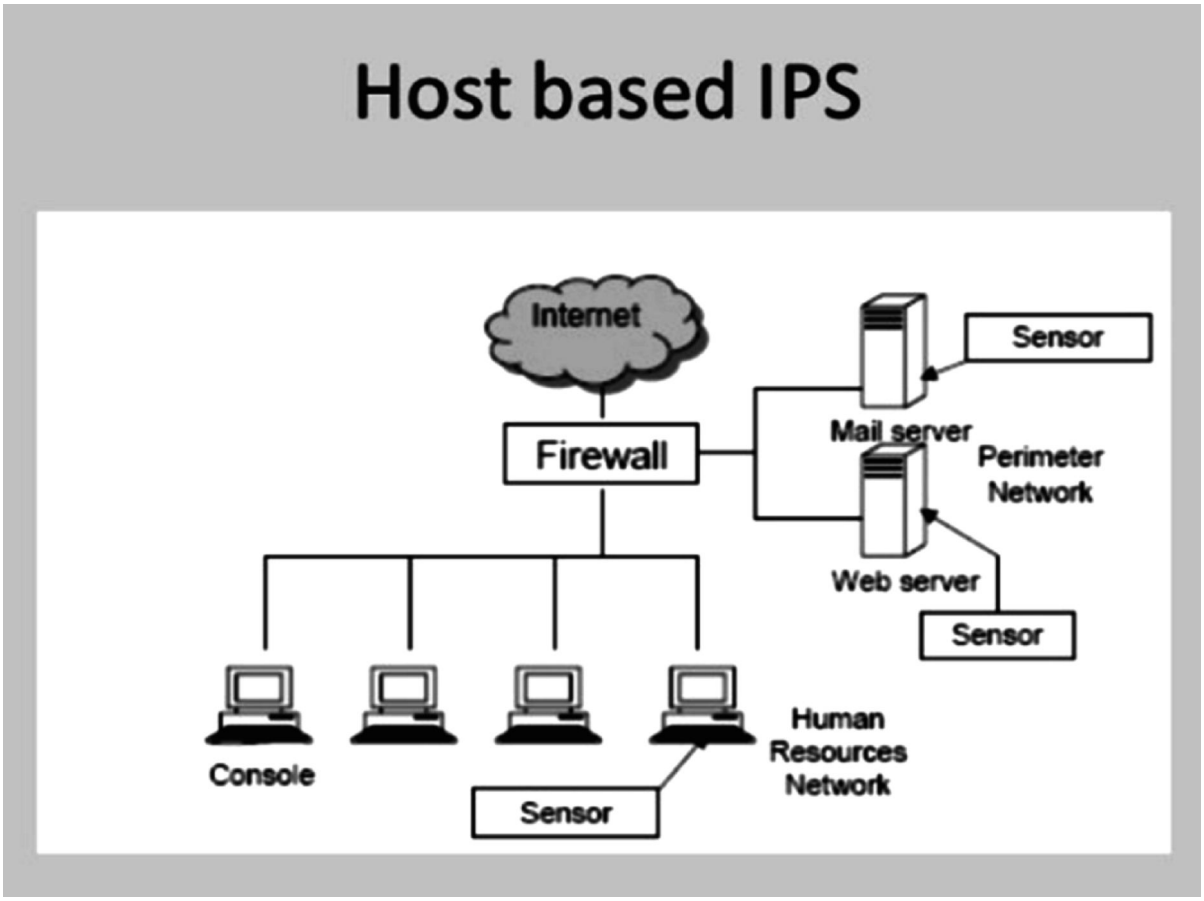
3.10 HOST BASED INTRUSION PREVENTION SYSTEMS

Q11. Explain about HIPS.

Ans :

The Host-based Intrusion Prevention System (HIPS) protects your system from malware and unwanted activity attempting to negatively affect your computer. HIPS utilizes advanced behavioural analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys. HIPS is separate from Real-time file system protection and is not a firewall; it only monitors processes running within the operating system.

HIPS settings can be found in Advanced setup (F5) > Detection engine > HIPS > Basic. The HIPS state (enabled/disabled) is shown in the ESET Endpoint Security main program window, in the Setup > Computer.



A host intrusion prevention system (HIPS) is an approach to security that relies on third-party software tools to identify and prevent malicious activities

Host-based intrusion prevention systems are typically used to protect endpoint devices. Once the malicious activity is detected, the HIPS tool can take a variety of actions, including sending an alarm to the computer user, logging the malicious activity for future investigation, resetting the connection, dropping malicious packets and blocking subsequent traffic from the suspect IP address.

Some host intrusion prevention systems allow users to send logs of malicious activity and fragments of suspicious code directly to the vendor for analysis and possible identification.

Most host intrusion prevention systems use known attack patterns, called signatures, to identify malicious activity. Signature-based detection is effective, but it can only protect the host device against known attacks. It cannot protect against zero day attacks or signatures that are not already in the provider's database.

The second approach to intrusion detection establishes a baseline of normal activity and then compares current activity against the baseline. The HIPS looks for anomalies, including deviations in bandwidth, protocols, and ports. When activity varies outside of an acceptable range — such as a remote application attempting to open a normally closed port - an intrusion may be in progress.

However, an anomaly, such as a sudden spike in bandwidth use, does not guarantee an actual attack, so this approach amounts to an educated guess and the chance for false positives can be high.

A third common intrusion-detection method uses stateful inspection to assess the actual protocols in packets traversing the network. The analysis is called stateful because the malware prevention tool tracks the state of each protocol. For example, it understands how TCP and UDP packets can or cannot carry DNS, SMTP, HTTP and other protocols — and what values should or should not be contained within each packet of each protocol. Stateful protocol analysis looks for deviations from normal states of protocol content and can flag a possible attack when an unexpected deviation occurs. Since stateful analysis is more aware of actual packet contents, the chances for false positives are somewhat lower than statistical anomaly detection.

HIPS products often focus on just one of the three approaches, though multiple approaches are sometimes used. For example, McAfee's Host Intrusion Prevention for Desktop and Dell's Managed iSensor Intrusion Prevention System (IPS) service are just two offerings that rely on multiple approaches to intrusion prevention.

3.11 Security Information Management

Q12.Explain Security Information Mnanagement.

Ans :

Security information management is a process of gathering, monitoring and investigating log data in order to find and report suspicious activities on the system. This process is automated by security information management systems or tools.

Log data is nothing but a file that collects and stores whatever happens in the system. The files (records) have information about system activities such as running applications, services, errors that occurred. So that is what security log data is.

With security log files, one can know the IP address of the system, MAC or internet address, login data and status of the system. If such details fall on bad guys, they might use the details destructively. This is one of the major reasons behind the birth of security information management.

Well, the log data is collected from various sources like firewalls, intrusion detection systems, antivirus software, proxy servers, file systems, etc. So based on the data gathered from all sources, security information is monitored and maintained.

Thus, this is what and how the SIM system does its job. Security management is categorized into three segments. One of them is SIM. Another one is SEM (Security Event Management) which deals with real-time monitoring and alerting the admins whenever it detects certain events occurring in the network activity. The last one is the fusion of SIM + SEM = SIEM (Apparently the abbreviation stands for Security Information Event Management). These days, businesses prefer the power-packed fusion of SIEM tools majorly.

What exactly SIM systems do ?

- SIM systems keep track and show the activity analytics of the system events as they happen.
- They then translate events data gathered from many resources into a general and simplified format. Usually, the data is translated into an XML file.

Rahul Publications

- SIM systems collect and coordinate data from various resources in such a way that helps administrators to recognize the real threats and false positives on the system. False positives mean events that seem to be a major threat but in reality it's not a threat.
- As soon as suspicious activities occur, the SIM tool responds to the event by sending alerts to administrators of organizations and by generating reports and graphical representations such as charts and graphs.

The reports generated by SIM systems are typically used to :

1. Detect unauthorized access as well as modifications to files and data breaches.
2. Identify data trends that can be leveraged potentially by business organizations for their progression.
3. They are also used to identify network behavior and assess performance.

The SIM tool (system) acts as a software agent which sends the reports about the events to the centralized server. By which admins are updated about the reports. That's all about Security Information Management.

3.12 Network Session Analysis

Q13. What is session data? Explain how the session can be analyzed in netrwork.

Ans :

A session, also known as a flow, a stream or a conversation, is a summary of a packet exchange between two systems."

the seven minimum elements of a session, namely:

- Timestamp (generally when the session began, preferably including the end of the session, too).
- Protocol.
- Source IP address.
- Source port (for protocols that offer ports, like TCP, SCTP and UDP).
- Destination IP address.
- Destination port.

Measure of the amount of information exchanged during the session (to include bytes sent by the source, bytes sent by the destination, packets sent by the source and packets sent by the destination).

The intrusion detection system can identify suspicious and malicious activity by inspecting network traffic. Snort makes a judgment based on its analytical capabilities and notifies the operator of its decision by generating an alert. I call the output of this collect-inspect-report process "alert data." No alerting system can perfectly identify all suspicious or malicious activity. In many cases it's simply not possible — especially on a packet-by-packet basis — to identify a packet or stream as being worthy of an operator's attention. In those cases it makes sense to keep a log of the traffic. Recording traffic or characteristics of traffic for later analysis has recently been labeled retrospective network analysis (RNA),

Network session data represents a high-level summary of "conversations" occurring between computer systems. No specifics about the content of the conversation such as packet payloads are maintained, but various elements about the conversation are kept and can be very useful in investigating an incident or as an indicator of suspicious activity. However the session data is generated, there are a number of common elements constituting the session, such as source IP address, source port, destination IP address, destination port, time-stamp information, and an array of metrics about the session, such as bytes transferred and packet distribution.

Using the collected session information, an analyst can examine traffic patterns on a network to identify which systems are communicating with each other and identify suspicious sessions that warrant further investigation.

For example, a server configured for internal use by users and having no legitimate reason to communicate with addresses on the Internet will cause an alarm to be generated if suddenly a session or sessions appear between the internal server and external addresses. At that point the analyst may suspect a malware infection or other system compromise and investigate further. Numerous

Rahul Publications

other queries can be generated to identify sessions that are abnormal in some way or another such as excessive byte counts, excessive session lifetime, or unexpected ports being utilized.

When run over a sufficient timeframe, a baseline for traffic sessions can be established and the analyst can query for sessions that don't fit the baseline. This sort of investigation is a form of anomaly detection based on high-level network data versus the more granular types discussed for NIDS and NIPS.

Another common use of network session analysis is to combine it with the use of a honeypot or honeynet . Any network activity, other than known-good maintenance traffic such as patch downloads, seen on these systems is, by definition, suspicious since there are no production business functions or users assigned to these systems. Their sole purpose is to act as a lure for an intruder. By monitoring network sessions to and from these systems, an early warning can be raised without even necessarily needing to perform any complex analysis.

3.13 System Integrity Validation

Q14. Write about system integrity validataion

Ans : **(Imp.)**

The System integrity check is a parameter that is responsible for checking the status of all security detectors and devices before arming. Checking is disabled by default.

This function is mandatory for professional security systems. It does not allow activating the arming mode if the window is not closed in the room, the detector lid is open, or communication with one of the devices is lost.

You can define restrictions in the hub settings. When this option is active, you can specify whether to allow arming with malfunctions or not.

If arming with malfunctions is allowed, and a malfunction was detected when trying to arm, you will need to confirm arming with the device from which you tried to arm (by pressing the arming button in the app or re-arming from Space Control/ Key Pad).

All users of the hub with the appropriate rights and settings receive notifications about arming with a complete list of malfunctions. The monitoring station of the security company also receives corresponding notifications.

Any system problems are caused by wrong software or hardware configuration - because of wrong installation, hardware or file system failure or software virus. Validation of software/hardware configuration is a must before system testing in development, during system manufacturing and field service.

Customizable System Integrity Check utility is used for validation of system software/hardware configuration. The utility provides recovery recommendation if problem is found.

Verification process is implemented in a number of stages. Each stage covers files with the same verification type and the same recovery recommendation. The following validation types may be used:

- Permanent files check - files that do not change
- Changeable files check - files that can change
- Registry entries check for Windows platform
- Custom software/hardware configuration check

Validation of the following file attributes is supported:

- Ownership, timestamp and permissions
- Check sum - for permanent files
- Non empty/non 0 content - for changeable files

Rahul Publications

Short Questions and Answers

1. What is Intrusion.

Ans :

An intrusion is any activity that is designed to compromise your data security. This can be through more menacing and pervasive formats like ransomware or unintentional data breaches by employees or others connected to your network.

An intrusion may include any of the following:

- Malware or ransomware
- Attempts to gain unauthorized access to a system
- DDOS attacks
- Cyber-enabled equipment destruction
- Accidental employee security breaches (like moving a secure file into a shared folder)
- Untrustworthy users both team members and those outside of your organization
- Social engineering attacks such as phishing campaigns and other ways of tricking users with seemingly legitimate communication

2. What is privilege abuse?

Ans :

Privileged account abuse occurs when the privileges associated with a particular user account are used inappropriately or fraudulently, either maliciously, accidentally or through willful ignorance of policie.

In a typical scenario, privilege abuse is the direct result of poor access control: Users have more access rights than they need to do their jobs, and the organization fails to properly monitor the activity of privileged accounts and establish appropriate controls.

These access control issues often stem from a lack of coordination between IT management and security teams. IT is in charge of user accounts, but its main goal is administration. Security teams, meanwhile, are responsible for monitoring privileged accounts to protect the company from insider and outsider threats and ensure compliance with regulatory requirements.

3. What is Unauthorized Access?

Ans :

Unauthorized access refers to individuals gaining access to an organization's data, networks, endpoints, applications or devices, without permission. It is closely related to authentication – a process that verifies a user's identity when they access a system. Broken, or misconfigured authentication mechanisms are a main cause of access by unauthorized parties.

4. Malware Infection.

Ans :

Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user's permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware and other malicious programs.

5. Types of Malware.

Ans :

- **Viruses**

  A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

- **Worms**

  Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.

- **Spyware**

  Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

Rahul Publications

- **Trojan horse**

  A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files.

- **Logic Bombs**

  A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cyber security specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.

6. Intrusion Detection System.

Ans :

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

7. Network Intrusion Detection System (NIDS).

Ans :

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

8. Host Intrusion Detection System (HIDS).

Ans :

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

9. Protocol-based Intrusion Detection System (PIDS).

Ans :

Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

Rahul Publications

10. Detection Method of IDS.

Ans :

1. Signature-based Method

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. Anomaly-based Method

Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

11. Anti - Malware Software.

Ans :

Antimalware is a type of software program created to protect information technology (IT) systems and individual computers from malicious software, or malware. Antimalware programs scan a computer system to prevent, detect and remove malware.

The three most common types of malware mentioned above are viruses, worms and Trojan horses. A virus is a piece of software that duplicates itself and spreads from one computer to another. A worm is similar to a virus, except that it doesn't need to infect other programs on a computer to spread. A worm can spread on its own. A Trojan horse appears to be something benign, such as a game or a screen saver, but it actually contains code that causes damage to the computer or enables the author to access the user's data.

12. HIPS.

Ans :

The Host-based Intrusion Prevention System (HIPS) protects your system from malware and unwanted activity attempting to negatively affect your computer. HIPS utilizes advanced behavioural analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys. HIPS is separate from Real-time file system protection and is not a firewall; it only monitors processes running within the operating system.

HIPS settings can be found in Advanced setup (F5)> Detection engine > HIPS > Basic. The HIPS state (enabled/disabled) is shown in the ESET Endpoint Security main program window, in the Setup >Computer.

Rahul Publications

Choose the Correct Answer

1. The full form of Malware is _____ [c]

   (a) Malfunctioned Software (b) Multipurpose Software

   (c) Malicious Software (d) Malfunctioning of Security

2. _____ is a type of software designed to help the user's computer detect viruses and avoid them. [c]

   (a) Malware (b) Adware

   (c) Antivirus (d) Both B and C

3. Which of this is an example of physical hacking ? [b]

   (a) Remote Unauthorised access

   (b) Inserting malware loaded USB to a system

   (c) SQL Injection on SQL vulnerable site

   (d) D DoS (Distributed Denial of Service) attack

4. Which among the following is the part of intrusion [d]

   (a) Malware or ransomware

   (b) Attempts to gain unauthorized access to a system

   (c) DDOS attacks

   (d) All the above

5. What are the different ways to classify an IDS? [b]

   (a) Zone based (b) Host & Network based

   (c) Network & Zone based (d) Level based

6. Where is an IPS commonly placed in a network ? [b]

   (a) In front of the firewall (b) In line with the firewall

   (c) Behind the firewall (d) On the end users' device

7. If it detects a threat, an IPS can: [d]

   (a) Record the details of the threat

   (b) Report the threat to security admins

   (c) Take preventative action to stop the threat

   (d) All of the above

8. Which of the following technique in not the part of Network Intrusion [d]

   (a) Multi-Routing (b) Detecting virus

   (c) Buffer Overflow Attacks (d) Traffic Flooding

Rahul Publications

9. Among the following which intrusion system generally resides within a group of servers. [c]

(a) Network Intrusion Detection System (NIDS)

(b) Host Intrusion Detection System (HIDS)

(c) Application Protocol-based Intrusion Detection System (APIDS)

(d) Protocol-based Intrusion Detection System (PIDS)

10. What are characteristics of Network based IDS ? [a]

(a) They look for attack signatures in network traffic

(b) Filter decides which traffic will not be discarded or passed

(c) It is programmed to interpret a certain series of packet

(d) It models the normal usage of network as a noise characterization

Rahul Publications

Fill in the blanks

1. An _____ is any activity that is designed to compromise your data security.
2. _____ refers to individuals gaining access to an organization's data, networks, endpoints, applications or devices, without permission.
3. _____ is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user's permission.
4. An Intrusion Detection System (IDS) is a system that monitors _____ for suspicious activity and issues alerts when such activity is discovered.
5. _____ comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server.
6. _____ is a network security application that monitors network or system activities for malicious activity.
7. _____ IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.
8. _____ programs scan a computer system to prevent, detect and remove malware.
9. _____ is often used as a method to filter out potentially malicious files and remove them before they have had a chance to do damage.
10. A _____ also known as a flow, a stream or a conversation, is a summary of a packet exchange between two systems.

Rahul Publications

ANSWERS

1. Intrusion
2. Unauthorized access
3. Malware
4. Network traffic
5. Protocol-based intrusion detection system (PIDS)
6. Intrusion Prevention System
7. Stateful protocol analysis detection
8. Antimalware
9. Sandboxing
10. Session

UNIT IV

Cryptography and Network Security:

Introduction to Cryptography, Symmetric key Cryptography, Asymmetric key Cryptography, Message Authentication, Digital Signatures, Applications of Cryptography. Overview of Firewalls- Types of Firewalls, User Management, VPN Security Security Protocols: - security at the Application Layer- PGP and S/MIME, Security at Transport Layer- SSL and TLS, Security at Network Layer- IPSec.

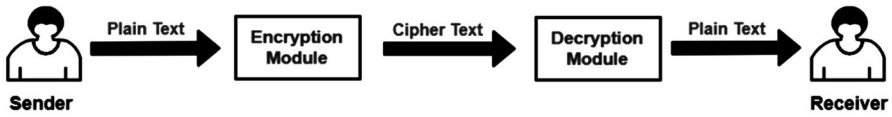
4.1 Introduction to Cryptography

Q1. What is Cryptography? Explain briefly.

Ans :

- Cryptography is a method of storing and transmitting data in a particular form.
- It ensures that only the person for whom the message is intended can read the message.

The message exchange using cryptography involves the following steps:



Cryptography

Step-1:

At sender side,

- Using an encryption algorithm, the message is converted into an unreadable form.
- The message in unreadable form is called as **cipher text**.

Step-2:

- The cipher text is sent to the receiver over the communication channel.
- Since the message is encrypted, the attackers can not read the message.

Step-3:

At receiver side,

- Using a decryption algorithm, the message is again converted into the readable form.
- Then, receiver can read the message.

Cryptography Techniques

Cryptography techniques may be classified as:

Symmetric Key Cryptography

1. Asymmetric Key Cryptography

Advantages and Disadvantages of Cryptography

Rahul Publications

Advantages

- Some techniques such as hashing, are known to preserve the integrity of the message.
- It is used to guard highly confidential information and data.
- It offers protection from users not intended to have access to a message.
- Digital signatures provide non-repudiation against disputes that arise in situations where the sender denies passing of the message.

Disadvantages

- It can prove to be dangerous if the system design is not properly managed.
- Sometimes, a strongly encrypted message cannot be read by even the intended or legitimate user. This has been known to happen in many cases.
- The whole concept of cryptography relies on the complexity of mathematical algorithms. What if someone breaks through the complex algorithms, the entire cryptosystem would be vulnerable to threats.

Types of Attacks in Cryptography

There are two types of cryptography attacks, passive and active attacks.

1. Passive

In a passive attack, the intruder can only see the private data but can hardly make any changes to it or alter it. Passive attacks are more dangerous because the intruder only sees the message without altering it. Then no one will ever know that an attack is taking place, and their hidden messages will no longer be hidden.

- **Snooping:** Also known as message content leakage, snooping is a nonaggressive attack where the intruder can only read a message. This jeopardizes the security goal of confidentiality.

2. Active

In this type of attack, the intruder can alter the private data.

- **Masquerade:** The intruder will try to gain as much access to the computer system as possible. Masquerade is an active attack that threatens the security goal of credibility.
- **Brute force attack:** A brute force attack occurs when hackers use computers to feedback loop over each letter in a character set systematically. A character set can consist of letters, numbers, symbols, or anything else that the hackers may desire. In the most general terms, a brute force attack is a method of trial and error that attempts all possible password combinations. This method works well for short passwords, but it takes a long time to try all possible passwords.
- **Dictionary attack:** It is a quick and easy password attack. Hackers generate thousands of candidate digests and their pre-matched plaintext passwords using a dictionary. These candidate digits are compared to those in a stolen digest file by hackers. If a match is found, they are given the password. Although this method appears to be feasible if done manually, computers are capable of processing millions of words in a matter of hours.

Rahul Publications

4.2 Symmetric key Cryptography

Q2. Explain about Symmetric key Cryptography.

Ans :

In this technique,

- Both sender and receiver uses a common key to encrypt and decrypt the message.
- This secret key is known only to the sender and to the receiver.
- It is also called as secret key cryptography.

Working

The message exchange using symmetric key cryptography involves the following steps:

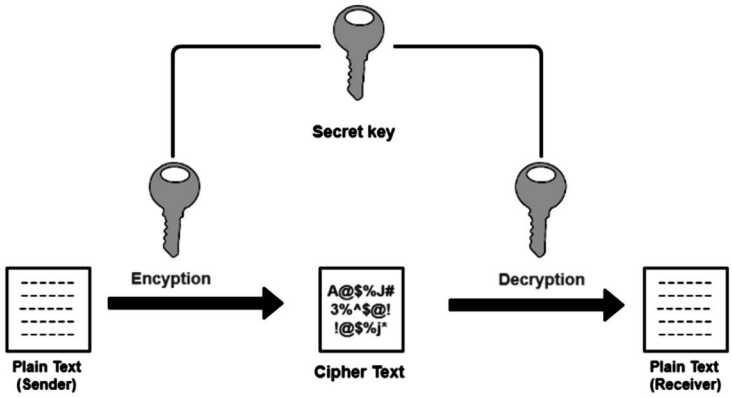


Fig.: Symmetric key Cryptography

- Before starting the communication, sender and receiver shares the secret key.
- This secret key is shared through some external means.
- At sender side, sender encrypts the message using his copy of the key.
- The cipher text is then sent to the receiver over the communication channel.
- At receiver side, receiver decrypts the cipher text using his copy of the key.
- After decryption, the message converts back into readable format.

In symmetric key cryptography,

- Both sender and receiver uses the same key.
- Sender encrypts the message using his copy of the key.
- Receiver decrypts the message using his copy of the key.
- The key must not be known to anyone else other than sender and receiver.
- If the secret key is known to any intruder, he could decrypt the message.

Point-2:

- This cryptography technique is called as symmetric key cryptography.
- It is because both sender and receiver use the same key on their sides.

Point-3:

- This cryptography technique is called as secret key cryptography.
- It is because the key has to be kept secret between the sender and receiver.

Q3. What are symmetric encryption algorithms? Explain AES algorithm.

Ans :

Symmetric Encryption Algorithms

Some of the encryption algorithms that use symmetric key are:

- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)

Advantages

The advantages of symmetric key algorithms are:

- They are efficient.
- They take less time to encrypt and decrypt the message.

Disadvantages

In symmetric key cryptography,

- Each pair of users require a unique secret key.
- If N people in the world wants to use this technique, then there needs to be N(N-1) / 2 secret keys.
- For 1 million people to communicate, a half billion secret keys would be needed.
- Sharing the secret key between the sender and receiver is an important issue.
- While sharing the key, attackers might intrude.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

Working of the cipher

AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

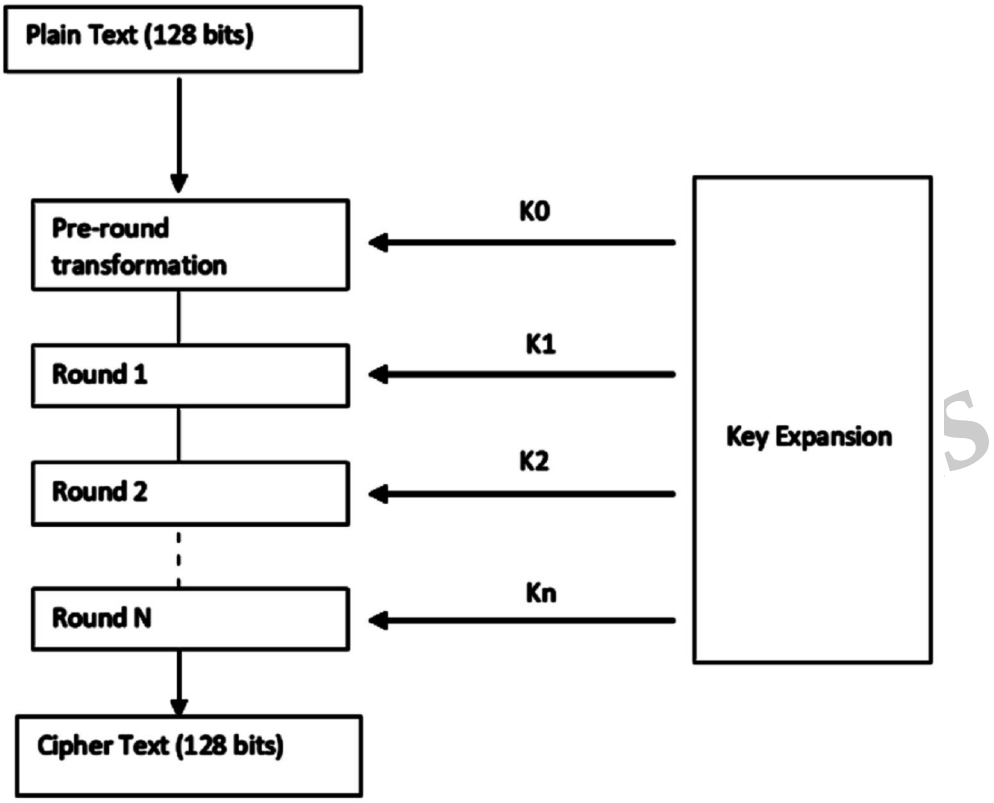
The number of rounds depends on the key length as follows :

- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds

Rahul Publications

Creation of Round keys

A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.



Encryption :

AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.

[b0 | b4 | b8 | b12 |

| b1 | b5 | b9 | b13 |

| b2 | b6 | b10| b14 |

| b3 | b7 | b11| b15]

Each round comprises of 4 steps :

1. SubBytes
2. ShiftRows
3. MixColumns
4. Add Round Key

The last round doesn't have the MixColumns round.

The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

1. SubBytes

This step implements the substitution.

In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 × 4) matrix like before.

The next two steps implement the permutation.

2. ShiftRows

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

(A left circular shift is performed.)

[b0 | b1 | b2 | b3]		[b0 | b1 | b2 | b3]
| b4 | b5 | b6 | b7 |	→	| b5 | b6 | b7 | b4 |
| b8 | b9 | b10 | b11 |		| b10 | b11 | b8 | b9 |
[b12 | b13 | b14 | b15]		[b15 | b12 | b13 | b14]

3. MixColumns

This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

This step is skipped in the last round.

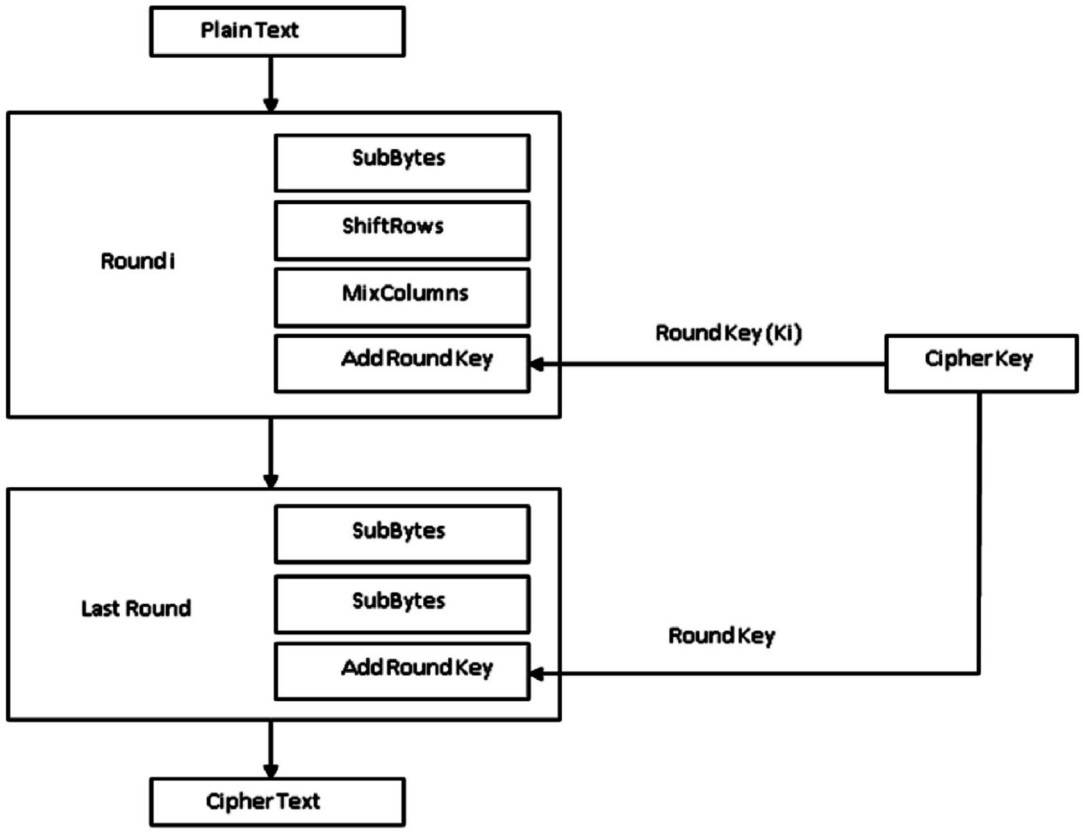
$$\begin{bmatrix} c0 \\ c1 \\ c2 \\ c3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix}$$

4. Add Round Keys

Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.

After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.

Rahul Publications



Decryption

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.

The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Inverse MixColumns

This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.

$$\begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{bmatrix} c0 \\ c1 \\ c2 \\ c3 \end{bmatrix}$$

Inverse SubBytes :

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

Q4. Explain Data Encryption Standard(DES) algorithm.

Ans : **(Imp.)**

Data Encryption Standard (DES)

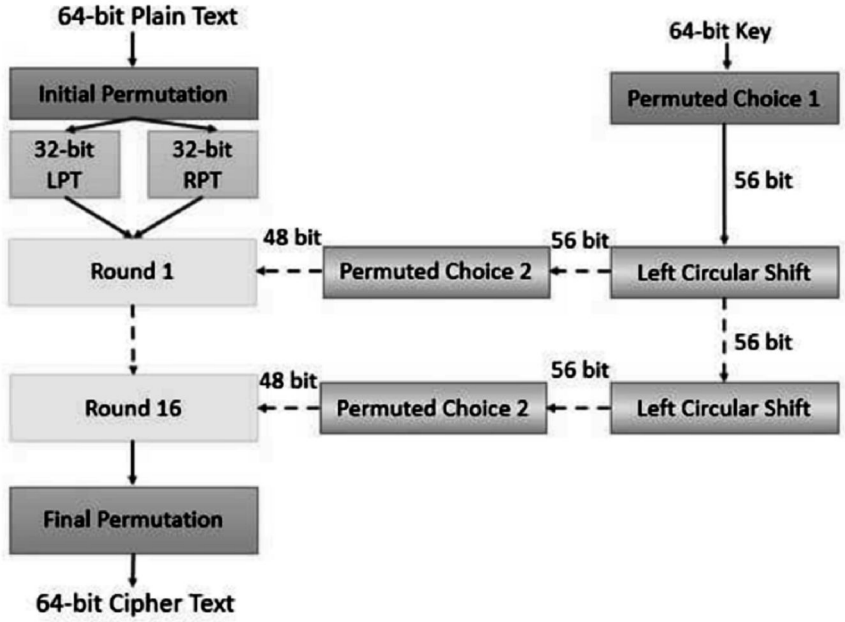
Data Encryption Standard (DES) is the symmetric block cipher which encrypts a 64-bit plain text in a 64-bit ciphertext.

The DES was introduced by the National Institute of Standard and Technology (NIST) in the 1970s. Initially, DES was only used in financial applications but later it was accepted as the cryptographic algorithm by other organizations too.

Being a symmetric cipher the same key is used in encryption and decryption process of DES. In this context, we will discuss the steps performed in DES and we will also discuss the advantages and disadvantages of DES.

DES Definition

Data Encryption Standard is a symmetric block cipher which takes the input of 64-bit plain text along with 64-bit key and process it, to generate the 64-bit ciphertext. The diagram below illustrates the working of DES. We will discuss its step in brief.



Data Encryption Standard (DES)

Encryption

Step 1:

In the first step the 64-bit plain text undergoes initial permutation which rearranges the bits to produce two 32-bit permuted block which is called left plain text (LPT 32-bit) and right plain text (RPT 32-bit).

Step 2:

Now, 16 rounds of DES encryption will be performed on this LPT and RPT with a 56-bit key.

Step 3:

After the 16_{th} round the 32-bit LPT and 32-bit RPT are integrated which forms a 64-bit block again and then the final permutation is applied to this 64-bit block, to obtain the 64-bit ciphertext.

Rounds in Data Encryption Standard

Now, we will discuss the process that takes place during the 16 rounds of DES algorithm. Each round of DES performs the same function. So, below are the steps of the function performed in each round of DES algorithm:

1. Key Transformation
2. Expansion Permutation
3. S-box Substitution
4. P-box Permutation
5. XOR and Swap

1. Key Transformation

Earlier we have discussed that the initial key size is 64-bit which is reduced to the 56-bit key. This is done by discarding every 8_{th} bit from the 64-bit key. So, for each round of DES, this 56-bit key is used. In the key transformation step, this 56-bit is transformed to the 48-bit key.

The 56-bit key is split into two halves. Each half is of 28-bit. Now, a left circular shift is implemented on both the halves which shift the bits in two halves by one or two positions depending on the order of the round.

If the round number is 1, 2, 9, 16 then the left circular shift is done by one position else, if any other order number is encountered the circular shift is done by two positions

After the left circular shift both the 28-bit halves are integrated and permutation is performed on a 56-bit key. And from this permuted 56-bit key 48-bit subkey is selected. As the key transformation step involves permutation along with compression of the 56-bit key to 48-bit subkey it is also called compression permutation.

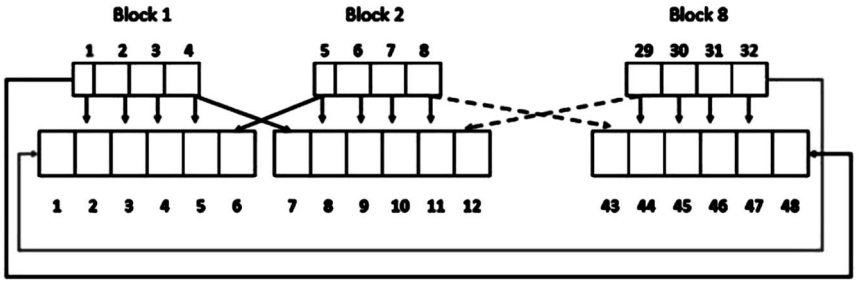
Thus, the key transformation step provides a different 48-bit subkey for each round of DES.

2. Expansion Permutation

In the first step of encryption, during the initial permutation of DES, the 64-bit plain text is permuted and we have 32-bit LPT and 32-bit RPT. Now, the expansion permutation is performed on the 32-bit RPT which transforms it from 32-bit to 48-bit. The 32-bit LPT is untouched during the process.

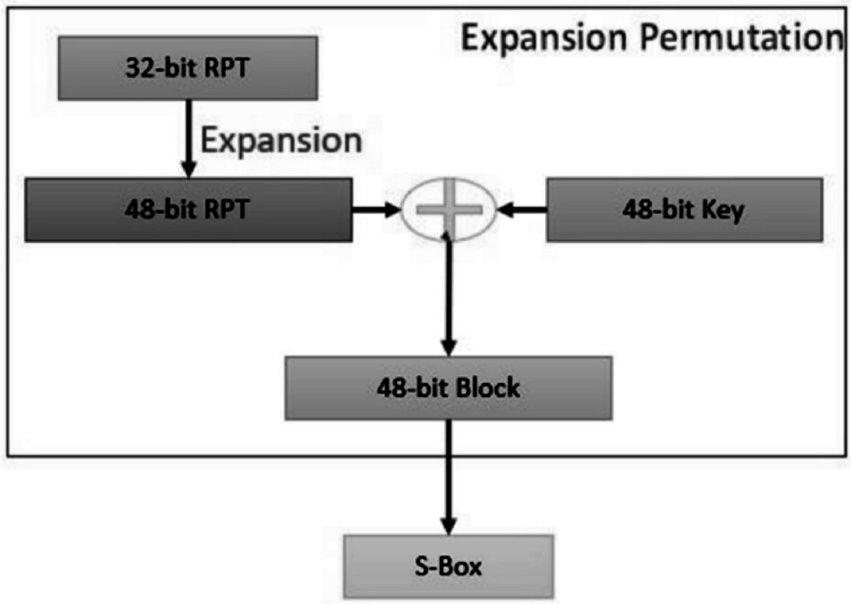
For expansion, the 32-bit RPT is divided 8 blocks, where each block is of 4-bit. Each block of 4-bit is expanded to block of 6-bit as you can see in the image below. The extreme two bits of the block are repeated and the middle two-bits is passed on as it is.

Rahul Publications



Expansion Permutation

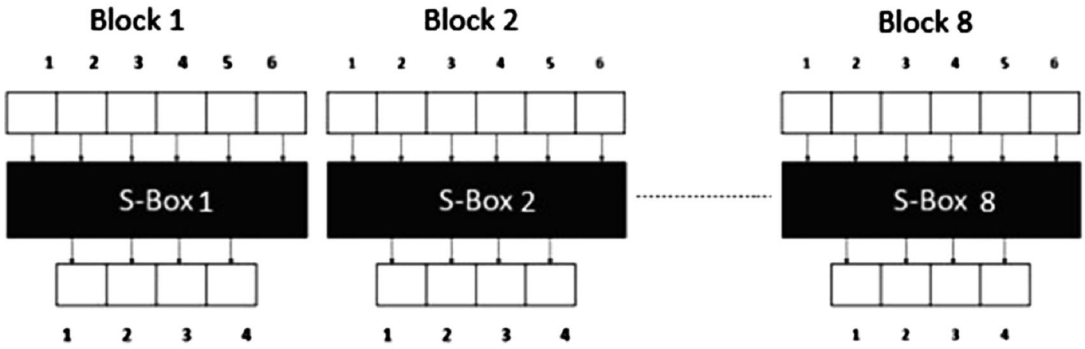
After expansion, now the 48-bit RPT is XORed with the 48-bit key and the resultant 48-bit block is transferred to S-box substitution.



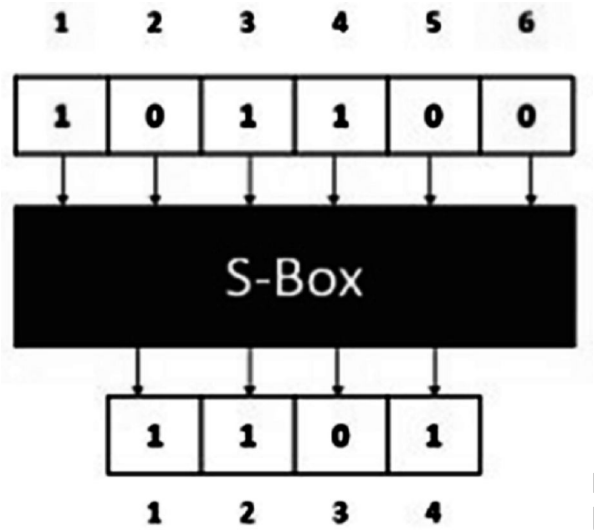
3. S-box Substitution

The input to S-box is 48-bit resultant block of expansion permutation. In S-box substitution, the input 48-bit block is transformed to 32-bit block but the question is how?

The 48-bit input block to S-box substitution is divided into 8 blocks of 6-bit each and is provided as input to 8 substitution boxes also called S-boxes. Each s-box has an input of 6-bit and its outputs 4-bit.



Each S-box is considered as the table which has 4 rows 0-3 and 16 columns i.e. 0-15. Why 4 rows and 16 columns? Because from the 6-bit input to s-box the two extreme bits are used to determine the number of rows.



2 bits can form 4 combinations of 0s and 1s:

2^2 = 4 rows

The middle 4 bits are used to determine the number of columns

4^2 = 16 columns

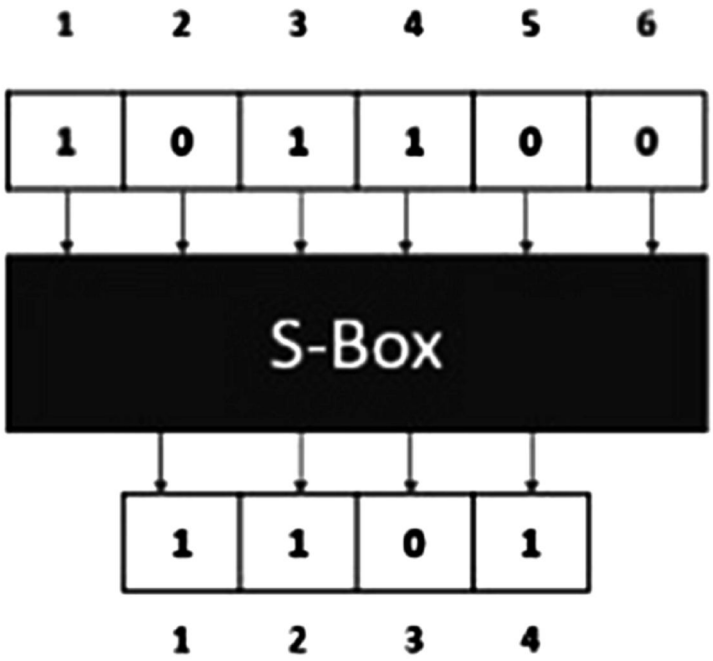
Now, we will see how the 6-bit input is transformed to the 4-bit output. For example, in the figure above you can see that input bit, at position 1 and 6 i.e. '10' that represent 2 which determines 2nd row and middle 4 bits i.e. '0110' that represent 6 which determines the 6th column of s-box. The value at the intersection of the 2nd row and 6th column will represent the 4-bit output of corresponding s-box.

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	2	6	13	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S-Box Table 1

In our example, the intersection of the 2nd row and 6th column is 13 its **4bit representation** is **1101**. So, the output of S-box 1 is 1101.

Rahul Publications



Similarly, the remaining S-boxes function will be carried out to find the remaining 4-bit outputs. In this way, the 8 s-boxes would generate 8, 4-bit output blocks which when integrated forms 32-bit output.

4. P-box Permutation

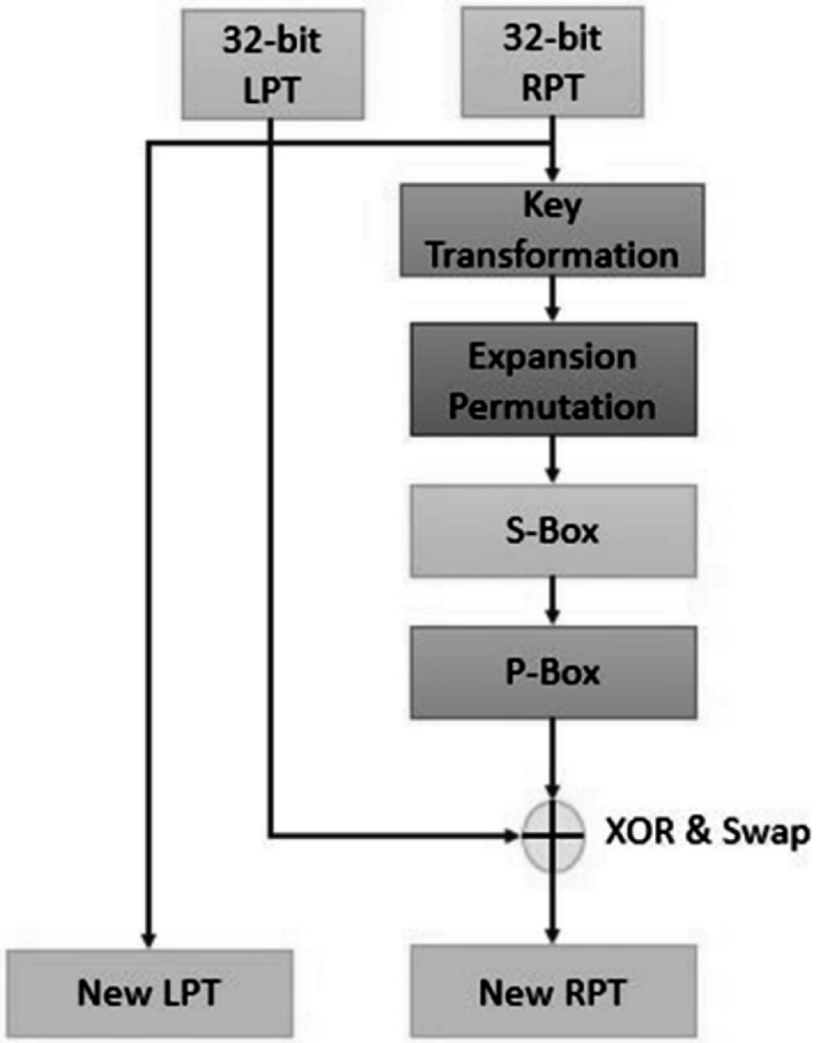
The 32-bit output obtained from s-box substitution is provided as an input to P-box. Here, the 32-bit input is simply permuted and send to the next step.

5. XOR and Swap

As you can observe so far, we have been operating on the 32-bit RPT of the initial 64-bit plain text. The 32-bit LPT is still untouched. In this step, the 32-bit LPT of the initial 64-bit plain text is **XOR** with the output of P-box permutation.

The result of the XOR is the new RPT for next round and the old RPT is swapped with LPT. S So, the old RPT is now new LPT for next round.o, the old RPT is now new LPT for next round.

Rahul Publications



So, here the process of a single round ends and next round start which has the same function.

After 16 such rounds, the output of the 16th round undergoes **final permutation**. The result of this final permutation is 64-bit ciphertext.

4.3 Asymmetric key Cryptography

Q5. Explain about the function of asymmetric key cryptography.

Ans :

When the two parties communicate to each other to transfer the intelligible or sensible message, referred to as plaintext, is converted into apparently random nonsense for security purpose referred to as ciphertext.

Encryption:

The process of changing the plaintext into the ciphertext is referred to as encryption.

The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext.

The security of conventional encryption depends on the major two factors:

1. The Encryption algorithm
2. Secrecy of the key

Once the ciphertext is produced, it may be transmitted. The Encryption algorithm will produce a different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm.

Once the ciphertext is produced, it may be transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

Decryption:

The process of changing the ciphertext to the plaintext that process is known as decryption

Public Key Encryption

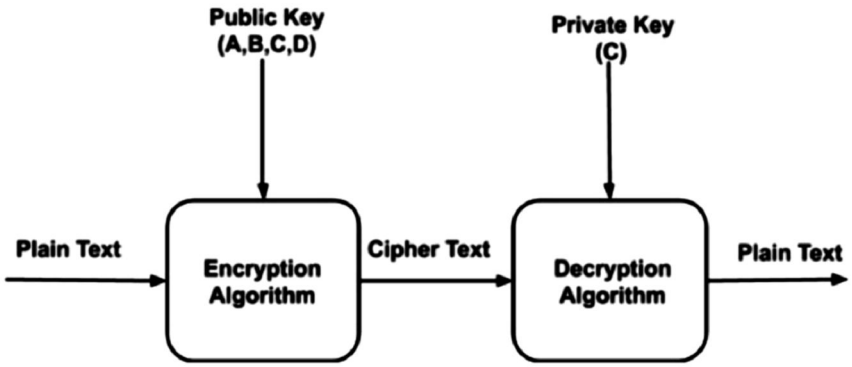
Asymmetric is a form of Cryptosystem in which encryption and decryption are performed using different keys-Public key (known to everyone) and Private key (Secret key). This is known as Public Key Encryption.

Characteristics of Public Encryption key

- Public key Encryption is important because it is infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and encryption key.
- Either of the two key (Public and Private key) can be used for encryption with other key used for decryption.
- Due to Public key cryptosystem, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.
- The most widely used public-key cryptosystem is RSA (Rivest–Shamir–Adleman). The difficulty of finding the prime factors of a composite number is the backbone of RSA.

Example:

Public keys of every user are present in the Public key Register. If B wants to send a confidential message to C, then B encrypt the message using C Public key. When C receives the message from B then C can decrypt it using its own Private key. No other recipient other than C can decrypt the message because only C know C's private key.



Rahul Publications

Components of Public Key Encryption:

- **Plain Text**

  This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.

- **Cipher Text**

  The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.

- **Encryption Algorithm**

  The encryption algorithm is used to convert plain text into cipher text.

- **Decryption Algorithm**

  It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text

- **Public and Private Key**

  One key either Private key (Secret key) or Public Key (known to everyone) is used for encryption and other is used for decryption

  Let's step through the high-level process of public key encryption.

Step 1: Key generation

Each person (or their computer) must generate a pair of keys that identifies them: a private key and a public key.

You can generate a pair below, using the same RSA algorithm that's used by your computer:

Step 2: Key exchange

The sending and receiving computers exchange *public keys* with each other via a reliable channel, like TCP/IP. The private keys are *never* exchanged.

Key exchange diagram with a laptop and a server. The laptop screen shows a browser with a password input field. An arrow goes from the server to the laptop and is labeled with "SERVER_PUBLIC_KEY". Under that, an arrow goes from the laptop to the server and is labeled with "CLIENT_PUBLIC_KEY."

Step 3: Encryption

The sending computer encrypts the secret data using the receiving computer's *public* key and a mathematical operation.

The power of public key encryption is in that mathematical operation. It's a "one-way function", which means it's incredibly difficult for a computer to reverse the operation and discover the original data. Even the public key cannot be used to decrypt the data.

Step 4: Sending encrypted data

The sender can now safely transmit the encrypted data over the Internet without worry of onlookers.

Key exchange diagram with a laptop and a server. The laptop screen shows a browser with a password input field. An arrow goes from the server to the laptop and is labeled with string of encrypted text. An attacker looks unhappily at the text.

Step 5: Decryption

Now the receiver can decrypt the message, using their *private key*. That's the only key that can be used to decrypt the message (in the world!).

Try it out below, with the encrypted message and private key from above:

Rahul Publications

Q6. Explain RSA algorithm with an example.

Ans :

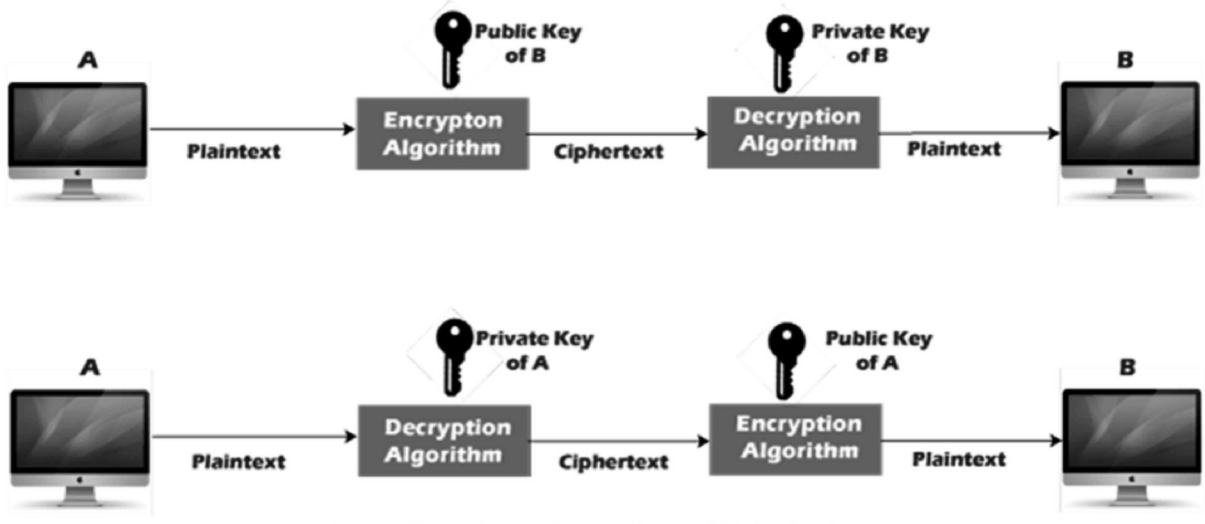
RSA Encryption Algorithm

Public Key encryption algorithm is also called the Asymmetric algorithm. Asymmetric algorithms are those algorithms in which sender and receiver use different keys for encryption and decryption. Each sender is assigned a pair of keys:

- **Public key**
- **Private key**

The Public key is used for encryption, and the Private Key is used for decryption. Decryption cannot be done using a public key. The two keys are linked, but the private key cannot be derived from the public key. The public key is well known, but the private key is secret and it is known only to the user who owns the key. It means that everybody can send a message to the user using user's public key. But only the user can decrypt the message using his private key.

The Public key algorithm operates in the following manner:

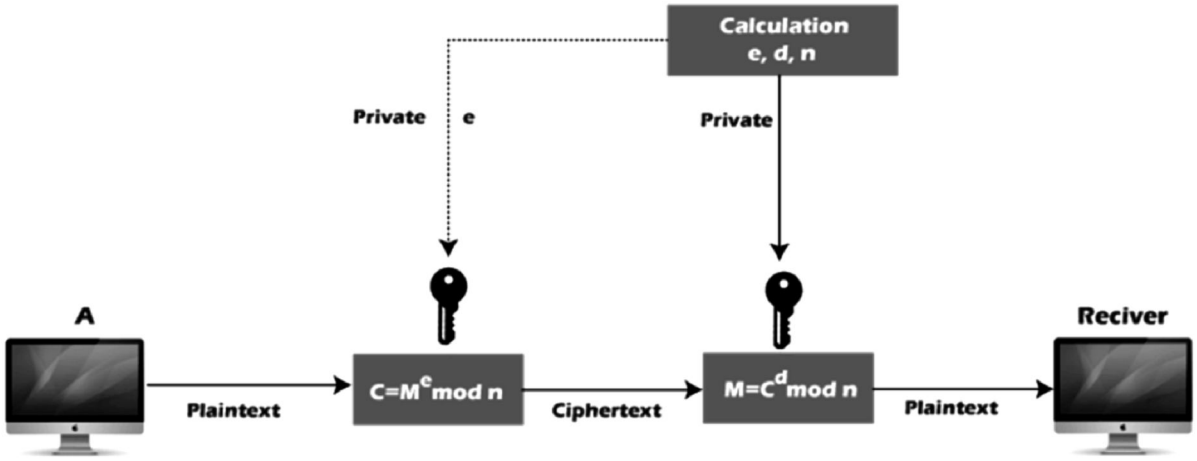


Encryption/decryption using public/private keys

- The data to be sent is encrypted by sender A using the public key of the intended receiver
- B decrypts the received ciphertext using its private key, which is known only to B. B replies to A encrypting its message using A's public key.
- A decrypts the received ciphertext using its private key, which is known only to him.

RSA encryption algorithm:

RSA is the most common public-key algorithm, named after its inventors Rivest, Shamir, and Adelman (RSA).



RSA

RSA algorithm uses the following procedure to generate public and private keys:

- Select two large prime numbers, p and q.
- Multiply these numbers to find n = p x q, where n is called the modulus for encryption and decryption.
- Choose a number *e* less than n, such that n is relatively prime to (p - 1) x (q -1). It means that *e* and (p - 1) x (q - 1) have no common factor except 1. Choose "*e*" such that 1<*e* < ö (n), e is prime to φ (n),gcd (e,d(n)) =1
- If n = p x q, then the public key is <*e*, n>. A plaintext message m is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.

  $C = m^e \mod n$

  Here, m must be less than n. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
- To determine the private key, we use the following formula to calculate the d such that:

  $D_e \mod \{(p - 1) \times (q - 1)\} = 1$

  Or

  $D_e \mod \varphi(n) = 1$
- The private key is <d, n>. A ciphertext message c is decrypted using private key <d, n>. To calculate plain text m from the ciphertext c following formula is used to get plain text m.

  $m = c^d \mod n$

  Let's take some example of RSA encryption algorithm:

Example 1:

This example shows how we can encrypt plaintext 9 using the RSA public-key encryption algorithm. This example uses prime numbers 7 and 11 to generate the public and private keys.

Explanation:

Step 1:

Select two large prime numbers, p, and q.

p = 7

q = 11

Rahul Publications

Step 2:

Multiply these numbers to find n = p x q, where n is called the modulus for encryption and decryption.

First, we calculate

n = p x q

n = 7 x 11

n = 77

Step 3:

Choose a number e less that n, such that n is relatively prime to (p – 1) × (q – 1). It means that e and (p – 1) x (q – 1) have no common factor except 1. Choose "e" such that $1<e < \varphi$ (n), e is prime to φ (n), gcd (e, d (n)) =1.

Second, we calculate

φ (n) = (p – 1) × (q – 1)

φ (n) = (7 – 1) × (11 – 1)

φ (n) = 6 x 10

φ (n) = 60

Let us now choose relative prime e of 60 as 7.

Thus the public key is <e, n> = (7, 77)

Step 4:

A plaintext message m is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.

To find ciphertext from the plain text following formula is used to get ciphertext C.

$C = m^e \mod n$

$C = 9^7 \mod 77$

C = 37

Step 5:

The private key is <d, n>. To determine the private key, we use the following formula d such that:

$D_e \mod \{(p - 1) \times (q - 1)\} = 1$

7d mod 60 = 1, which gives d = 43

The private key is <d, n> = (43, 77)

Step 6:

A ciphertext message c is decrypted using private key <d, n>. To calculate plain text m from the ciphertext c following formula is used to get plain text m.

$m = c^d \mod n$

$m = 37^{43} \mod 77$

m = 9

In this example, Plain text = 9 and the ciphertext = 37

Rahul Publications

Example 2:

In an RSA cryptosystem, a particular A uses two prime numbers, 13 and 17, to generate the public and private keys. If the public of A is 35. Then the private key of A is ……?.

Explanation:

Step 1:

in the first step, select two large prime numbers, p and q.

p = 13

q = 17

Step 2:

Multiply these numbers to find n = p x q, where n is called the modulus for encryption and decryption.

First, we calculate

n = p x q

n = 13 x 17

n = 221

Step 3:

Choose a number e less that n, such that n is relatively prime to (p – 1) × (q – 1). It means that e and (p – 1) × (q – 1) have no common factor except 1. Choose "e" such that $1<e<\varphi(n)$, e is prime to ö (n), gcd (e, .d (n)) =1.

Second, we calculate

$\varphi(n) = (p - 1) \times (q - 1)$

$\varphi(n) = (13 - 1) \times (17 - 1)$

$\varphi(n) = 12 \times 16$

$\varphi(n) = 192$

g.c.d (35, 192) = 1

Step 3:

To determine the private key, we use the following formula to calculate the d such that:

Calculate $d = d_e \bmod \varphi(n) = 1$

$d = d \times 35 \bmod 192 = 1$

$d = (1 + k.\varphi(n))/e$ [let k = 0, 1, 2, 3……]

Put k = 0

$d = (1 + 0 \times 192)/35$

d = 1/35

Put k = 1

$d = (1 + 1 \times 192)/35$

d = 193/35

Rahul Publications

Put k = 2

d = (1 + 2 x 192)/35

d = 385/35

d = 11

The private key is <d, n> = (11, 221)

Hence, private key i.e. d = 11

4.4 MESSAGE AUTHENTICATION

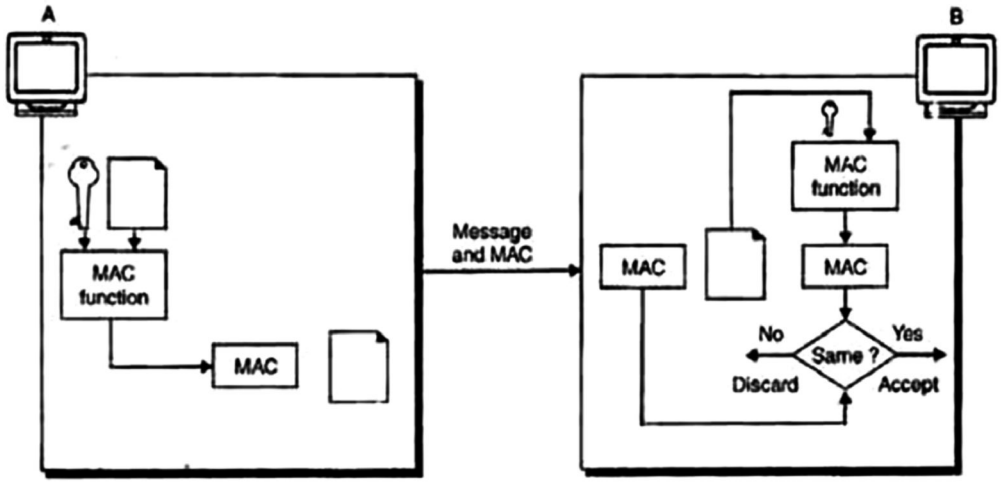
Q7. Explain about Message Authentication service.

Ans :

Message authentication ensures that the message has been sent by a genuine identity and not by an imposter.

- The service used to provide message authentication is a Message Authentication Code (MAC).
- A MAC uses a keyed hash function that includes the symmetric key between the sender and receiver when creating the digest.
- Figure shows how a sender A uses a keyed hash function to authenticate his message and how the receiver B can verify the authenticity of the message.
- This system makes use of a symmetric key shared by A and B.
- A, using this symmetric key and a keyed hash function, generates a MAC.
- A then sends this MAC along with the original message to B.

  B receives the message and the MAC and separates the message from the MAC.
- B then applies the same keyed hash function to the message using the same symmetric key to get a fresh MAC.
- B then compares the MAC sent by A with the newly generated MAC.
- If the two MACs are identical, it shows that the message has not been modified and the sender of the message is definitely A.



MAC created by A and checked by B.

Rahul Publications

4.5 DIGITAL SIGNATURES

Q8. What is digital signature? Explain about it.

Ans :

Meaning

A digital signature is a mathematical technique which validates the authenticity and integrity of a message, software or digital documents. It allows us to verify the author name, date and time of signatures, and authenticate the message contents. The digital signature offers far more inherent security and intended to solve the problem of tampering and impersonation (Intentionally copy another person's characteristics) in digital communications.

The computer-based business information authentication interrelates both technology and the law. It also calls for cooperation between the people of different professional backgrounds and areas of expertise. The digital signatures are different from other electronic signatures not only in terms of process and result, but also it makes digital signatures more serviceable for legal purposes. Some electronic signatures that legally recognizable as signatures may not be secure as digital signatures and may lead to uncertainty and disputes.

Application

The important reason to implement digital signature to communication is:

- Authentication
- Non-repudiation
- Integrity

- **Authentication**

  Authentication is a process which verifies the identity of a user who wants to access the system. In the digital signature, authentication helps to authenticate the sources of messages.

- **Non-repudiation**

  Non-repudiation means assurance of something that cannot be denied. It ensures that someone to a contract or communication cannot later deny the authenticity of their signature on a document or in a file or the sending of a message that they originated.

- **Integrity**

  Integrity ensures that the message is real, accurate and safeguards from unauthorized user modification during the transmission.

Algorithms in Digital Signature

A digital signature consists of three algorithms:

1. Key generation algorithm

The key generation algorithm selects private key randomly from a set of possible private keys. This algorithm provides the private key and its corresponding public key.

2. Signing algorithm

A signing algorithm produces a signature for the document.

3. Signature verifying algorithm

A signature verifying algorithm either accepts or rejects the document's authenticity.

Rahul Publications

How digital signatures work

Digital signatures are created and verified by using public key cryptography, also known as asymmetric cryptography. By the use of a public key algorithm, such as RSA, one can generate two keys that are mathematically linked- one is a private key, and another is a public key.

The user who is creating the digital signature uses their own private key to encrypt the signature-related document. There is only one way to decrypt that document is with the use of signer's public key.

This technology requires all the parties to trust that the individual who creates the signature has been able to keep their private key secret. If someone has access the signer's private key, there is a possibility that they could create fraudulent signatures in the name of the private key holder.

The steps which are followed in creating a digital signature are:

1. Select a file to be digitally signed.
2. The hash value of the message or file content is calculated. This message or file content is encrypted by using a private key of a sender to form the digital signature.
3. Now, the original message or file content along with the digital signature is transmitted.
4. The receiver decrypts the digital signature by using a public key of a sender.
5. The receiver now has the message or file content and can compute it.
6. Comparing these computed message or file content with the original computed message. The comparison needs to be the same for ensuring integrity.

Types of Digital Signature

Different document processing platform supports different types of digital signature. They are described below:

- **Certified Signatures**

  The certified digital signature documents display a unique blue ribbon across the top of the document. The certified signature contains the name of the document signer and the certificate issuer which indicate the authorship and authenticity of the document.

- **Approval Signatures**

  The approval digital signatures on a document can be used in the organization's business workflow. They help to optimize the organization's approval procedure. The procedure involves capturing approvals made by us and other individuals and embedding them within the PDF document. The approval signatures to include details such as an image of our physical signature, location, date, and official seal.

- **Visible Digital Signature**

  The visible digital signature allows a user to sign a single document digitally. This signature appears on a document in the same way as signatures are signed on a physical document.

- **Invisible Digital Signature**

  The invisible digital signatures carry a visual indication of a blue ribbon within a document in the taskbar. We can use invisible digital signatures when we do not have or do not want to display our signature but need to provide the authenticity of the document, its integrity, and its origin.

Rahul Publications

4.6 Applications of Cryptography

Q9. Write about applications of cryptography.

Ans :

1. Digital Currency

A much-known application of cryptography is digital currency wherein cryptocurrencies are traded over the internet. Top cryptocurrencies like Bitcoin, Ethereum, and Ripple have been developed and traded over time.

With cashless economies emerging, digital currencies have grabbed the attention of the world. Unregulated by any government or banks, cryptocurrencies are our upcoming future.

Blockchain technology has a lot to do with this application. Several nodes in the blockchain are empowered with cryptography that enables the secure trade of a cryptocurrency in a digital ledger system.

These ledgers are protected, preserved, and cannot be accessed by any other person or organization.

2. E-commerce

With the current pandemic shackling us to our homes, the rise of e-commerce has been tremendous. Well, who wouldn't like to enjoy the comfort of shopping in your living room and receiving your hampers the next morning?

However, there's something we should know about e-commerce in order to understand how it works. E-commerce startups enable us to shop items online and pay for them online.

These transactions are encrypted and perhaps cannot be altered by any third party. Moreover, the passwords we set for such sites are also protected under keys to ensure that no hacker gets access to our e-commerce details for harmful purposes.

3. Military Operations

The applications of cryptography in the military are well-known. Military operations have also derived great use from cryptography for a long time. Used for encrypting military communication channels, military encryption devices convert the real communication characters so that the enemies cannot come to know about their upcoming plans.

Simply put, cryptography safely transmits messages from one end to the other without letting the enemy forces intercept the real meaning. This is a very important application of cryptology as it can be of both public and private use.

On the large scale, it can be widely used for declaring wars and sending crucial messages without the involvement of a messenger. Unlike traditional times, this technology can be precisely used to enhance the military strength of a nation.

4.7 Overview of Firewalls-Types of Firewalls

Q10. What is a Firewall? Explain about the types of firewalls.

Ans : **(Imp.)**

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Rahul Publications

Software Firewalls

Software firewalls are installed separately on individual devices. They provide more granular control to allow access to one application or feature while blocking others. But they can be expensive in terms of resources since they utilize the CPU and RAM of the devices they are installed on, and administrators must configure and manage them individually for each device. Additionally, all devices within an intranet may not be compatible with a single software firewall, and several different firewalls may be required.

Hardware Firewalls

On the other hand, hardware firewalls are physical devices, each with its computing resources. They act as gateways between internal networks and the internet, keeping data packets and traffic requests from untrusted sources outside the private network. Physical firewalls are convenient for organizations with many devices on the same network. While they block malicious traffic well before it reaches any endpoints, they do not provide security against insider attacks. Therefore, a combination of software and hardware firewalls can provide optimal protection to your organization's network.

Types of Firewall

Besides, there are many other types of firewalls depending on their features and the level of security they provide. The following are types of firewall techniques that can be implemented as software or hardware:

1. Packet-filtering Firewalls
2. Circuit-level Gateways
3. Application-level Gateways (Proxy Firewalls)
4. Stateful Multi-layer Inspection (SMLI) Firewalls
5. Next-generation Firewalls (NGFW)
6. Threat-focused NGFW
7. Network Address Translation (NAT) Firewalls
8. Cloud Firewalls
9. Unified Threat Management (UTM) Firewalls

1. Packet-filtering Firewalls

A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules. These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.

While packet-filtering firewalls can be considered a fast solution without many resource requirements, they also have some limitations. Because these types of firewalls do not prevent web-based attacks, they are not the safest.

2. Circuit-level Gateways

Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources. These types of firewalls typically operate at the session-level of the OSI model by verifying

TCP (Transmission Control Protocol)connections and sessions. Circuit-level gateways are designed to ensure that the established sessions are protected.

Rahul Publications

Typically, circuit-level firewalls are implemented as security software or pre-existing firewalls. Like packet-filtering firewalls, these firewalls do not check for actual data, although they inspect information about transactions. Therefore, if a data contains malware, but follows the correct TCP connection, it will pass through the gateway. That is why circuit-level gateways are not considered safe enough to protect our systems.

3. Application-level Gateways (Proxy Firewalls)

Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called 'Application-level Gateways'.

Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks. Once the connection is established, the proxy firewall inspects data packets coming from the source. If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client. This approach creates an additional layer of security between the client and many different sources on the network.

4. Stateful Multi-layer Inspection (SMLI) Firewalls

Stateful multi-layer inspection firewalls include both packet inspection technology and TCP handshake verification, making SMLI firewalls superior to packet-filtering firewalls or circuit-level gateways. Additionally, these types of firewalls keep track of the status of established connections.

In simple words, when a user establishes a connection and requests data, the SMLI firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc. Connection information is stored for each session in the state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.

5. Next-generation Firewalls (NGFW)

Many of the latest released firewalls are usually defined as 'next-generation firewalls'. However, there is no specific definition for next-generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include deep-packet inspection (DPI), surface-level packet inspection, and TCP handshake testing, etc.

NGFW includes higher levels of security than packet-filtering and stateful inspection firewalls. Unlike traditional firewalls, NGFW monitors the entire transaction of data, including packet headers, packet contents, and sources. NGFWs are designed in such a way that they can prevent more sophisticated and evolving security threats such as malware attacks, external threats, and advance intrusion.

6. Threat-focused NGFW

Threat-focused NGFW includes all the features of a traditional NGFW. Additionally, they also provide advanced threat detection and remediation. These types of firewalls are capable of reacting against attacks quickly. With intelligent security automation, threat-focused NGFW set security rules and policies, further increasing the security of the overall defense system.

In addition, these firewalls use retrospective security systems to monitor suspicious activities continuously. They keep analyzing the behavior of every activity even after the initial inspection. Due to this functionality, threat-focus NGFW dramatically reduces the overall time taken from threat detection to cleanup.

Rahul Publications

7. Network Address Translation (NAT) Firewalls

Network address translation or NAT firewalls are primarily designed to access Internet traffic and block all unwanted connections. These types of firewalls usually hide the IP addresses of our devices, making it safe from attackers.

When multiple devices are used to connect to the Internet, NAT firewalls create a unique IP address and hide individual devices' IP addresses. As a result, a single IP address is used for all devices. By doing this, NAT firewalls secure independent network addresses from attackers scanning a network for accessing IP addresses. This results in enhanced protection against suspicious activities and attacks.

In general, NAT firewalls works similarly to proxy firewalls. Like proxy firewalls, NAT firewalls also work as an intermediate device between a group of computers and external traffic.

8. Cloud Firewalls

Whenever a firewall is designed using a cloud solution, it is known as a cloud firewall or FaaS (firewall-as-service). Cloud firewalls are typically maintained and run on the Internet by third-party vendors. This type of firewall is considered similar to a proxy firewall. The reason for this is the use of cloud firewalls as proxy servers. However, they are configured based on requirements.

The most significant advantage of cloud firewalls is scalability. Because cloud firewalls have no physical resources, they are easy to scale according to the organization's demand or traffic-load. If demand increases, additional capacity can be added to the cloud server to filter out the additional traffic load. Most organizations use cloud firewalls to secure their internal networks or entire cloud infrastructure.

9. Unified Threat Management (UTM) Firewalls

UTM firewalls are a special type of device that includes features of a stateful inspection firewall with anti-virus and intrusion prevention support. Such firewalls are designed to provide simplicity and ease of use. These firewalls can also add many other services, such as cloud management, etc.

4.8 User Management

Q11. What is firewall management? Explain about firewall user authentication.

Ans :

Firewall management is the process of configuring and monitoring a firewall to maintain a secure network. Firewalls are an integral part of protecting private networks in both a personal and business setting.

An organization may have many different firewalls protecting its devices and network as standard. Management of these firewalls means setting rules and policies, tracking changes, and monitoring compliance logs. It also includes the monitoring of user access to firewall settings. The configuration ensures the firewall functions securely and efficiently.

Any size organization which has a private network will utilize a firewall to protect their systems. This could be a large contractor subject to Cybersecurity Maturity Model Certification (CMMC) or a small office-based network. Firewalls are an important aspect of cybersecurity, so form a key area of IT security policies. The final responsibility for firewall management is held by those leading the organization's IT security or compliance efforts.

Firewall User Authentication

Various authentication techniques can be supported by a firewall. In its most basic form, authentication

Rahul Publications

means that a user is claiming to be who they say they are and is granted access to the resources for which they are authenticating.

This is similar to how we prove our identity when we connect into our Microsoft Windows computer and tell Windows who we are by entering our username and then our password. Finally, Windows restricts our access to only those resources to which we have permission.

Various functionalities can employ firewall authentication. SSL VPN and web filtering are two of the most prevalent applications.

The following are some of the most frequent authentication methods supported by most firewalls:

Database authentication is built-in.

A firewall with a built-in authentication database has a built-in authentication database. Multiple users and passwords are frequently set up in the database.

The use of built-in database authentication is simple to set up and very effective, but it is not scalable. And the database must be updated on frequent basis in order to keep the record of the users and there authentication.

Certificate authentication

For firewall authentication, most firewalls allow us to utilize either a public signed certificate or a self-signed certificate. There are certain public identifiable certificate to authenticate the anonymous users. If the firewall is open for all to use, then it must be configured accordingly.

A publicly recognized certificate is one that is issued by a company like VeriSign, GoDaddy, or Thawte and is recognized by popular browsers like Internet Explorer and Mozilla Firefox, making it instantly trustworthy.

The firewall provider can freely issue a self-signed certificate, and because we have control over the clients, we can install the certificate on their browsers.

Using Active Directory group policy or something similar, we can deliver certificates to a large number of client systems at once.

SSL VPN users are a common use case here. Because SSL VPN is a safe browser-based tool, we can utilize self-signed certificates to avoid the error message "This website's security certificate was not issued by a trustworthy certificate authority."

LDAP authentication

We can query and authenticate against our directory server using the Lightweight Directory Access Protocol (LDAP). Active Directory is the most common example, however any directory service that supports LDAP, such as Novell Directory Open LDAP, and others, can also be used.

A more scalable method is to keep the record in the directory up to date. Because if the local firewall is querying the directory server, we don't need to update it. But if the query is made through any other server, then directory must be updated for it to perform the query.

Two Factor Authentications

Two-factor authentication means that we must authenticate with two separate factors before being granted access. It usually takes the form of a combination of something we know (password) and something we have (key) (software or hardware token). It could possibly be something we're interested in (finger print).

Configuring our firewall to require authentication using both a hardware token and our personal password is a standard way. We will not be permitted access unless we have a combination of the two.

Rahul Publications

This provides significantly more security than simply using a single password. And even after all the security if our password is stolen and used by someone else or lost and we are afraid that the person who has stolen the password can hard the organisation using the network. Then in this case one can use two-factor authentication and there are some famous manufacturers, such as RSA, CryptoCard, and others, which can be easily integrated with most firewalls in order to provide full security.

Single sign on

A single sign on method ensures that a user is transparently authenticated to a firewall or a network even without having to actively log in.

A firewall agent queries Active Directory for information and transmits it to the firewall when a user logs into the network.

As a result, when a user challenges a policy that requires authentication, the firewall recognizes that the person is already logged in to the network.

Because of which the user is automatically authorized even without asking for the login password.

We can build a policy that requires users to authenticate themselves using one of two most common authentication techniques after we define firewall users:

Pass-through authentication

This type of authentication occurs when a host or user from one zone attempts to access resources in a different zone. In order to access the IP address of the protected resource and be authorized by the firewall, we must use an HTTP client, FTP client, a Telnet client or an HTTPS client.

The device collects username and password information via FTP, Telnet, HTTP, or HTTPS, and future traffic from the user or host is allowed or refused based on the result of this authentication. If the authentication is not successful, following communications from the user is always terminated when the device is utilizing an HTTPS server and it will only pass through after the authentication is completed.

Web-redirect authentication with pass-through

For HTTP or HTTPS client requests, we use this authentication mechanism. We can use the web-redirect functionality to direct user queries to the device's internal webserver when we setup firewall authentication to use pass-through authentication for HTTP and HTTPs client requests.

The redirect response is provided to the same interface that the client's request is received on.

This feature enables for a more personalized user login experience. In this feature the users are directly redirected to the login page where he will fill his credentials and login simply, instead of popup prompt asking for the login credentials. When we enable web-redirect, it's as though the user input the web authentication IP address into a client browser.

So, this is the mechanism behind the logic that how web-redirect delivers a seamless authentication experience. Where the user only has to know the IP address of the resource they want to access. And even there is no need for the user to know the IP address of the web authentication provider.

4.9 VPN SECURITY

Q12. What is VPN? Explain about VPN security.

Ans : **(Imp.)**

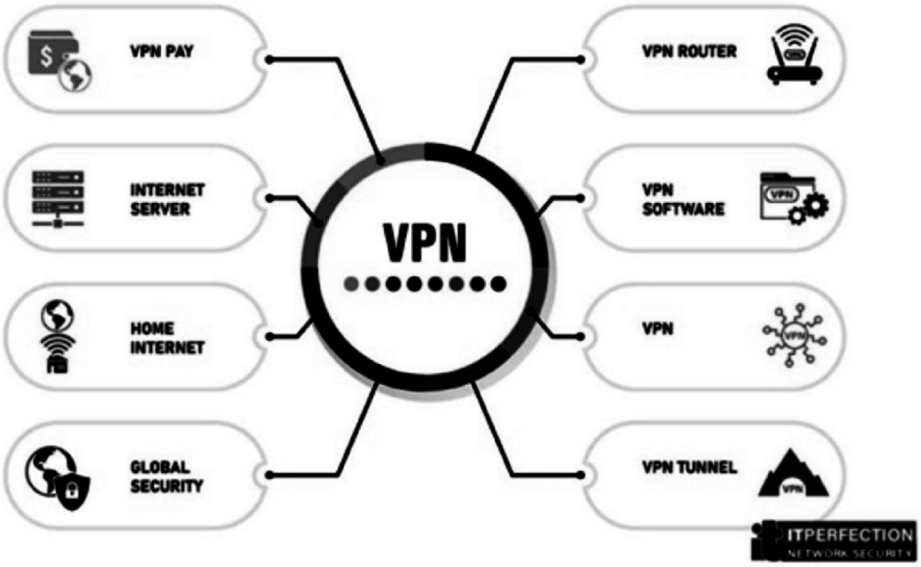
VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.

Rahul Publications

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. In other words, A Virtual Private Network is a connection method used to add security and privacy to private and public networks.

In very simple terms, a virtual private network connects your PC, smartphone, or tablet to another computer (called a server) somewhere on the internet, and allows you to browse the internet using that computer's internet connection.

A virtual private network is commonly used to secure connection to public Wi-FI hotspot, hide IP address and make your browsing private. For security, the private network connection may be established using an encrypted layered tunneling protocol, and users may be required to pass various authentication methods to gain access to the virtual private network.



So, the encryption and anonymity that a virtual private network provides helps protect your online activities:

- Sending emails
- Access Geo-Blocked websites
- Shopping online
- Access a business network while traveling
- Web browsing anonymously
- Downloading files by torrent

VPNs use encryption to scramble data when it's sent over an internet connection. Encryption makes the data unreadable. Data security is especially important when using a public Wi-Fi network, because it prevents anyone else on the network from eavesdropping on your internet activity.

Privacy is very important for us. Without a VPN, your internet service provider can know your entire browsing history. With a virtual private network, your search history is hidden. That's because your web activity will be associated with the VPN server's IP address, not yours. A virtual private network service provider may have servers all over the world. That means your search activity could appear to originate at any one of them.

A virtual private network can hide a lot of information that can put your privacy at risk:

1. Web browsing history
2. IP address and location
3. Location for streaming
4. Device type and device information
5. Web activity to maintain internet freedom

Security

VPNs use advanced encryption protocols and secure tunneling techniques to encapsulate all online data transfers. Evolving security threats and ever increasing reliance on the Internet make a Virtual Private Network an essential part of well-rounded security. Integrity checks ensure no lost data and the connection not hijacked. To prevent disclosure of private information, virtual private networks typically allow only authenticated remote access using tunneling protocols and encryption techniques.

The VPN security model provides:

- **Confidentiality**: Even if the network traffic is sniffed at the packet level, an attacker would see only encrypted data sender authentication to prevent unauthorized users from accessing the VPN message integrity to detect any instances of tampering with transmitted messages.
- **Authentication**: Tunnel endpoints must be authenticated before secure VPN tunnels can be established. User-created remote-access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods.

Secure VPN protocols include the following:

- **IPsec**: This protocol uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination. Read more here about IPsec.
- **SSL/TLS**: These protocols can tunnel an entire network's traffic or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules. Read more here about SSL/TLS.
- **Datagram Transport Layer Security (DTLS)**: This protocol used in Cisco AnyConnect VPN and in OpenConnect VPN to solve the issues SSL/TLS has with tunneling over TCP.
- **Microsoft Point-to-Point Encryption (MPPE)**: This protocol works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- **Microsoft Secure Socket Tunneling Protocol (SSTP)**: this protocol tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL/TLS channel.
- **Secure Shell (SSH) VPN**: OpenSSH offers VPN tunneling to secure remote connections to a network or to inter-network links. OpenSSH server provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.
- **WireGuard**: This new protocol supports was added to both the Linux and Android kernels, opening it up to adoption by VPN providers.

Site-to-site

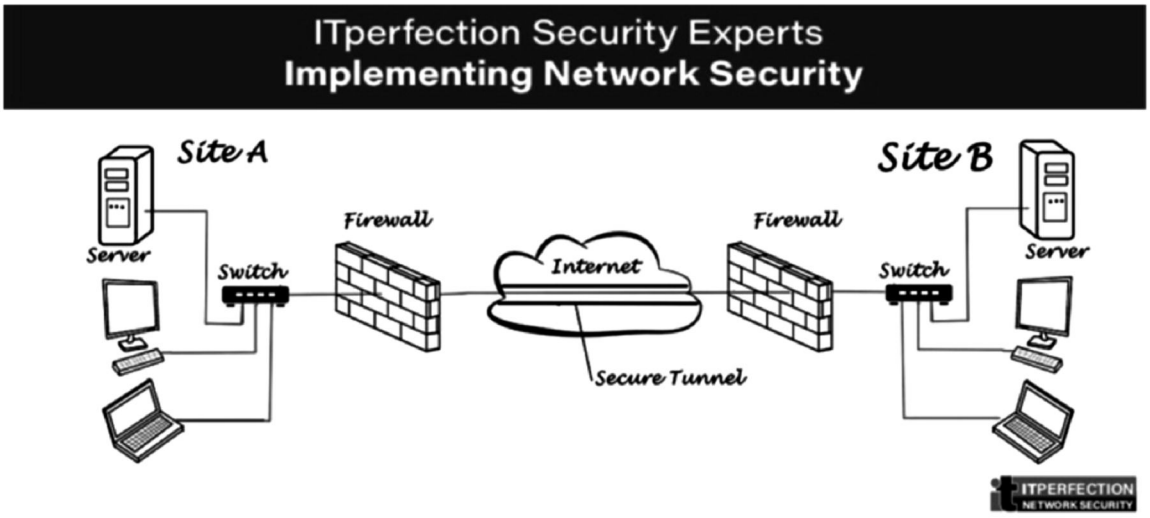
A Site-to-Site VPN is also called as Router-to-Router VPN and is mostly used in the corporates. Companies, with offices in different geographical locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

- **Intranet based VPN**: When multiple offices of the same company are connected using Site-to-Site VPN type.

Rahul Publications

- **Extranet based VPN**: When companies use Site-to-site VPN type to connect to the office of another company.

Basically, Site-to-site creates a virtual bridge between the networks at geographically distant offices and connect them through the Internet and maintain a secure and private communication between the networks.

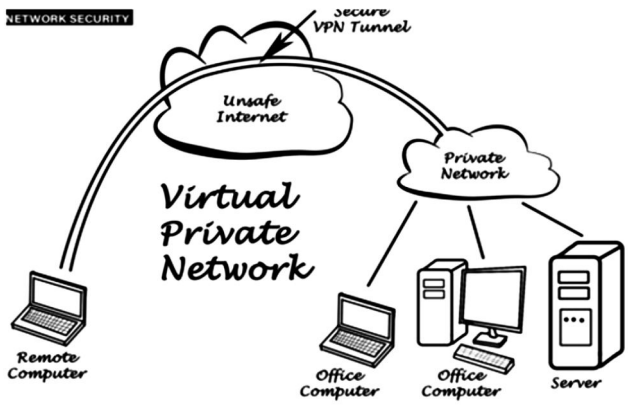


Anyway, in this VPN type one router acts as a virtual private network Client and another router as a VPN Server. The communication between the two routers starts only after an authentication is validated between the two.

Remote Access

Remote access VPN allows a user to connect to a private network and access its services and resources remotely. The connection between the user and the private network happens through the Internet and the connection is secure and private. A corporate employee, while traveling, uses a virtual private network to connect to his/her company's private network and remotely access files and resources on the private network.

Home users, or private users of virtual private network, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users conscious of Internet security also use VPN services to enhance their Internet security and privacy.



The main benefits of remote access VPNs are easy setups and hassle-free use. With the right software, this type of VPN can be easily accessible to newcomers and veterans alike, and is ideal for personal use. However, it may be unsuitable for (and even incompatible with) large-scale business needs.

4.10 Security Protocols

4.10.1 Security at the Application Layer

Q13. Write about security protocols at application layer.

Ans : **(Imp.)**

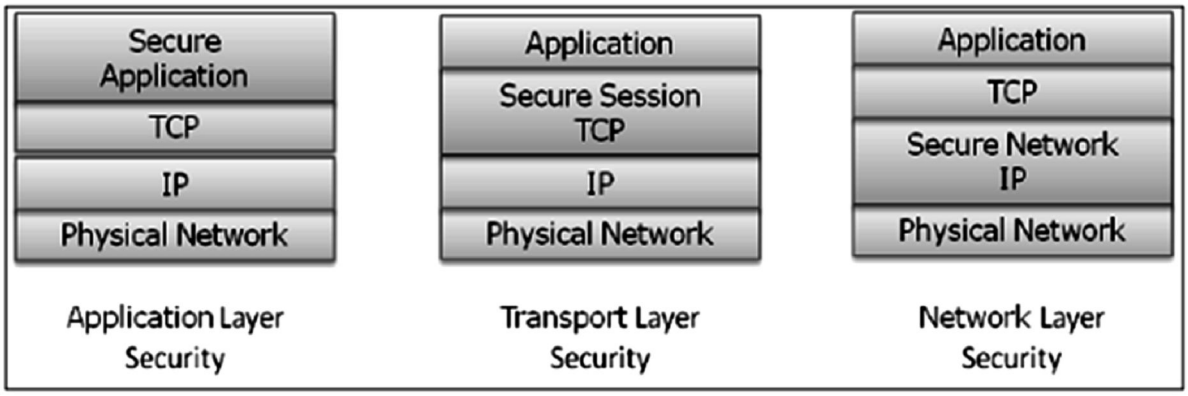
Various business services are now offered online though client-server applications. The most popular forms are web application and e-mail. In both applications, the client communicates to the designated server and obtains services.

While using a service from any server application, the client and server exchange a lot of information on the underlying intranet or Internet. We are aware of fact that these information transactions are vulnerable to various attacks.

Network security entails securing data against attacks while it is in transit on a network. To achieve this goal, many real-time security protocols have been designed. Such protocol needs to provide at least the following primary objectives:

- The parties can negotiate interactively to authenticate each other.
- Establish a secret session key before exchanging information on network.
- Exchange the information in encrypted form.

Interestingly, these protocols work at different layers of networking model. For example, S/MIME protocol works at Application layer, SSL protocol is developed to work at transport layer, and IPsec protocol works at Network layer.



In this chapter, we will discuss different processes for achieving security for e-mail communication and associated security protocols. The method for securing DNS is covered subsequently.

E-mail Security

Nowadays, e-mail has become very widely used network application. Let's briefly discuss the e-mail infrastructure before proceeding to know about e-mail security protocols.

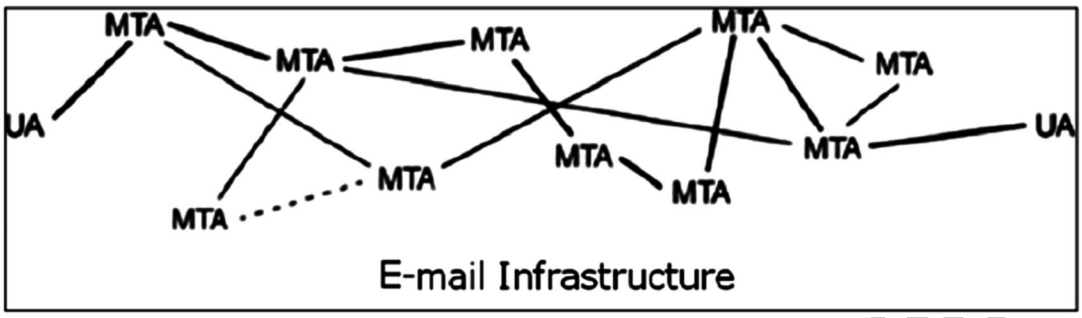
E-mail Infrastructure

The simplest way of sending an e-mail would be sending a message directly from the sender's machine to the recipient's machine. In this case, it is essential for both the machines to be running on the network simultaneously. However, this setup is impractical as users may occasionally connect their machines to the network.

Hence, the concept of setting up e-mail servers arrived. In this setup, the mail is sent to a mail server which is permanently available on the network. When the recipient's machine connects to the network, it reads the mail from the mail server.

In general, the e-mail infrastructure consists of a mesh of mail servers, also termed as Message Transfer Agents (MTAs) and client machines running an e-mail program comprising of User Agent (UA) and local MTA.

Typically, an e-mail message gets forwarded from its UA, goes through the mesh of MTAs and finally reaches the UA on the recipient's machine.



The protocols used for e-mail are as follows:

- Simple mail Transfer Protocol (SMTP) used for forwarding e-mail messages.
- Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) are used to retrieve the messages by recipient from the server.

MIME

Basic Internet e-mail standard was written in 1982 and it describes the format of e-mail message exchanged on the Internet. It mainly supports e-mail message written as text in basic Roman alphabet.

By 1992, the need was felt to improve the same. Hence, an additional standard Multipurpose Internet Mail Extensions (MIME) was defined. It is a set of extensions to the basic Internet E-mail standard. MIME provides an ability to send e-mail using characters other than those of the basic Roman alphabet such as Cyrillic alphabet (used in Russian), the Greek alphabet, or even the ideographic characters of Chinese.

Another need fulfilled by MIME is to send non-text contents, such as images or video clips. Due to this features, the MIME standard became widely adopted with SMTP for e-mail communication.

E-Mail Security Services

Growing use of e-mail communication for important and crucial transactions demands provision of certain fundamental security services as the following "

- **Confidentiality:** E-mail message should not be read by anyone but the intended recipient.
- **Authentication:** E-mail recipient can be sure of the identity of the sender.
- **Integrity:** Assurance to the recipient that the e-mail message has not been altered since it was transmitted by the sender.
- **Non-repudiation:** E-mail recipient is able to prove to a third party that the sender really did send the message.
- **Proof of submission:** E-mail sender gets the confirmation that the message is handed to the mail delivery system.

Rahul Publications

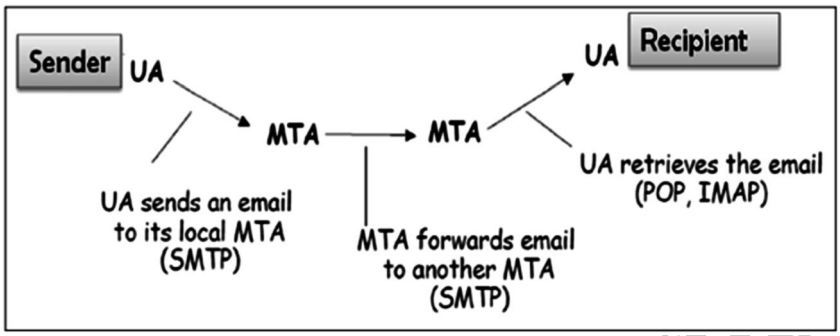
- **Proof of delivery** " Sender gets a confirmation that the recipient received the message.

Security services such as privacy, authentication, message integrity, and non-repudiation are usually provided by using public key cryptography.

Typically, there are three different scenarios of e-mail communication. We will discuss the methods of achieving above security services in these scenarios.

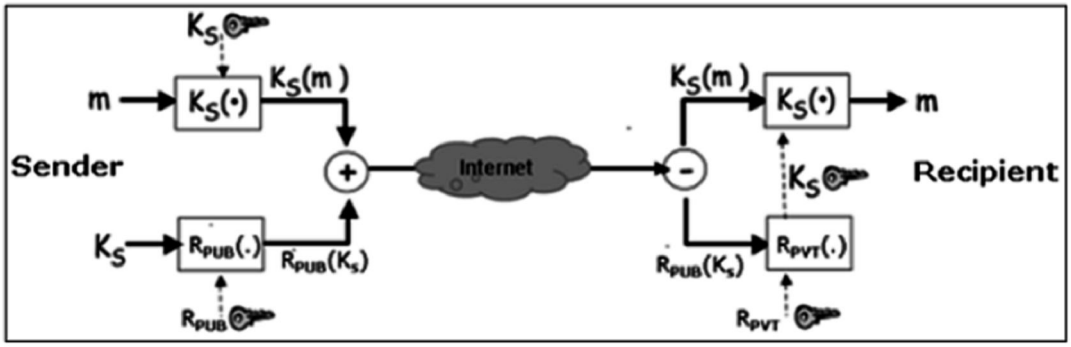
One-to-One E-mail

In this scenario, the sender sends an e-mail message to only one recipient. Usually, not more than two MTA are involved in the communication.



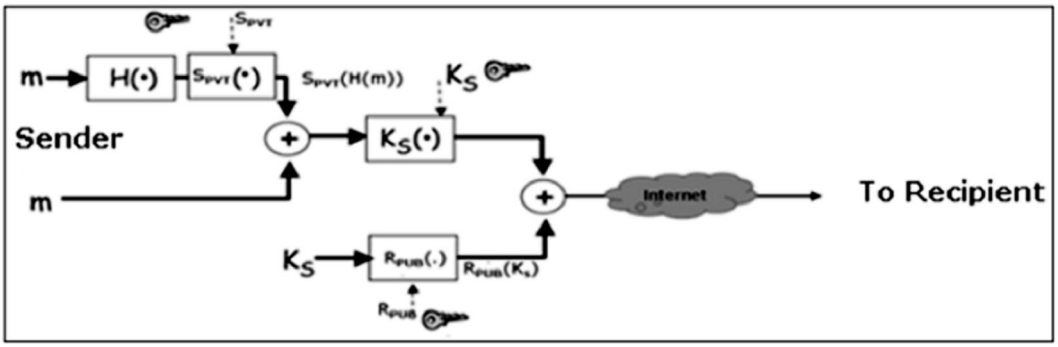
Let's assume a sender wants to send a confidential e-mail to a recipient. The provision of privacy in this case is achieved as follows:

- The sender and receiver have their private-public keys as (S_{PVT}, S_{PUB}) and (R_{PVT}, R_{PUB}) respectively.
- The sender generates a secret symmetric key, K_S for encryption. Though the sender could have used R_{PUB} for encryption, a symmetric key is used to achieve faster encryption and decryption.
- The sender encrypts message with key K_S and also encrypts K_S with public key of the recipient, R_{PUB}.
- The sender sends encrypted message and encrypted K_S to the recipient.
- The recipient first obtains K_S by decrypting encoded K_S using his private key, R_{PVT}.
- The recipient then decrypts message using the symmetric key, K_S.



If message integrity, authentication, and non-repudiation services are also needed in this scenario, the following steps are added to the above process.

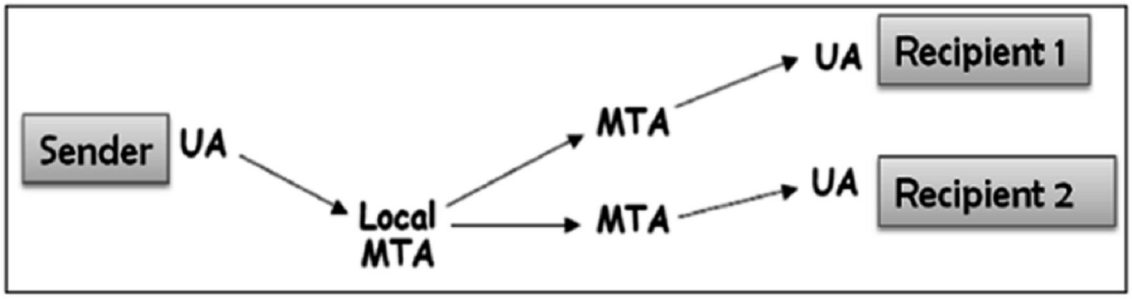
- The sender produces hash of message and digitally signs this hash with his private key, S_{PVT}.
- The sender sends this signed hash to the recipient along with other components.



- The recipient uses public key S_{PUB} and extracts the hash received under the sender's signature.
- The recipient then hashes the decrypted message and now compares the two hash values. If they match, message integrity is considered to be achieved.
- Also, the recipient is sure that the message is sent by the sender (authentication). And lastly, the sender cannot deny that he did not send the message (non-repudiation).

One-to-Multiple Recipients E-mail

In this scenario, the sender sends an e-mail message to two or more recipients. The list is managed by the sender's e-mail program (UA + local MTA). All recipients get the same message.



Let's assume, the sender wants to send confidential e-mail to many recipients (say R1, R2, and R3). The provision of privacy in this case is achieved as follows "

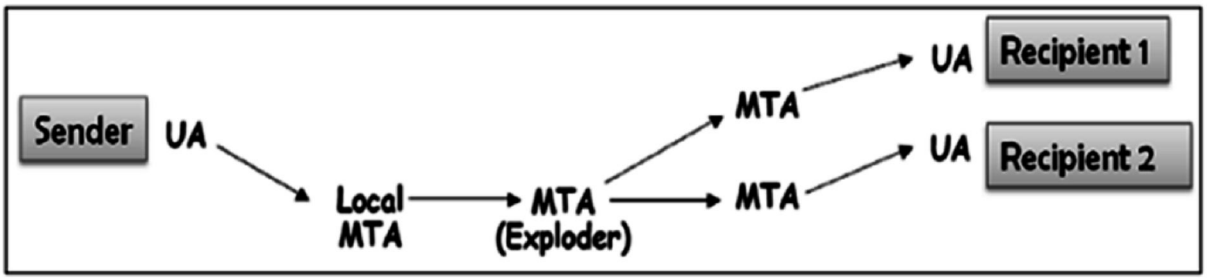
- The sender and all recipients have their own pair of private-public keys.
- The sender generates a secret symmetric key, K_s and encrypts the message with this key.
- The sender then encrypts K_S multiple times with public keys of R1, R2, and R3, getting $R1_{PUB}(K_S)$, $R2_{PUB}(K_S)$, and $R3_{PUB}(K_S)$.
- The sender sends encrypted message and corresponding encrypted K_S to the recipient. For example, recipient 1 (R1) receives encrypted message and $R1_{PUB}(K_S)$.
- Each recipient first extracts key K_S by decrypting encoded K_S using his private key.
- Each recipient then decrypts the message using the symmetric key, K_S.

For providing the message integrity, authentication, and non-repudiation, the steps to be followed are similar to the steps mentioned above in one-to-one e-mail scenario.

One-to-Distribution List E-mail

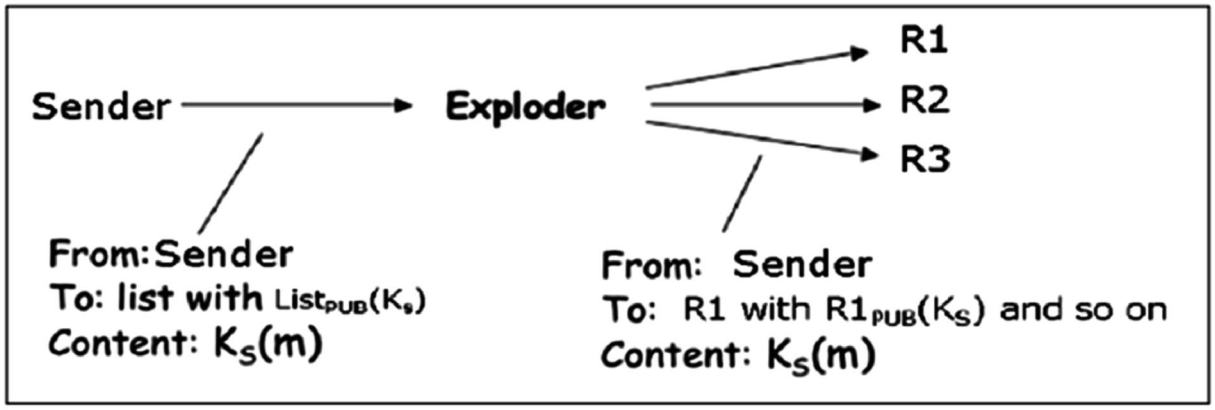
In this scenario, the sender sends an e-mail message to two or more recipients but the list of recipients is not managed locally by the sender. Generally, the e-mail server (MTA) maintains the mailing list.

The sender sends a mail to the MTA managing the mailing list and then the mail is exploded by MTA to all recipients in the list.



In this case, when the sender wants to send a confidential e-mail to the recipients of the mailing list (say R1, R2, and R3); the privacy is ensured as follows:

- The sender and all recipients have their own pair of private-public keys. The Exploder Server has a pair of private-public key for each mailing list ($List_{PUB}$, $List_{PVT}$) maintained by it.
- The sender generates a secret symmetric key K_s and then encrypts the message with this key.
- The sender then encrypts K_S with the public key associated with the list, obtains $List_{PUB}(K_S)$.
- The sender sends encrypted message and $List_{PUB}(K_S)$. The exploder MTA decrypts $List_{PUB}(K_S)$ using $List_{PVT}$ and obtains K_S.
- The exploder encrypts K_S with as many public keys as there are members in the list.
- The Exploder forwards the received encrypted message and corresponding encrypted K_S to all recipients in the list. For example, the Exploder forwards the encrypted message and $R1_{PUB}(K_S)$ to recipient 1 and so on.



For providing the message integrity, authentication, and non-repudiation the steps to be followed are similar as given in case of one-to-one e-mail scenario.

Interestingly, the e-mail program employing above security method for securing e-mail is expected to work for all the possible scenarios discussed above. Most of the above security mechanisms for e-mail are provided by two popular schemes, Pretty Good Privacy (PGP) and S/MIME. We discuss both in the following sections.

4.11 PGP AND S/MIME

Q14. Explain PGP scheme.

(OR)

Explain working mechanism of PGP.

Ans : **(Imp.)**

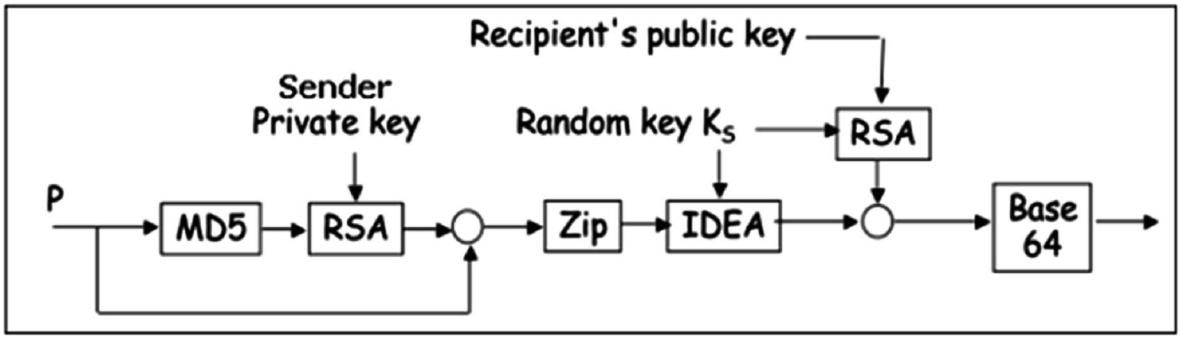
Pretty Good Privacy (PGP) is an e-mail encryption scheme. It has become the de-facto standard for providing security services for e-mail communication.

As discussed above, it uses public key cryptography, symmetric key cryptography, hash function, and digital signature. It provides:

- Privacy
- Sender Authentication
- Message Integrity
- Non-repudiation

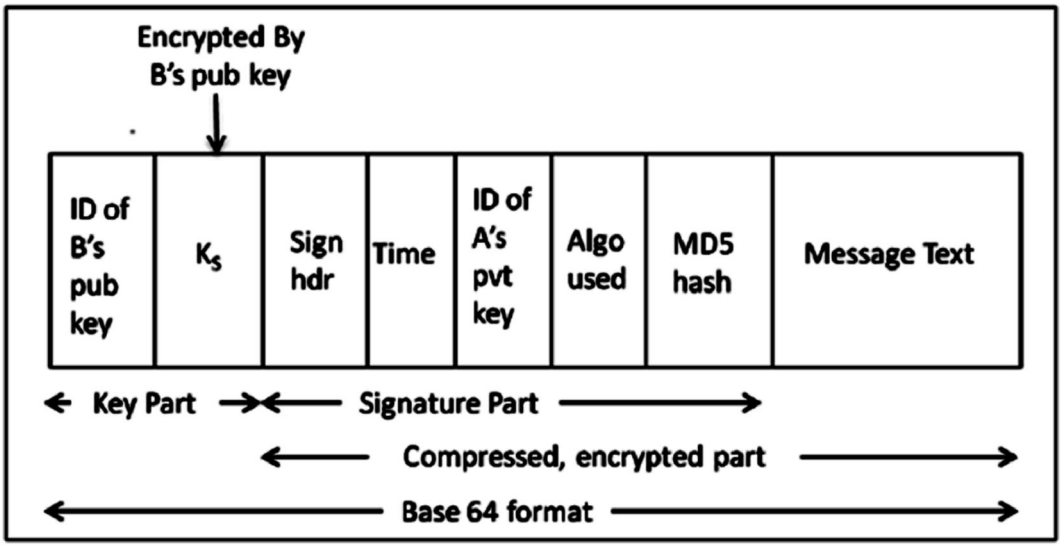
Along with these security services, it also provides data compression and key management support. PGP uses existing cryptographic algorithms such as RSA, IDEA, MD5, etc., rather than inventing the new ones.

Working of PGP



- Hash of the message is calculated. (MD5 algorithm)
- Resultant 128 bit hash is signed using the private key of the sender (RSA Algorithm).
- The digital signature is concatenated to message, and the result is compressed.
- A 128-bit symmetric key, K_S is generated and used to encrypt the compressed message with IDEA.
- K_S is encrypted using the public key of the recipient using RSA algorithm and the result is appended to the encrypted message.

The format of PGP message is shown in the following diagram. The IDs indicate which key is used to encrypt KS and which key is to be used to verify the signature on the hash.



In PGP scheme, a message in signed and encrypted, and then MIME is encoded before transmission.

PGP Certificate

PGP key certificate is normally established through a chain of trust. For example, A's public key is signed by B using his public key and B's public key is signed by C using his public key. As this process goes on, it establishes a web of trust.

In a PGP environment, any user can act as a certifying authority. Any PGP user can certify another PGP user's public key. However, such a certificate is only valid to another user if the user recognizes the certifier as a trusted introducer.

Several issues exist with such a certification method. It may be difficult to find a chain leading from a known and trusted public key to desired key. Also, there might be multiple chains which can lead to different keys for desired user.

PGP can also use the PKI infrastructure with certification authority and public keys can be certified by CA (X.509 certificate).

Q15. Explain briefly about S/MIME.

Ans : **(Imp.)**

S / MIME

S/MIME stands for Secure Multipurpose Internet Mail Extension. S/MIME is a secure e-mail standard. It is based on an earlier non-secure e-mailing standard called MIME.

Working of S/MIME

S/MIME approach is similar to PGP. It also uses public key cryptography, symmetric key cryptography, hash functions, and digital signatures. It provides similar security services as PGP for e-mail communication.

The most common symmetric ciphers used in S/MIME are RC2 and TripleDES. The usual public key method is RSA, and the hashing algorithm is SHA-1 or MD5.

S/MIME specifies the additional MIME type, such as "application/pkcs7-mime", for data enveloping after encrypting. The whole MIME entity is encrypted and packed into an object. S/MIME has standardized cryptographic message formats (different from PGP). In fact, MIME is extended with some keywords to identify the encrypted and/or signed parts in the message.

Rahul Publications

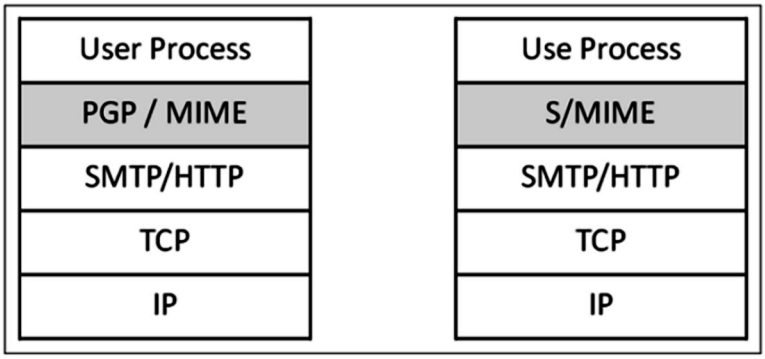
S/MIME relies on X.509 certificates for public key distribution. It needs top-down hierarchical PKI for certification support.

Employability of S/MIME

Due to the requirement of a certificate from certification authority for implementation, not all users can take advantage of S/MIME, as some may wish to encrypt a message, with a public/private key pair. For example, without the involvement or administrative overhead of certificates.

In practice, although most e-mailing applications implement S/MIME, the certificate enrollment process is complex. Instead PGP support usually requires adding a plug-in and that plug-in comes with all that is needed to manage keys. The Web of Trust is not really used. People exchange their public keys over another medium. Once obtained, they keep a copy of public keys of those with whom e-mails are usually exchanged.

Implementation layer in network architecture for PGP and S/MIME schemes is shown in the following image. Both these schemes provide application level security of for e-mail communication.



One of the schemes, either PGP or S/MIME, is used depending on the environment. A secure e-email communication in a captive network can be provided by adapting to PGP. For e-mail security over Internet, where mails are exchanged with new unknown users very often, S/MIME is considered as a good option.

4.12 Security at Transport Layer- SSL and TLS

Q16. What is the need for transport layer security?

Ans :

Need for Transport Layer Security

Let's discuss a typical Internet-based business transaction.

Bob visits Alice's website for selling goods. In a form on the website, Bob enters the type of good and quantity desired, his address and payment card details. Bob clicks on Submit and waits for delivery of goods with debit of price amount from his account. All this sounds good, but in absence of network security, Bob could be in for a few surprises.

- If transactions did not use confidentiality (encryption), an attacker could obtain his payment card information. The attacker can then make purchases at Bob's expense.
- If no data integrity measure is used, an attacker could modify Bob's order in terms of type or quantity of goods.
- Lastly, if no server authentication is used, a server could display Alice's famous logo but the site

could be a malicious site maintained by an attacker, who is masquerading as Alice. After receiving Bob's order, he could take Bob's money and flee. Or he could carry out an identity theft by collecting Bob's name and credit card details.

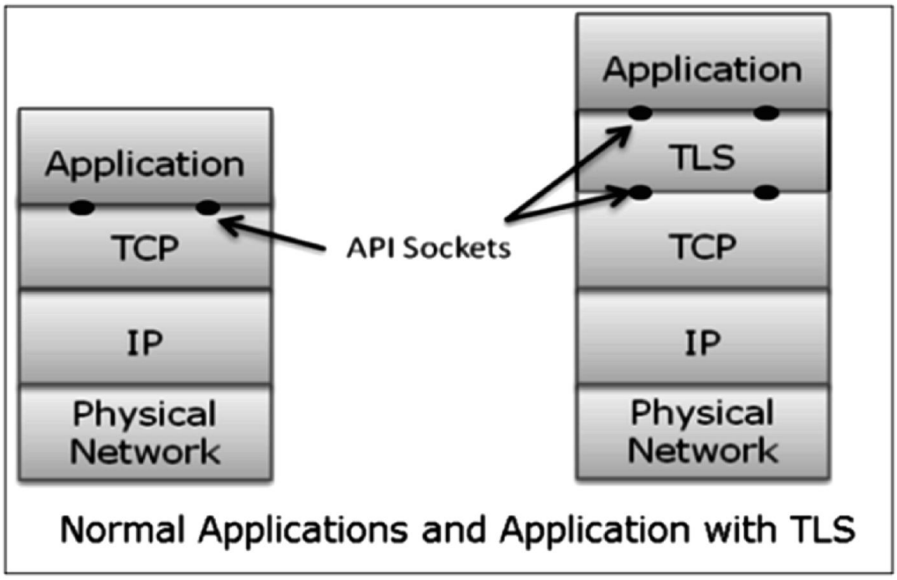
Transport layer security schemes can address these problems by enhancing TCP/IP based network communication with confidentiality, data integrity, server authentication, and client authentication.

The security at this layer is mostly used to secure HTTP based web transactions on a network. However, it can be employed by any application running over TCP.

Philosophy of TLS Design

Transport Layer Security (TLS) protocols operate above the TCP layer. Design of these protocols use popular Application Program Interfaces (API) to TCP, called "sockets" for interfacing with TCP layer.

Applications are now interfaced to Transport Security Layer instead of TCP directly. Transport Security Layer provides a simple API with sockets, which is similar and analogous to TCP's API.



In the above diagram, although TLS technically resides between application and transport layer, from the common perspective it is a transport protocol that acts as TCP layer enhanced with security services.

TLS is designed to operate over TCP, the reliable layer 4 protocol (not on UDP protocol), to make design of TLS much simpler, because it doesn't have to worry about 'timing out' and 'retransmitting lost data'. The TCP layer continues doing that as usual which serves the need of TLS.

Q17. Explain about Secure Socket layer Protocol.

Ans :

Secure Socket Layer (SSL)

In this section, we discuss the family of protocols designed for TLS. The family includes SSL versions 2 and 3 and TLS protocol. SSLv2 has been now replaced by SSLv3, so we will focus on SSL v3 and TLS.

TLS modified the cryptographic algorithms for key expansion and authentication. Also, TLS suggested use of open crypto Diffie-Hellman (DH) and Digital Signature Standard (DSS) in place of patented RSA crypto used in SSL. But due to expiry of RSA patent in 2000, there existed no strong reasons for users to shift away from the widely deployed SSLv3 to TLS.

Salient Features of SSL

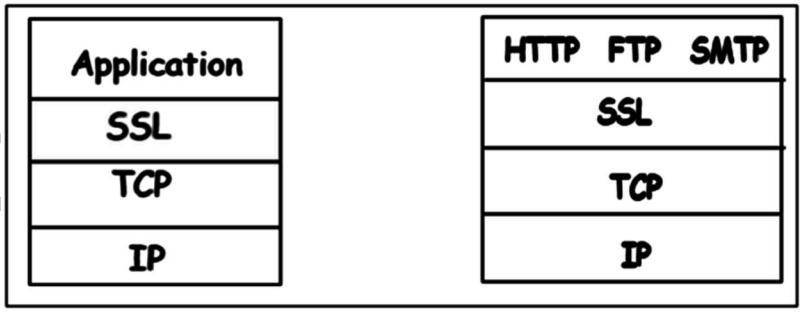
The salient features of SSL protocol are as follows "

- SSL provides network connection security through "
  - **Confidentiality:** Information is exchanged in an encrypted form.
  - **Authentication:** Communication entities identify each other through the use of digital certificates. Web-server authentication is mandatory whereas client authentication is kept optional.
  - **Reliability :** Maintains message integrity checks.
- SSL is available for all TCP applications.
- Supported by almost all web browsers.
- Provides ease in doing business with new online entities.
- Developed primarily for Web e-commerce.

Architecture of SSL

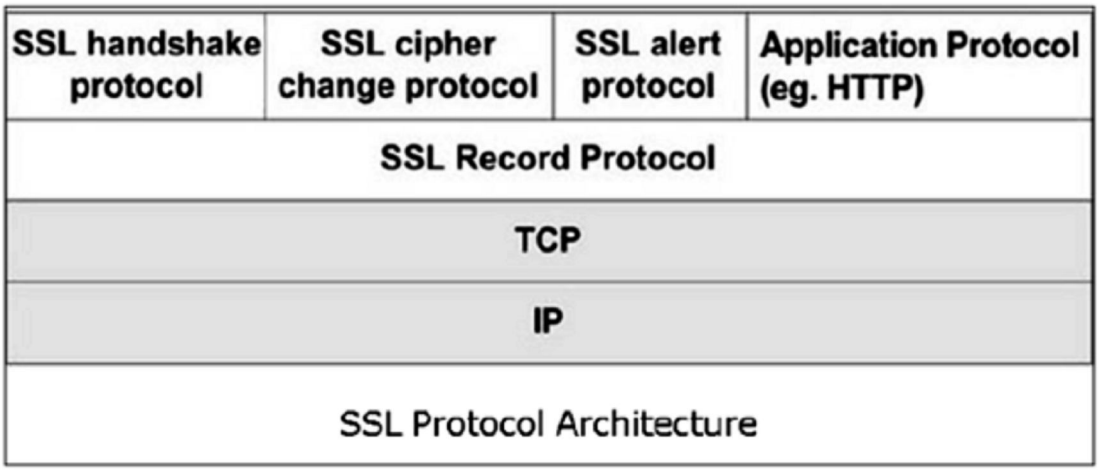
SSL is specific to TCP and it does not work with UDP. SSL provides Application Programming Interface (API) to applications. C and Java SSL libraries/classes are readily available.

SSL protocol is designed to interwork between application and transport layer as shown in the following image.



SSL itself is not a single layer protocol as depicted in the image; in fact it is composed of two sub-layers.

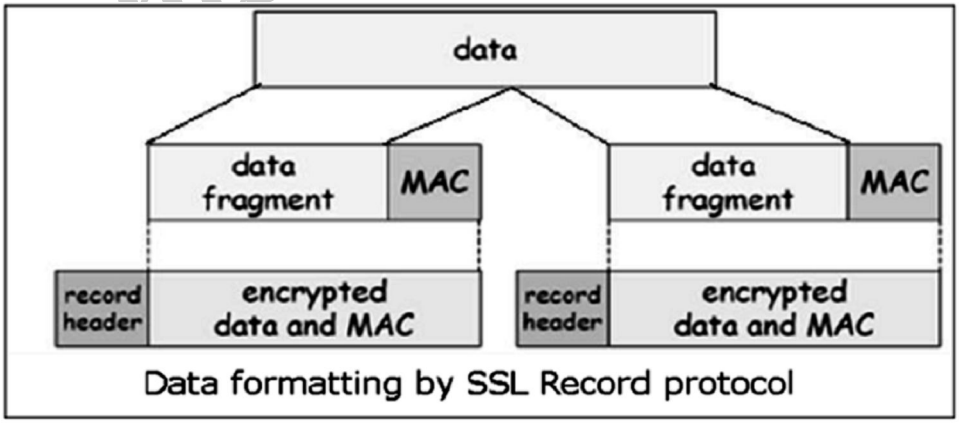
- Lower sub-layer comprises of the one component of SSL protocol called as SSL Record Protocol. This component provides integrity and confidentiality services.
- Upper sub-layer comprises of three SSL-related protocol components and an application protocol. Application component provides the information transfer service between client/server interactions. Technically, it can operate on top of SSL layer as well. Three SSL related protocol components are:
  - SSL Handshake Protocol
  - Change Cipher Spec Protocol
  - Alert Protocol.
- These three protocols manage all of SSL message exchanges and are discussed later in this section.



Functions of SSL Protocol Components

The four sub-components of the SSL protocol handle various tasks for secure communication between the client machine and the server.

- **Record Protocol**
  - The record layer formats the upper layer protocol messages.
  - It fragments the data into manageable blocks (max length 16 KB). It optionally compresses the data.
  - Encrypts the data.
  - Provides a header for each message and a hash (Message Authentication Code (MAC)) at the end.
  - Hands over the formatted blocks to TCP layer for transmission.



- **SSL Handshake Protocol**
  - It is the most complex part of SSL. It is invoked before any application data is transmitted. It creates SSL sessions between the client and the server.
  - Establishment of session involves Server authentication, Key and algorithm negotiation, Establishing keys and Client authentication (optional).
  - A session is identified by unique set of cryptographic security parameters.

Rahul Publications

- Multiple secure TCP connections between a client and a server can share the same session.
- Handshake protocol actions through four phases. These are discussed in the next section.

➢ **ChangeCipherSpec Protocol**

- Simplest part of SSL protocol. It comprises of a single message exchanged between two communicating entities, the client and the server.
- As each entity sends the ChangeCipherSpec message, it changes its side of the connection into the secure state as agreed upon.
- The cipher parameters pending state is copied into the current state.
- Exchange of this Message indicates all future data exchanges are encrypted and integrity is protected.

➢ **SSL Alert Protocol**

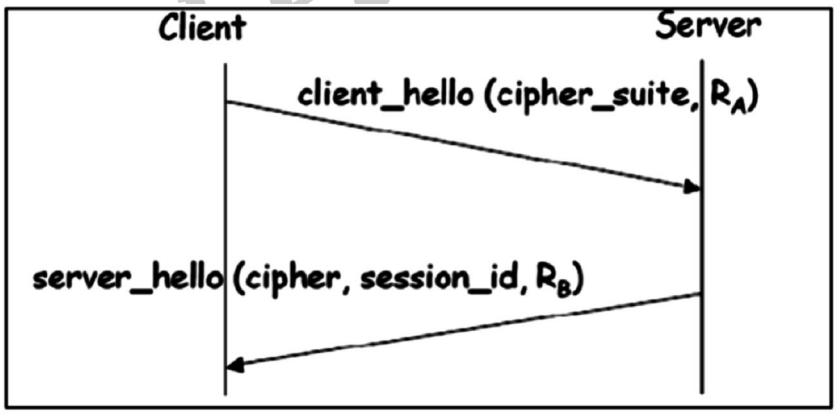
- This protocol is used to report errors – such as unexpected message, bad record MAC, security parameters negotiation failed, etc.
- It is also used for other purposes – such as notify closure of the TCP connection, notify receipt of bad or unknown certificate, etc.

Establishment of SSL Session

As discussed above, there are four phases of SSL session establishment. These are mainly handled by SSL Handshake protocol.

Phase 1: Establishing security capabilities.

➢ This phase comprises of exchange of two messages – Client_hello and Server_hello.



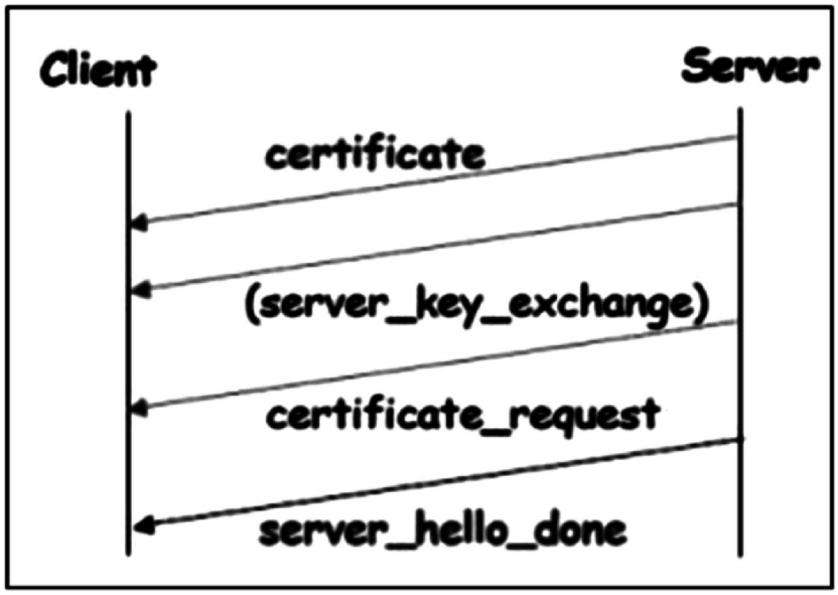
➢ Client_hello contains of list of cryptographic algorithms supported by the client, in decreasing order of preference.

➢ Server_hello contains the selected Cipher Specification (CipherSpec) and a new session_id.

➢ The CipherSpec contains fields like

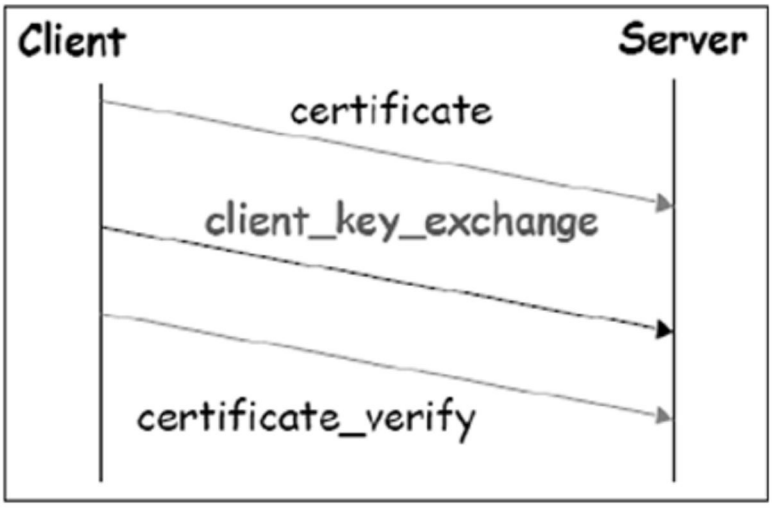
- Cipher Algorithm (DES, 3DES, RC2, and RC4)
- MAC Algorithm (based on MD5, SHA-1)
- Public-key algorithm (RSA)
- Both messages have “nonce” to prevent replay attack.

Phase 2: Server authentication and key exchange.



- Server sends certificate. Client software comes configured with public keys of various "trusted" organizations (CAs) to check certificate.
- Server sends chosen cipher suite.
- Server may request client certificate. Usually it is not done.
- Server indicates end of *Server_hello*.

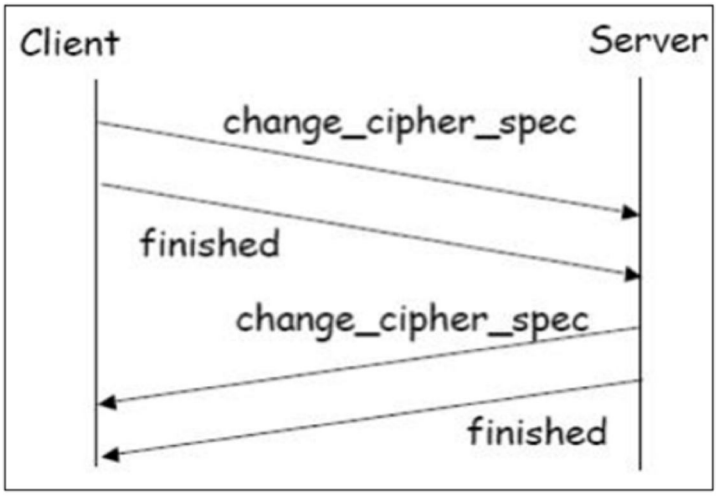
Phase 3: Client authentication and key exchange.



- Client sends certificate, only if requested by the server.
- It also sends the Pre-master Secret (PMS) encrypted with the server's public key.
- Client also sends *Certificate_verify* message if certificate is sent by him to prove he has the private key associated with this certificate. Basically, the client signs a hash of the previous messages.

Rahul Publications

Phase 4: Finish.



- Client and server send *Change_cipher_spec* messages to each other to cause the pending cipher state to be copied into the current state.
- From now on, all data is encrypted and integrity protected.
- Message "Finished" from each end verifies that the key exchange and authentication processes were successful.

All four phases, discussed above, happen within the establishment of TCP session. SSL session establishment starts after TCP SYN/ SYNACK and finishes before TCP Fin.

Resuming a Disconnected Session

- It is possible to resume a disconnected session (through *Alert* message), if the client sends a *hello_request* to the server with the encrypted *session_id* information.
- The server then determines if the *session_id* is valid. If validated, it exchanges ChangeCipherSpec and *finished* messages with the client and secure communications resume.
- This avoids recalculating of session cipher parameters and saves computing at the server and the client end.

SSL Session Keys

We have seen that during Phase 3 of SSL session establishment, a pre-master secret is sent by the client to the server encrypted using server's public key. The master secret and various session keys are generated as follows:

- The master secret is generated (via pseudo random number generator) using:
  - The pre-master secret.
  - Two nonces (RA and RB) exchanged in the client_hello and server_hello messages.
- Six secret values are then derived from this master secret as:
  - Secret key used with MAC (for data sent by server)
  - Secret key used with MAC (for data sent by client)
  - Secret key and IV used for encryption (by server)
  - Secret key and IV used for encryption (by client)

Rahul Publications

Q18. Explain briefly about TLS Protocol.

Ans : **(Imp.)**

TLS Protocol

In order to provide an open Internet standard of SSL, IETF released The Transport Layer Security (TLS) protocol in January 1999. TLS is defined as a proposed Internet Standard in RFC 5246.

Features

- TLS protocol has same objectives as SSL.
- It enables client/server applications to communicate in a secure manner by authenticating, preventing eavesdropping and resisting message modification.
- TLS protocol sits above the reliable connection-oriented transport TCP layer in the networking layers stack.
- The architecture of TLS protocol is similar to SSLv3 protocol. It has two sub protocols: the TLS Record protocol and the TLS Handshake protocol.
- Though SSLv3 and TLS protocol have similar architecture, several changes were made in architecture and functioning particularly for the handshake protocol.

Comparison of TLS and SSL Protocols

There are main eight differences between TLS and SSLv3 protocols. These are as follows "

- **Protocol Version:** The header of TLS protocol segment carries the version number 3.1 to differentiate between number 3 carried by SSL protocol segment header.
- **Message Authentication:** TLS employs a keyed-hash message authentication code (H-MAC). Benefit is that H-MAC operates with any hash function, not just MD5 or SHA, as explicitly stated by the SSL protocol.
- **Session Key Generation:** There are two differences between TLS and SSL protocol for generation of key material.
  - Method of computing pre-master and master secrets is similar. But in TLS protocol, computation of master secret uses the HMAC standard and pseudorandom function (PRF) output instead of ad-hoc MAC.
  - The algorithm for computing session keys and initiation values (IV) is different in TLS than SSL protocol.
- **Alert Protocol Message**
  - TLS protocol supports all the messages used by the Alert protocol of SSL, except No certificate alert message being made redundant. The client sends empty certificate in case client authentication is not required.
  - Many additional Alert messages are included in TLS protocol for other error conditions such as record_overflow, decode_error etc.
- **Supported Cipher Suites:** SSL supports RSA, Diffie-Hellman and Fortezza cipher suites. TLS protocol supports all suits except Fortezza.
- **Client Certificate Types:** TLS defines certificate types to be requested in a certificate_request message. SSLv3 support all of these. Additionally, SSL support certain other types of certificate such as Fortezza.

Rahul Publications

- Certificate Verify and Finished Messages "
  - In SSL, complex message procedure is used for the *certificate_verify* message. With TLS, the verified information is contained in the handshake messages itself thus avoiding this complex procedure.
  - Finished message is computed in different manners in TLS and SSLv3.
- **Padding of Data:** In SSL protocol, the padding added to user data before encryption is the minimum amount required to make the total data-size equal to a multiple of the cipher's block length. In TLS, the padding can be any amount that results in data-size that is a multiple of the cipher's block length, up to a maximum of 255 bytes.

The above differences between TLS and SSLv3 protocols are summarized in the following table.

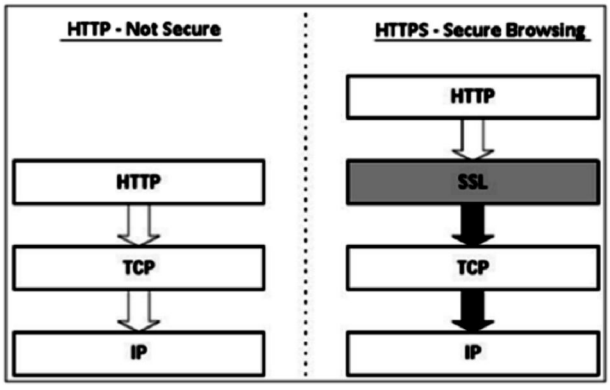
	SSL v3.0	TLS v1.0
Protocol version in messages	3.0	3.1
Alert protocol message types	12	23
Message authentication	ad hoc	standard
Key material generation	ad hoc	PRF
CertificateVerify	complex	simple
Finished	ad hoc	PRF
Baseline cipher suites	includes Fortezza	no Fortezza

Q19. Explain how can you secure your browser using HTTPS.

Ans :

Secure Browsing - HTTPS

Hyper Text Transfer Protocol (HTTP) protocol is used for web browsing. The function of HTTPS is similar to HTTP. The only difference is that HTTPS provides "secure" web browsing. HTTPS stands for HTTP over SSL. This protocol is used to provide the encrypted and authenticated connection between the client web browser and the website server.



The secure browsing through HTTPS ensures that the following content are encrypted:

- URL of the requested web page.
- Web page contents provided by the server to the user client.
- Contents of forms filled in by user.
- Cookies established in both directions.

Working of HTTPS

HTTPS application protocol typically uses one of two popular transport layer security protocols - SSL or TLS. The process of secure browsing is described in the following points.

- You request a HTTPS connection to a webpage by entering https:// followed by URL in the browser address bar.
- Web browser initiates a connection to the web server. Use of https invokes the use of SSL protocol.
- An application, browser in this case, uses the system port 443 instead of port 80 (used in case of http).
- The SSL protocol goes through a handshake protocol for establishing a secure session as discussed in earlier sections.
- The website initially sends its SSL Digital certificate to your browser. On verification of certificate, the SSL handshake progresses to exchange the shared secrets for the session.
- When a trusted SSL Digital Certificate is used by the server, users get to see a padlock icon in the browser address bar. When an Extended Validation Certificate is installed on a website, the address bar turns green.

- Once established, this session consists of many secure connections between the web server and the browser.

Use of HTTPS

- Use of HTTPS provides confidentiality, server authentication and message integrity to the user. It enables safe conduct of e-commerce on the Internet.
- Prevents data from eavesdropping and denies identity theft which are common attacks on HTTP.

Present day web browsers and web servers are equipped with HTTPS support. The use of HTTPS over HTTP, however, requires more computing power at the client and the server end to carry out encryption and SSL handshake.

Q20. Explain about SSH protocol.

Ans :

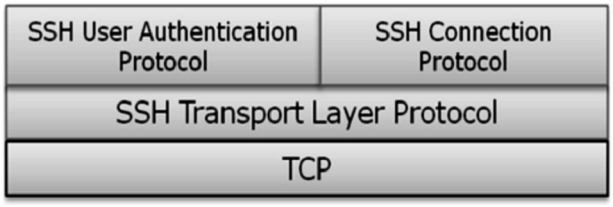
Secure Shell Protocol (SSH)

The salient features of SSH are as follows:

- SSH is a network protocol that runs on top of the TCP/IP layer. It is designed to replace the TELNET which provided unsecure means of remote logon facility.
- SSH provides a secure client/server communication and can be used for tasks such as file transfer and e-mail.
- SSH2 is a prevalent protocol which provides improved network communication security over earlier version SSH1.

SSH Defined

SSH is organized as three sub-protocols.



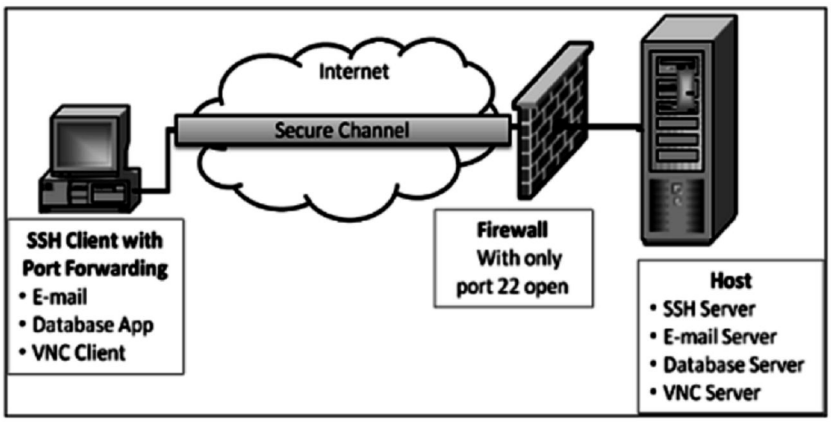
- **Transport Layer Protocol:** This part of SSH protocol provides data confidentiality, server (host) authentication, and data integrity. It may optionally provide data compression as well.
  - **Server Authentication:** Host keys are asymmetric like public/private keys. A server uses a public key to prove its identity to a client. The client verifies that contacted server is a "known" host from the database it maintains. Once the server is authenticated, session keys are generated.
  - **Session Key Establishment:** After authentication, the server and the client agree upon cipher to be used. Session keys are generated by both the client and the server. Session keys are generated before user authentication so that usernames and passwords can be sent encrypted. These keys are generally replaced at regular intervals (say, every hour) during the session and are destroyed immediately after use.
  - **Data Integrity:** SSH uses Message Authentication Code (MAC) algorithms to for data integrity check. It is an improvement over 32 bit CRC used by SSH1.
- **User Authentication Protocol:** This part of SSH authenticates the user to the server. The server verifies that access is given to intended users only. Many authentication methods are currently used such as, typed passwords, Kerberos, public-key authentication, etc.
- **Connection Protocol:** This provides multiple logical channels over a single underlying SSH connection.

SSH Services

SSH provides three main services that enable provision of many secure solutions. These services are briefly described as follows:

- **Secure Command-Shell (Remote Logon):** It allows the user to edit files, view the contents of directories, and access applications on connected device. Systems administrators can remotely start/ view/stop services and processes, create user accounts, and change file/directories permissions and so on. All tasks that are feasible at a machine's command prompt can now be performed securely from the remote machine using secure remote logon.
- **Secure File Transfer:** SSH File Transfer Protocol (SFTP) is designed as an extension for SSH-2 for secure file transfer. In essence, it is a separate protocol layered over the Secure Shell protocol to handle file transfers. SFTP encrypts both the username/password and the file data being transferred. It uses the same port as the Secure Shell server, i.e. system port no 22.
- **Port Forwarding (Tunneling):** It allows data from unsecured TCP/IP based applications to be secured. After port forwarding has been set up, Secure Shell reroutes traffic from a program (usually a client) and sends it across the encrypted tunnel to the program on the other side (usually a server). Multiple applications can transmit data over a single multiplexed secure channel, eliminating the need to open many ports on a firewall or router.

Rahul Publications



Benefits & Limitations

The benefits and limitations of employing communication security at transport layer are as follows:

➢ **Benefits**

- Transport Layer Security is transparent to applications.
- Server is authenticated.
- Application layer headers are hidden.
- It is more fine-grained than security mechanisms at layer 3 (IPsec) as it works at the transport connection level.

➢ **Limitations**

- Applicable to TCP-based applications only (not UDP).
- TCP/IP headers are in clear.
- Suitable for direct communication between the client and the server. Does not cater for secure applications using chain of servers (e.g. email)
- SSL does not provide non-repudiation as client authentication is optional.
- If needed, client authentication needs to be implemented above SSL.

Rahul Publications

4.13 Security at Network Layer-IPSec

Q21. Explain how security in the network layer managed using IPSec protocol.

Ans :

Security in Network Layer

Any scheme that is developed for providing network security needs to be implemented at some layer in protocol stack as depicted in the diagram below "

The popular framework developed for ensuring security at network layer is Internet Protocol Security (IPsec).

Features of IPsec

➢ IPsec is not designed to work only with TCP as a transport protocol. It works with UDP as well as any other protocol above IP such as ICMP, OSPF etc.

- IPsec protects the entire packet presented to IP layer including higher layer headers.
- Since higher layer headers are hidden which carry port number, traffic analysis is more difficult.
- IPsec works from one network entity to another network entity, not from application process to application process. Hence, security can be adopted without requiring changes to individual user computers/applications.
- Tough widely used to provide secure communication between network entities, IPsec can provide host-to-host security as well.
- The most common use of IPsec is to provide a Virtual Private Network (VPN), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway).

Security Functions

The important security functions provided by the IPsec are as follows "

- **Confidentiality**
  - Enables communicating nodes to encrypt messages.
  - Prevents eavesdropping by third parties.
- **Origin authentication and data integrity**
  - Provides assurance that a received packet was actually transmitted by the party identified as the source in the packet header.
  - Confirms that the packet has not been altered or otherwise.
- **Key management**
  - Allows secure exchange of keys.
  - Protection against certain types of security attacks, such as replay attacks.

  specify some portions of the protocol, while others address the solution as a whole.

Operations Within IPsec

The IPsec suite can be considered to have two separate operations, when performed in unison, providing a complete set of security services. These two operations are IPsec Communication and Internet Key Exchange.

- **IPsec Communication**
  - It is typically associated with standard IPsec functionality. It involves encapsulation, encryption, and hashing the IP datagrams and handling all packet processes.
  - It is responsible for managing the communication according to the available Security Associations (SAs) established between communicating parties.
  - It uses security protocols such as Authentication Header (AH) and Encapsulated SP (ESP).
  - IPsec communication is not involved in the creation of keys or their management.
  - IPsec communication operation itself is commonly referred to as IPsec.
- **Internet Key Exchange (IKE)**
  - IKE is the automatic key management protocol used for IPsec.

Rahul Publications

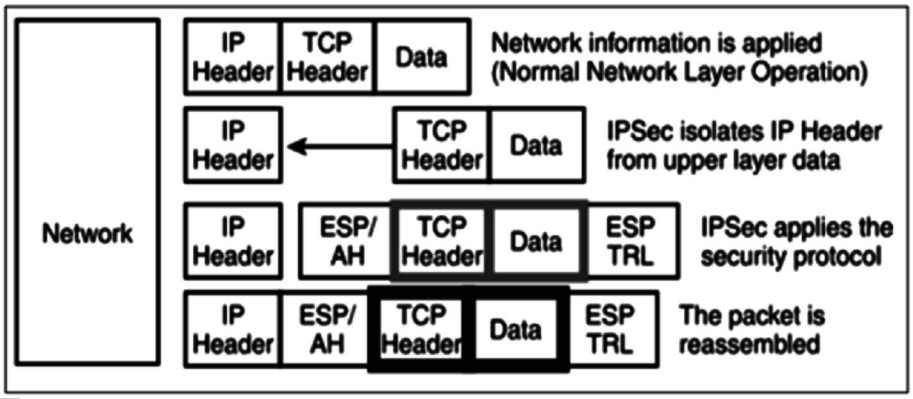
- Technically, key management is not essential for IPsec communication and the keys can be manually managed. However, manual key management is not desirable for large networks.
- IKE is responsible for creation of keys for IPsec and providing authentication during key establishment process. Though, IPsec can be used for any other key management protocols, IKE is used by default.
- IKE defines two protocol (Oakley and SKEME) to be used with already defined key management framework Internet Security Association Key Management Protocol (ISAKMP).
- ISAKMP is not IPsec specific, but provides the framework for creating SAs for any protocol.

IPsec Communication Modes

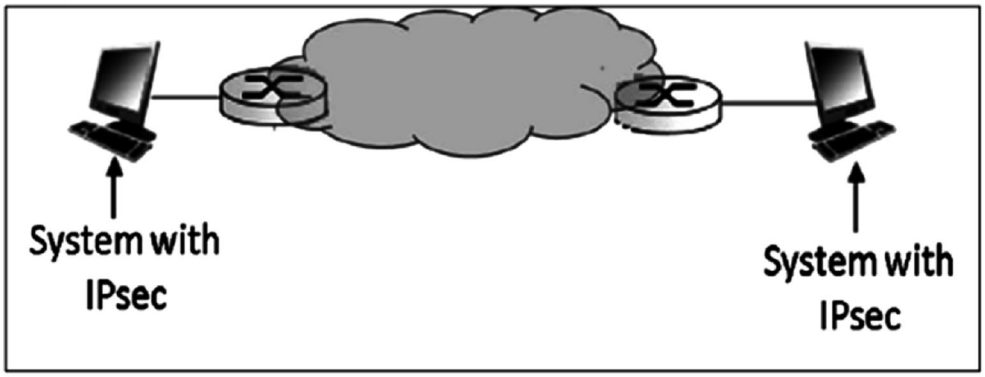
IPsec Communication has two modes of functioning; transport and tunnel modes. These modes can be used in combination or used individually depending upon the type of communication desired.

Transport Mode

- IPsec does not encapsulate a packet received from upper layer.
- The original IP header is maintained and the data is forwarded based on the original attributes set by the upper layer protocol.
- The following diagram shows the data flow in the protocol stack.



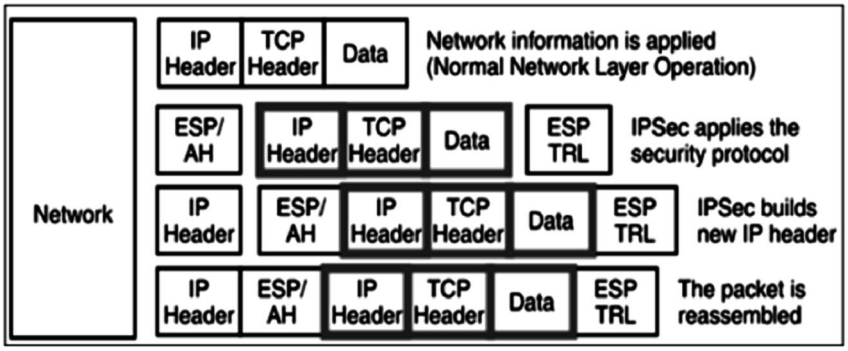
- The limitation of transport mode is that no gateway services can be provided. It is reserved for point-to-point communications as depicted in the following image.



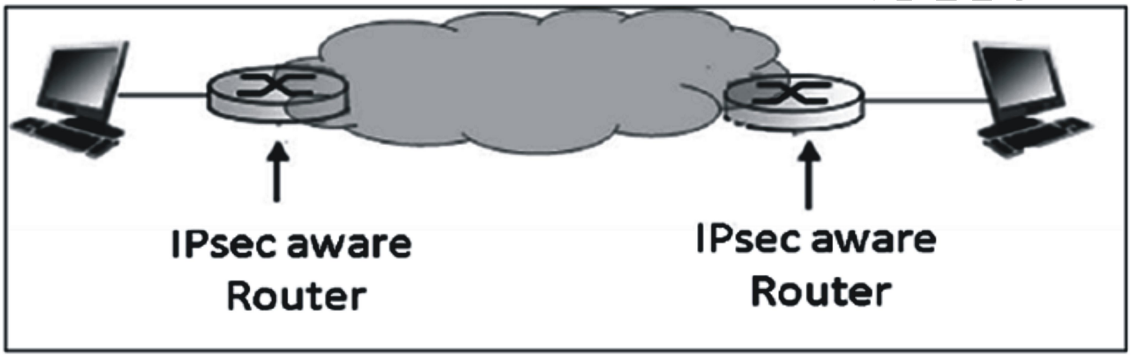
Tunnel Mode

- This mode of IPsec provides encapsulation services along with other security services.

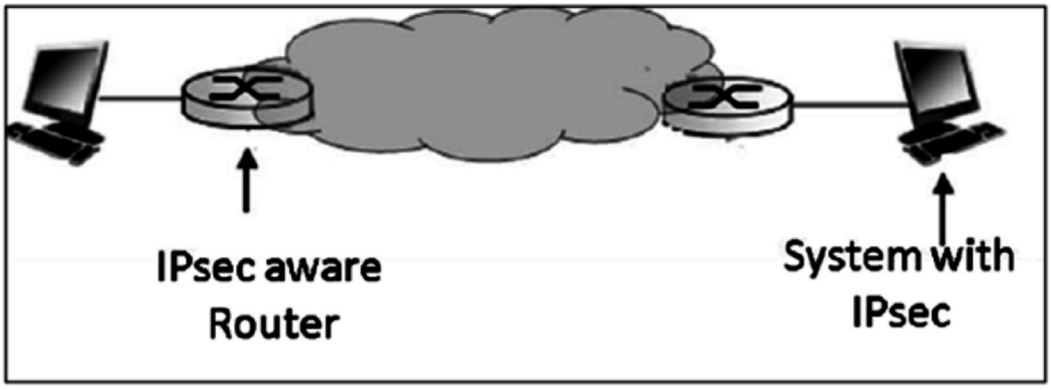
- In tunnel mode operations, the entire packet from upper layer is encapsulated before applying security protocol. New IP header is added.
- The following diagram shows the data flow in the protocol stack.



- Tunnel mode is typically associated with gateway activities. The encapsulation provides the ability to send several sessions through a single gateway.
- The typical tunnel mode communication is as depicted in the following diagram.



- As far as the endpoints are concerned, they have a direct transport layer connection. The datagram from one system forwarded to the gateway is encapsulated and then forwarded to the remote gateway. The remote associated gateway de-encapsulates the data and forwards it to the destination endpoint on the internal network.
- Using IPsec, the tunneling mode can be established between the gateway and individual end system as well.



IPsec Protocols

IPsec uses the security protocols to provide desired security services. These protocols are the heart of IPsec operations and everything else is designed to support these protocol in IPsec.

Security associations between the communicating entities are established and maintained by the security protocol used.

There are two security protocols defined by IPsec — Authentication Header (AH) and Encapsulating Security Payload (ESP).

Authentication Header

The AH protocol provides service of data integrity and origin authentication. It optionally caters for message replay resistance. However, it does not provide any form of confidentiality.

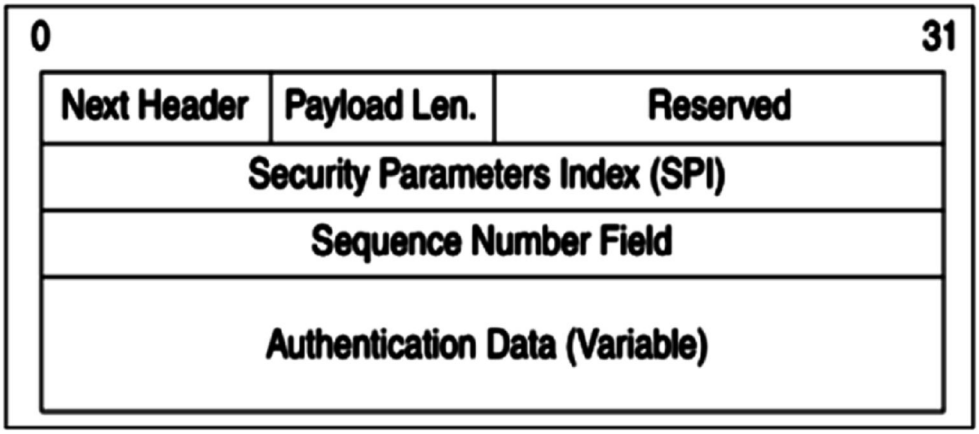
AH is a protocol that provides authentication of either all or part of the contents of a datagram by the addition of a header. The header is calculated based on the values in the datagram. What parts of the datagram are used for the calculation, and where to place the header, depends on the mode cooperation (tunnel or transport).

The operation of the AH protocol is surprisingly simple. It can be considered similar to the algorithms used to calculate checksums or perform CRC checks for error detection.

The concept behind AH is the same, except that instead of using a simple algorithm, AH uses special hashing algorithm and a secret key known only to the communicating parties. A security association between two devices is set up that specifies these particulars.

The process of AH goes through the following phases.

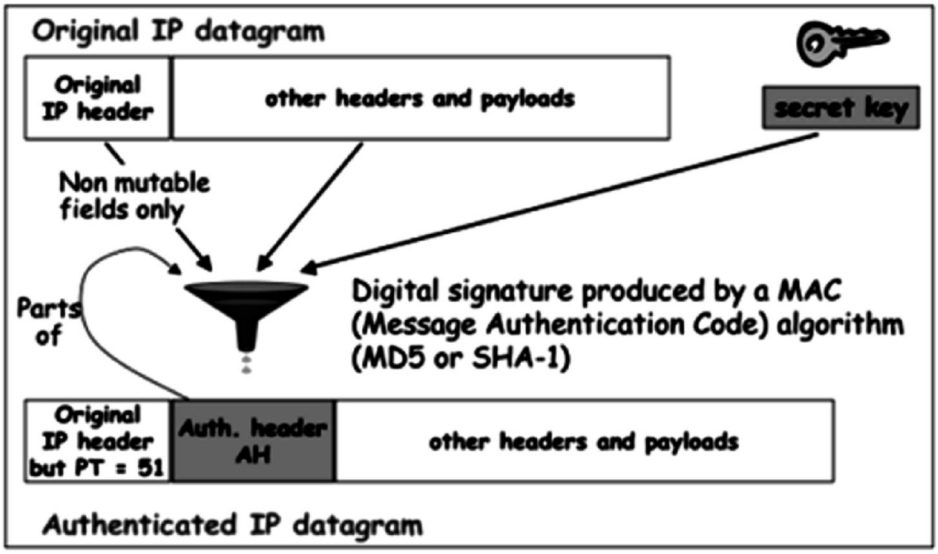
- When IP packet is received from upper protocol stack, IPsec determine the associated Security Association (SA) from available information in the packet; for example, IP address (source and destination).
- From SA, once it is identified that security protocol is AH, the parameters of AH header are calculated. The AH header consists of the following parameters:



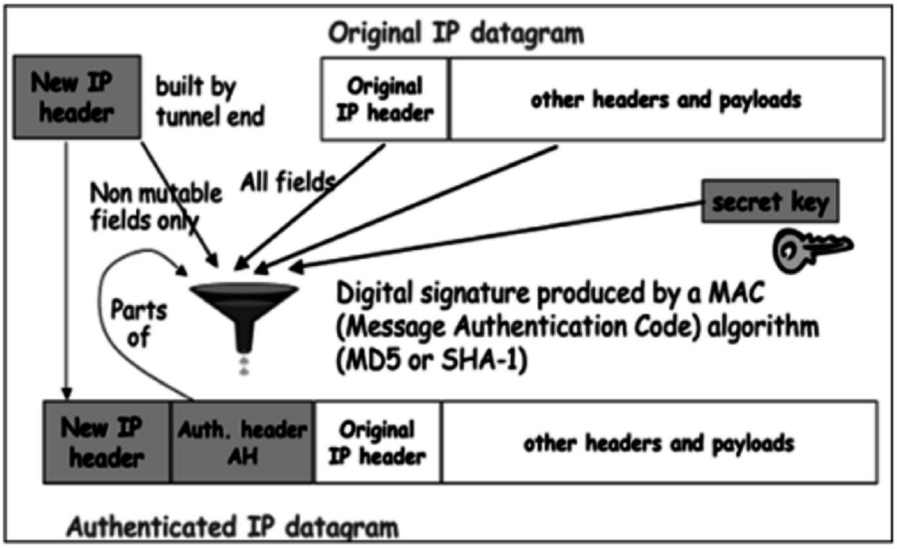
- The header field specifies the protocol of packet following AH header. Sequence Parameter Index (SPI) is obtained from SA existing between communicating parties.
- Sequence Number is calculated and inserted. These numbers provide optional capability to AH to resist replay attack.
- Authentication data is calculated differently depending upon the communication mode.

Rahul Publications

- In transport mode, the calculation of authentication data and assembling of final IP packet for transmission is depicted in the following diagram. In original IP header, change is made only in protocol number as 51 to indicated application of AH.



- In Tunnel mode, the above process takes place as depicted in the following diagram.



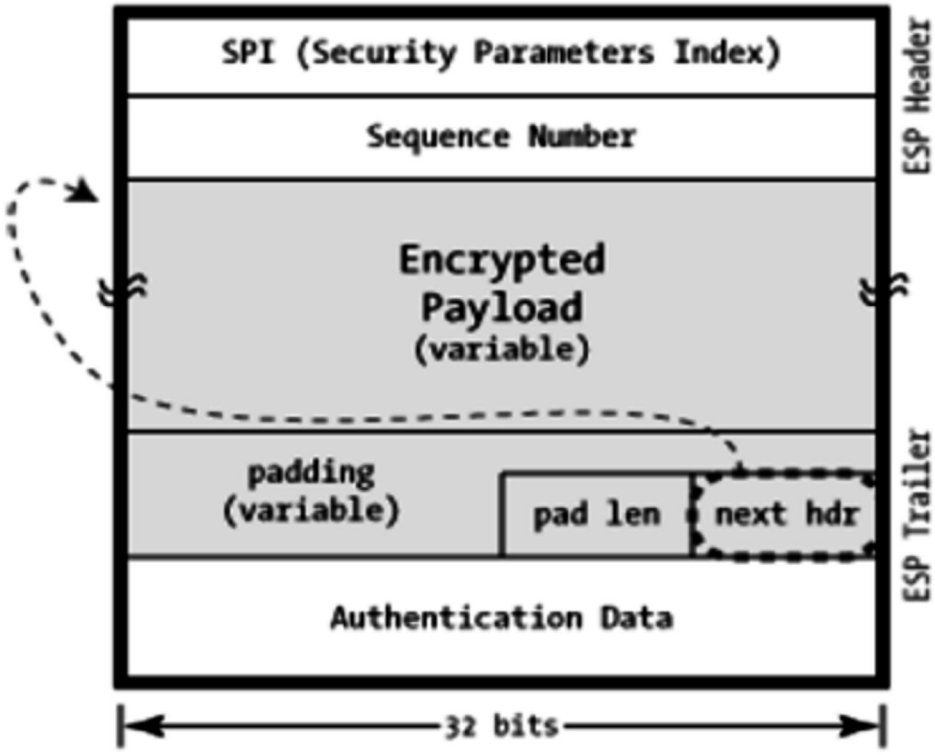
Encapsulation Security Protocol (ESP)

ESP provides security services such as confidentiality, integrity, origin authentication, and optional replay resistance. The set of services provided depends on options selected at the time of Security Association (SA) establishment.

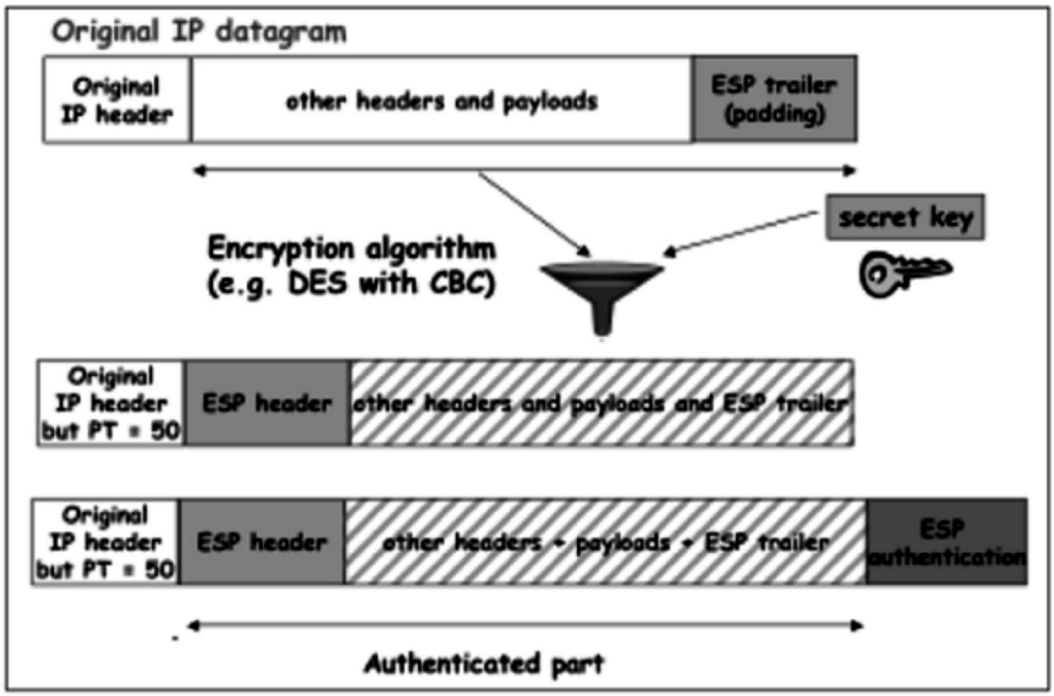
In ESP, algorithms used for encryption and generating authenticator are determined by the attributes used to create the SA.

The process of ESP is as follows. The first two steps are similar to process of AH as stated above.

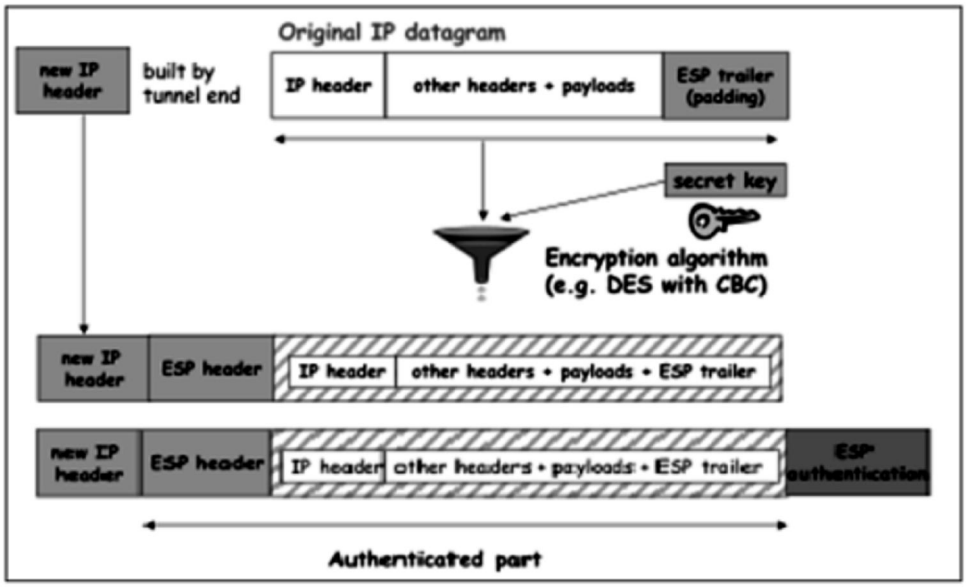
- Once it is determined that ESP is involved, the fields of ESP packet are calculated. The ESP field arrangement is depicted in the following diagram.



- Encryption and authentication process in transport mode is depicted in the following diagram.



- In case of Tunnel mode, the encryption and authentication process is as depicted in the following diagram.



Although authentication and confidentiality are the primary services provided by ESP, both are optional. Technically, we can use NULL encryption without authentication. However, in practice, one of the two must be implemented to use ESP effectively.

The basic concept is to use ESP when one wants authentication and encryption, and to use AH when one wants extended authentication without encryption.

Security Associations in IPsec

Security Association (SA) is the foundation of an IPsec communication. The features of SA are "

- Before sending data, a virtual connection is established between the sending entity and the receiving entity, called "Security Association (SA)".
- IPsec provides many options for performing network encryption and authentication. Each IPsec connection can provide encryption, integrity, authenticity, or all three services. When the security service is determined, the two IPsec peer entities must determine exactly which algorithms to use (for example, DES or 3DES for encryption; MD5 or SHA-1 for integrity). After deciding on the algorithms, the two devices must share session keys.
- SA is a set of above communication parameters that provides a relationship between two or more systems to build an IPsec session.
- SA is simple in nature and hence two SAs are required for bi-directional communications.
- SAs are identified by a Security Parameter Index (SPI) number that exists in the security protocol header.
- Both sending and receiving entities maintain state information about the SA. It is similar to TCP endpoints which also maintain state information. IPsec is connection-oriented like TCP.

Parameters of SA

Any SA is uniquely identified by the following three parameters:

- Security Parameters Index (SPI).
  - It is a 32-bit value assigned to SA. It is used to distinguish among different SAs terminating at the same destination and using the same IPsec protocol.

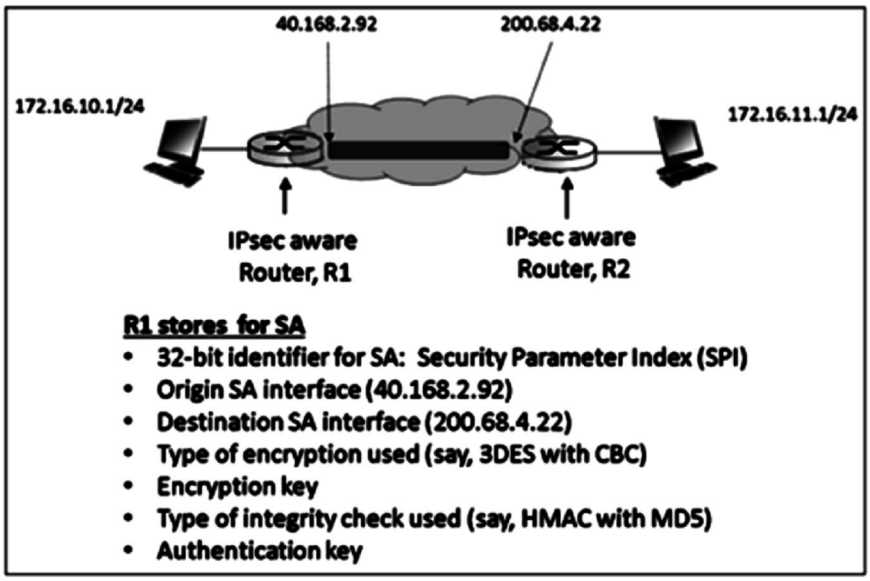
Rahul Publications

- Every packet of IPsec carries a header containing SPI field. The SPI is provided to map the incoming packet to an SA.
- The SPI is a random number generated by the sender to identify the SA to the recipient.

➢ **Destination IP Address:** It can be IP address of end router.

➢ **Security Protocol Identifier:** It indicates whether the association is an AH or ESP SA.

Example of SA between two router involved in IPsec communication is shown in the following diagram.



Security Administrative Databases

In IPsec, there are two databases that control the processing of IPsec datagram. One is the Security Association Database (SAD) and the other is the Security Policy Database (SPD). Each communicating endpoint using IPsec should have a logically separate SAD and SPD.

Any observed path maximum transmission unit (to avoid fragmentation)

All SA entries in the SAD are indexed by the three SA parameters: Destination IP address, Security Protocol Identifier, and SPI.

Security Policy Database

SPD is used for processing outgoing packets. It helps in deciding what SAD entries should be used. If no SAD entry exists, SPD is used to create new ones.

Any SPD entry would contain:

➢ Pointer to active SA held in SAD.

➢ Selector fields – Field in incoming packet from upper layer used to decide application of IPsec. Selectors can include source and destination address, port numbers if relevant, application IDs, protocols, etc.

Outgoing IP datagrams go from the SPD entry to the specific SA, to get encoding parameters. Incoming IPsec datagram get to the correct SA directly using the SPI/DEST IP/Protocol triple, and from there extracts the associated SAD entry.

SPD can also specify traffic that should bypass IPsec. SPD can be considered as a packet filter where the actions decided upon are the activation of SA processes.

Short Question and Answers

1. Data Encryption Standard.

Ans :

Data Encryption Standard (DES) is the symmetric block cipher which encrypts a 64-bit plain text in a 64-bit ciphertext.

The DES was introduced by the National Institute of Standard and Technology (NIST) in the 1970s. Initially, DES was only used in financial applications but later it was accepted as the cryptographic algorithm by other organizations too.

Being a symmetric cipher the same key is used in encryption and decryption process of DES. In this context, we will discuss the steps performed in DES and we will also discuss the advantages and disadvantages of DES.

2. Asymmetric key cryptography.

Ans :

When the two parties communicate to each other to transfer the intelligible or sensible message, referred to as plaintext, is converted into apparently random nonsense for security purpose referred to as ciphertext.

Encryption:

The process of changing the plaintext into the ciphertext is referred to as encryption.

The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext.

The security of conventional encryption depends on the major two factors:

(i) The Encryption algorithm

(ii) Secrecy of the key

Once the ciphertext is produced, it may be transmitted. The Encryption algorithm will produce a different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm.

Once the ciphertext is produced, it may be transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

3. Message Authentication service.

Ans :

Message authentication ensures that the message has been sent by a genuine identity and not by an imposter.

- The service used to provide message authentication is a Message Authentication Code (MAC).
- A MAC uses a keyed hash function that includes the symmetric key between the sender and receiver when creating the digest.
- Figure shows how a sender A uses a keyed hash function to authenticate his message and how the receiver B can verify the authenticity of the message.
- This system makes use of a symmetric key shared by A and B.
- A, using this symmetric key and a keyed hash function, generates a MAC.
- A then sends this MAC along with the original message to B.

  B receives the message and the MAC and separates the message from the MAC.
- B then applies the same keyed hash function to the message using the same symmetric key to get a fresh MAC.
- B then compares the MAC sent by A with the newly generated MAC.
- If the two MACs are identical, it shows that the message has not been modified and the sender of the message is definitely A.

4. What is digital signature?

Ans :

A digital signature is a mathematical technique which validates the authenticity and integrity of a message, software or digital documents. It allows us to verify the author name, date and time of signatures, and authenticate the message contents. The digital signature offers far more inherent security and intended to solve the problem of tampering and impersonation (Intentionally copy another person's characteristics) in digital communications.

Rahul Publications

The computer-based business information authentication interrelates both technology and the law. It also calls for cooperation between the people of different professional backgrounds and areas of expertise. The digital signatures are different from other electronic signatures not only in terms of process and result, but also it makes digital signatures more serviceable for legal purposes. Some electronic signatures that legally recognizable as signatures may not be secure as digital signatures and may lead to uncertainty and disputes.

5. Types of Digital Signature.

Ans :

Different document processing platform supports different types of digital signature. They are described below:

- **Certified Signatures**

  The certified digital signature documents display a unique blue ribbon across the top of the document. The certified signature contains the name of the document signer and the certificate issuer which indicate the authorship and authenticity of the document.

- **Approval Signatures**

  The approval digital signatures on a document can be used in the organization's business workflow. They help to optimize the organization's approval procedure. The procedure involves capturing approvals made by us and other individuals and embedding them within the PDF document. The approval signatures to include details such as an image of our physical signature, location, date, and official seal.

- **Visible Digital Signature**

  The visible digital signature allows a user to sign a single document digitally. This signature appears on a document in the same way as signatures are signed on a physical document.

- **Invisible Digital Signature**

  The invisible digital signatures carry a visual indication of a blue ribbon within a document in the taskbar. We can use invisible digital signatures when we do not have or do not want to display our signature but need to provide the authenticity of the document, its integrity, and its origin.

6. What is a Firewall?

Ans :

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

7. Types of Firewall.

Ans :

(i) Packet-filtering Firewalls

A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules. These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.

While packet-filtering firewalls can be considered a fast solution without many resource requirements, they also have some limitations. Because these types of firewalls do not prevent web-based attacks, they are not the safest.

(ii) Circuit-level Gateways

Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources. These types of firewalls typically operate at the session-level of the OSI model by verifying

TCP (Transmission Control Protocol)connections and sessions. Circuit-level gateways are designed to ensure that the established sessions are protected.

Typically, circuit-level firewalls are implemented as security software or pre-existing firewalls. Like packet-filtering firewalls, these firewalls do not check for actual data, although they inspect information about transactions. Therefore, if a data contains malware, but follows the correct TCP connection, it will pass through the gateway. That is why circuit-level gateways are not considered safe enough to protect our systems.

(iii) Application-level Gateways (Proxy Firewalls)

Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called 'Application-level Gateways'.

Rahul Publications

Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks. Once the connection is established, the proxy firewall inspects data packets coming from the source. If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client. This approach creates an additional layer of security between the client and many different sources on the network.

(iv) Stateful Multi-layer Inspection (SMLI) Firewalls

Stateful multi-layer inspection firewalls include both packet inspection technology and TCP handshake verification, making SMLI firewalls superior to packet-filtering firewalls or circuit-level gateways. Additionally, these types of firewalls keep track of the status of established connections.

In simple words, when a user establishes a connection and requests data, the SMLI firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc. Connection information is stored for each session in the state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.

(v) Next-generation Firewalls (NGFW)

Many of the latest released firewalls are usually defined as 'next-generation firewalls'. However, there is no specific definition for next-generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include deep-packet inspection (DPI), surface-level packet inspection, and TCP handshake testing, etc.

NGFW includes higher levels of security than packet-filtering and stateful inspection firewalls. Unlike traditional firewalls, NGFW monitors the entire transaction of data, including packet headers, packet contents, and sources. NGFWs are designed in such a way that they can prevent more sophisticated and evolving security threats such as malware attacks, external threats, and advance intrusion.

8. What is firewall management?

Ans :

Firewall management is the process of configuring and monitoring a firewall to maintain a secure network. Firewalls are an integral part of protecting private networks in both a personal and business setting.

An organization may have many different firewalls protecting its devices and network as standard. Management of these firewalls means setting rules and policies, tracking changes, and monitoring compliance logs. It also includes the monitoring of user access to firewall settings. The configuration ensures the firewall functions securely and efficiently.

Any size organization which has a private network will utilize a firewall to protect their systems. This could be a large contractor subject to Cybersecurity Maturity Model Certification (CMMC) or a small office-based network. Firewalls are an important aspect of cybersecurity, so form a key area of IT security policies. The final responsibility for firewall management is held by those leading the organization's IT security or compliance efforts.

9. What is VPN? Explain about VPN security.

Ans :

VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. In other words, A Virtual Private Network is a connection method used to add security and privacy to private and public networks.

In very simple terms, a virtual private network connects your PC, smartphone, or tablet to another computer (called a server) somewhere on the internet, and allows you to browse the internet using that computer's internet connection.

10. Pretty Good Privacy (PGP).

Ans :

Pretty Good Privacy (PGP) is an e-mail encryption scheme. It has become the de-facto standard for providing security services for e-mail communication.

Rahul Publications

As discussed above, it uses public key cryptography, symmetric key cryptography, hash function, and digital signature. It provides:

- Privacy
- Sender Authentication
- Message Integrity
- Non-repudiation

11. S / MIME.

Ans :

S/MIME stands for Secure Multipurpose Internet Mail Extension. S/MIME is a secure e-mail standard. It is based on an earlier non-secure e-mailing standard called MIME.

Working of S/MIME

S/MIME approach is similar to PGP. It also uses public key cryptography, symmetric key cryptography, hash functions, and digital signatures. It provides similar security services as PGP for e-mail communication.

The most common symmetric ciphers used in S/MIME are RC2 and TripleDES. The usual public key method is RSA, and the hashing algorithm is SHA-1 or MD5.

S/MIME specifies the additional MIME type, such as "application/pkcs7-mime", for data enveloping after encrypting. The whole MIME entity is encrypted and packed into an object. S/MIME has standardized cryptographic message formats (different from PGP). In fact, MIME is extended with some keywords to identify the encrypted and/or signed parts in the message.

S/MIME relies on X.509 certificates for public key distribution. It needs top-down hierarchical PKI for certification support.

12. Explain briefly about TLS Protocol.

Ans :

In order to provide an open Internet standard of SSL, IETF released The Transport Layer Security (TLS) protocol in January 1999. TLS is defined as a proposed Internet Standard in RFC 5246.

Features

- TLS protocol has same objectives as SSL.
- It enables client/server applications to communicate in a secure manner by authenticating, preventing eavesdropping and resisting message modification.
- TLS protocol sits above the reliable connection-oriented transport TCP layer in the networking layers stack.
- The architecture of TLS protocol is similar to SSLv3 protocol. It has two sub protocols: the TLS Record protocol and the TLS Handshake protocol.
- Though SSLv3 and TLS protocol have similar architecture, several changes were made in architecture and functioning particularly for the handshake protocol.

Rahul Publications

Choose the Correct Answers

1. It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the _____. [b]

   (a) Antivirus (b) Firewall

   (c) Cookies (d) Malware

2. Using the cipher algorithm, which of these types of text would be transformed? [a]

   (a) Plain text (b) Scalar text

   (c) Complex text (d) Transformed text

3. The response time and transit time is used to measure the _____ of a network. [d]

   (a) Security (b) Longevity

   (c) Reliability (d) Performance

4. In the computer networks, the encryption techniques are primarily used for improving the _____. [a]

   (a) Security (b) Performance

   (c) Reliability (d) Longevity

5. Which of the following statements is true about the VPN in Network security? [d]

   (a) It is a type of device that helps to ensure that communication between a device and a network is secure.

   (b) It is usually based on the IPsec(IP Security) or SSL (Secure Sockets Layer)

   (c) It typically creates a secure, encrypted virtual “tunnel” over the open internet

   (d) All of the above

6. In order to ensure the security of the data/ information, we need to _____ the data: [a]

   (a) Encrypt (b) Decrypt

   (c) Delete (d) None of the above

7. A transposition cipher reorders (permutes) symbols in a _____. [d]

   (a) block of packets (b) block of slots

   (c) block of signals (d) block of symbols

8. The DES Algorithm Cipher System consists of _____ rounds (iterations) each with a round key [d]

   (a) 12 (b) 18

   (c) 9 (d) 16

9. Which of the following modes of operation in DES is used for operating? [c]

   (a) Cipher Feedback Mode (CFB) (b) Cipher Block chaining (CBC)

   (c) Electronic code book (ECB) (d) Output Feedback Modes (OFB)

10. Which authentication method uses two separate factors before being granted access to provide significantly more security than simply using a single password [c]

    (a) Certificate authentication (b) LDAP authentication

    (c) Two Factor Authentications (d) None of the above

Rahul Publications

Fill in the blanks

1. _____ is a method of storing and transmitting data in a particular form.
2. _____ is the process of transforming plain text into unreadable text.
3. The process of changing the ciphertext to the plaintext that process is known as _____.
4. An asymmetric-key (or public-key) cipher uses _____.
5. The RSA algorithm is a _____ algorithm that uses a random number generator.
6. A MAC uses a _____ function that includes the symmetric key between the sender and receiver when creating the digest.
7. _____ is the process of configuring and monitoring a firewall to maintain a secure network.
8. A _____ method ensures that a user is transparently authenticated to a firewall or a network even without having to actively log in.
9. Full form of VPN _____.
10. _____ protocol is used for forwarding e-mail messages.

ANSWERS

1. Cryptography
2. encryption
3. decryption
4. 2 keys
5. symmetric cryptography
6. keyed hash
7. Firewall management
8. single sign on
9. Virtual Private Network
10. Simple mail Transfer Protocol (SMTP)

Rahul Publications

UNIT V

Cyberspace and The Law, Cyber Forensics:

Cyberspace and The Law: Introduction, Cyber Security Regulations, Roles of International Law, the state and Private Sector in Cyberspace, Cyber Security Standards. The INDIAN Cyberspace, NationalCyber Security Policy 2013.

Cyber Forensics: Introduction to Cyber Forensics, Handling Preliminary Investigations, Controlling anInvestigation, Conducting disk-based analysis, Investigating Information-hiding, Scrutinizing E-mail,Validating E-mail header information, Tracing Internet access, Tracing memory in real-time.

5.1 Cyberspace and The Law

5.1.1 Introduction

Q1. Define Cyber space and cyber law. Explain the importance of cyber law.

Ans : **(Imp.)**

1. Cyber space

Cyber space can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyber space today has become a common pool used by citizens, businesses, critical information infrastructure, military and govern- ments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyber space is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

2. Cyber law

Cyber law is the type of law that deals with the relationship of the internet to the technological and electronic elements such as software, information system (IS), hardware, and computers. It is nothing but a part of a legal system that deals with the cyber space, internet and their legal issues.

Importance

Cyber law is used by smaller business organizations which are extremely vulnerable because of the ineffective cyber security. It is very important to all types of business organizations, particularly when you think about the importance or advantages of the internet as well as digital systems are for your day-to-day operations. There are various reasons for which Cyber Law, is very important, are listed below;

- **It allows employees to work safely**

  With the help of cyber law, you and the employees of your company haven't got any risk from a potential cyber attack. If your system becomes infected than that can really hamper their productivity.

- **It can protect your business**

  This is one of the biggest factors, because of which cyber law is very important. It allows the employees to surf the internet as and when they require it. You have to ensure that they can't at risk from potential threats.

- **It protects the personal information of the user**

  One of the most important factors in the digital world is to keep your personal information secret. It is very essential for the customer that they are quite capable of selling the information.

- **It protects productivity**

  There are many viruses present which can slow down your personal computer. It may often bring your personal business to a standstill.

Rahul Publications

5.1.2 Cyber Security Regulations

Q2. Explain cyber security regulations.

Ans : **(Imp.)**

Regulations

There are five predominant laws to cover when it comes to cyber security:

Information Technology Act, 2000 The Indian cyber laws are governed by the Information Technology Act, penned down back in 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to eCommerce, facilitating registration of real-time records with the Government.

But with the cyber attackers getting sneakier, topped by the human tendency to misuse technology, a series of amendments followed.

The ITA, enacted by the Parliament of India, highlights the grievous punishments and penalties safeguarding the e-governance, e-banking, and e-commerce sectors. Now, the scope of ITA has been enhanced to encompass all the latest communication devices.

The IT Act is the salient one, guiding the entire Indian legislation to govern cyber crimes rigorously:

- **Section 43**

  Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.

- **Section 66**

  Applicable in case a person is found to dishonestly or fraudulently committing any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.

- **Section 66B**

  Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by Rs. 1 lakh fine, depending upon the severity.

- **Section 66C**

  This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs.1 lakh fine.

- **Section 66 D**

  This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

Indian Penal Code (IPC) 1980

Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000.

The primary relevant section of the IPC covers cyber frauds:

- Forgery (Section 464)
- Forgery pre-planned for cheating (Section 468)
- False documentation (Section 465)
- Presenting a forged document as genuine (Section 471)
- Reputation damage (Section 469)

Companies Act of 2013

The corporate stakeholders refer to the Companies Act of 2013 as the legal obligation necessary for the refinement of daily operations. The directives of this Act cements all the required techno-legal compliances, putting the less compliant companies in a legal fix.

The Companies Act 2013 vested powers in the hands of the SFIO (Serious Frauds Investigation Office) to prosecute Indian companies and their directors. Also, post the notification of the Companies Inspection, Investment, and Inquiry Rules, 2014, SFIOs has become even more proactive and stern in this regard.

The legislature ensured that all the regulatory compliances are well-covered, including cyber forensics, e-discovery, and cyber security diligence.

Rahul Publications

The Companies (Management and Administration) Rules, 2014 prescribes strict guidelines confirming the cyber security obligations and responsibilities upon the company directors and leaders.

NIST Compliance

The Cyber security Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cyber security as the most reliable global certifying body.

NIST Cyber security Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly. This framework is prioritized on flexibility and cost-effectiveness.

It promotes the resilience and protection of critical infrastructure by: Allowing better interpretation, management, and reduction of cyber security risks – to mitigate data loss, data misuse, and the subsequent restoration costs Determining the most important activities and critical operations - to focus on securing them Demonstrates the trust-worthiness of organizations who secure critical assets Helps to prioritize investments to maximize the cybersecurity ROI Addresses regulatory and contractual obligations Supports the wider information security program .

Final Thoughts As human dependence on technology intensifies, cyber laws in India and across the globe need constant up-gradation and refinements. The pandemic has also pushed much of the workforce into a remote working module increasing the need for app security. Lawmakers have to go the extra mile to stay ahead of the impostors, in order to block them at their advent.

Cyber crimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users. Only the prudent efforts of these stakeholders, ensuring their confinement to the law of the cyber land - can bring about online safety and resilience.

5.1.3 Roles of International Law

Q3. Write about the roles of international cyber law.

Ans : **(Imp.)**

In various countries, areas of the computing and communication industries are regulated by governmental bodies

- There are specific rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming
- There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes
- There are laws governing trade on the Internet, taxation, consumer protection, and advertising
- There are laws on censorship versus freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies
- Some states limit access to the Internet, by law as well as by technical means.

International Law For Cyber Crime

Cyber crime is “international” that there are ‘no cyber-borders between countries’

- The complexity in types and forms of cyber crime increases the difficulty to fight back
- fighting cybercrime calls for international cooperation
- Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale.

Rahul Publications

5.1.4 The state and private sector in cyber space

Q4. Write about the roles of state and private sector in cyber space.

Ans : **(Imp.)**

Roles and Responsibilities defined by the Private Sector cluster

Assumed Roles and Responsibilities

The following roles and responsibilities have thus far been agreed by the private sector in developed initiatives and attempts at self-regulation:

Awareness raising among the wider pool of end-users and the developer community on threats and protection methods. Special focus of some initiatives is placed on the Internet of Things (IoT).

- Capacity building of the private sector and the general public through education and engagement in public-private partnerships
- Cooperation through information sharing on best practice and vulnerabilities.
- Norm development for the industry through standardisation, focused on software assurance and secure development practices ('security by design' standards).
- Ensuring security of end-users, primarily through 'security by design' principles, prioritising security, privacy, integrity and reliability.
- Responsible behaviour, namely through transparency. Recent examples include pledges to inform users of potential account attacks and breaches by suspected state-sponsored actors.

Negative responsibilities of the private sector refer to agreements not to aid governments in launching cyber attacks

Advocated Roles and Responsibilities

The following roles and responsibilities have thus far been proposed by the private sector in developed initiatives and attempts at self-regulation:

- Cooperation at the international level, primarily through information sharing on incidents, as well as coordination of vulnerability responses.
- Norm development through development of shared principles and standards aimed at selfregulation.
- Engagement in public-private partnerships aimed at providing cyber security through provision of support to authorities, incident response and policy input.
- Ensure security, both own and that of end-users, through abiding by 'security by design' principles, including products, functionalities, processes, technologies, operations, architectures, and business models, as well as standardisation and engagement in public-private cooperation.
- Policy development in terms of providing policy input and technical expertise to make policies developed feasible.
- Responsible behaviour through practicing restraint by limiting support to governments to genuinely defensive scenarios.
- Suggested negative responsibilities relate to not aiding attacks on end-users anywhere.

Roles and Responsibilities of the Private Sector suggested by other actor clusters

States have thus far argued that the private sector should, among other, bear the responsibility of:

Capacity building through training and education of technology security experts, as well as bolstering the capacities of small and medium enterprise and individuals.

- Norm development through developing codes of practice by 'peak industry groups' as well as technical standards to protect security.
- Ensuring security, primarily its own, through capacity building and adopting adequate levels of cyber security safeguards in business practice, including adoption of 'security by

Rahul Publications

design' principles as well as through engagement in public-private partnerships.

- Responsible behaviour, ensuring that security measures included in ICT products and services do not undermine human rights, abiding also by principles of transparency and accountability accordingly.
- Expert communities and users have thus far argued that the private sector should, among other, bear the responsibility of: - Adopting a cyber security framework, developing policies based on existing legislation.
- Capacity building of the workforce through education.
- Cooperation through information sharing, establishing potentially a formal legal regime
- but primarily assist public sector efforts to proactively defend against cyber attacks and minimize the duration and impact of such attacks
- Norm development, as a bottom-up approach, primarily through standardisation.
- Ensuring security, primarily their own, though acting on intelligence obtained, correcting software vulnerabilities, adopting 'security by design' principles and encryption.
- Seen as providing the first line of security by some actors the private sector is further expected to engage in information sharing and threat awareness to fulfil this role, responsibly developing patch management processes and keeping software up to date.
- One specific claims that private sector actors are better positioned than most national governments to develop real-time threat awareness, contributing thus to the maintenance of cyber defence postures.
- Responsible behaviour mainly in term of negative responsibilities of not engaging in activities damaging the stability of cyberspace, trafficking in cyber vulnerabilities for offensive purposes,attacking the information infra-structure or exploiting users.
- Optimisation of data collected is also seen as an element of responsible behaviour.
- A specific task attributed to the private sector is to also ensure that the role of Computer Emergency Response Teams is by no means politicised.
- Additionally, academic actors have suggested that private sector should develop public-private partnerships enabling this actor cluster to gain access to the experience it lacks and develop better comprehension of its own responsibilities.
- Civil society actors have also recognised that the private sector has thus far already engaged in norm development through promoting standards as well as general efforts aimed policy development through provision of policy input and technical expertise.

Should the state have a greater role in private sector claims of attribution?

- A greater role for the government in responding to private sector claims of attribution has been argued as potentially increasing accountability.
- The government's heightened responsibility would, in this view, increase its own accountability, as well as that of the private sector, through scrutiny of its attribution claim.
- Should the state have a greater role in private sector claims of attribution and what effect could this potentially have on the private sector in return?
- Can national normative frameworks socialise norms at the international level? Even among like-minded countries, understandings and approaches to issues such as cyber security or human rights such as privacy vary, despite the fact that end-users' expectations generally do not
- National legislative frameworks that have cross-border effects on the other hand necessitate changes in domestic normative frameworks of other countries – an example being EU's General Data Protection Regulation

Rahul Publications

- How effectively can national normative frameworks push for adoption of principles and standards on a wider international scale, ultimately establishing specific patterns and norms of behavior?

5.1.5 Cyber security standards

Q5. What are cyber security standards? Explain various cyber security stand ards.

Ans : **(Imp.)**

To make cyber security measures explicit, the written norms are required. These norms are known as cyber security standards: the generic sets of prescriptions for an ideal execution of certain measures. The standards may involve methods, guidelines, reference frameworks, etc. It ensures efficiency of security, facilitates integration and interoperability, enables meaningful comparison of measures, reduces complexity, and provide the structure for new developments.

A security standard is "a published specification that establishes a common language, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition." The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. The Well-Written cyber security standards enable consistency among product developers and serve as a reliable standard for purchasing security products.

Security standards are generally provided for all organizations regardless of their size or the industry and sector in which they operate. This section includes information about each standard that is usually recognized as an essential component of any cyber security strategy.

ISO

ISO stands for International Organization for Standardization. International Standards make things to work. These standards provide a world-class specification for products, services and computers, to ensure quality, safety and efficiency. They are instrumental in facilitating international trade.

ISO standard is officially established On 23 February 1947. It is an independent, non-governmental international organization. Today, it has a membership of 162 national standards bodies and 784 technical committees and subcommittees to take care of standards development. ISO has published over 22336 International Standards and its related documents which covers almost every industry, from information technology, to food safety, to agriculture and healthcare.

1. ISO 27000 Series

It is the family of information security standards which is developed by the International Organization for Standardization and the International Electrotechnical Commission to provide a globally recognized framework for best information security management. It helps the organization to keep their information assets secure such as employee details, financial information, and intellectual property.

The need of ISO 27000 series arises because of the risk of cyber-attacks which the organization face. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology.

The ISO 27000 series can be categorized into many types. They are-

- **ISO 27001**

This standard allows us to prove the clients and stakeholders of any organization to managing the best security of their confidential data and information. This standard involves a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving our ISMS.

- **ISO 27000**

This standard provides an explanation of terminologies used in ISO 27001.

- **ISO 27002**

This standard provides guidelines for organizational information security standards and information security management

Rahul Publications

practices. It includes the selection, implementation, operating and management of controls taking into consideration the organization's information security risk environment(s).

- **ISO 27005**

This standard supports the general concepts specified in 27001. It is designed to provide the guidelines for implementation of information security based on a risk management approach. To completely understand the ISO/IEC 27005, the knowledge of the concepts, models, processes, and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is required. This standard is capable for all kind of organizations such as non-government organization, government agencies, and commercial enterprise

- **ISO 27032**

It is the international Standard which focuses explicitly on cyber security. This Standard includes guidelines for protecting the information beyond the borders of an organization such as in collaborations, partnerships or other information sharing arrangements with clients and suppliers.

2. IT Act

The Information Technology Act also known as ITA-2000, or the IT Act main aims is to provide the legal infrastructure in India which deal with cybercrime and e-commerce. The IT Act is based on the United Nations Model Law on E-Commerce 1996 recommended by the General Assembly of United Nations. This act is also used to check misuse of cyber network and computer in India. It was officially passed in 2000 and amended in 2008. It has been designed to give the boost to Electronic commerce, e-transactions and related activities associated with commerce and trade. It also facilitate electronic governance by means of reliable electronic records.

IT Act 2000 has 13 chapters, 94 sections and 4 schedules. The first 14 sections concerning digital signatures and other sections deal with the certifying authorities who are licenced to issue digital signature certificates, sections 43 to 47 provides penalties and compensation, section 48 to 64 deal with appeal to high court, sections 65 to 79 deal with offences, and the remaining section 80 to 94 deal with miscellaneous of the act.

3. Copyright Act

The Copyright Act 1957 amended by the Copyright Amendment Act 2012 governs the subject of copyright law in India. This Act is applicable from 21 January 1958. Copyright is a legal term which describes the ownership of control of the rights to the authors of "original works of authorship" that are fixed in a tangible form of expression. An original work of authorship is a distribution of certain works of creative expression including books, video, movies, music, and computer programs. The copyright law has been enacted to balance the use and reuse of creative works against the desire of the creators of art, literature, music and monetize their work by controlling who can make and sell copies of the work.

The copyright act covers the following-

- Rights of copyright owners
- Works eligible for protection
- Duration of copyright
- Who can claim copyright

The copyright act does not covers the following-

- Ideas, procedures, methods, processes, concepts, systems, principles, or discoveries
- Works that are not fixed in a tangible form (such as a choreographic work that has not been notated or recorded or an improvisational speech that has not been written down)

Rahul Publications

- Familiar symbols or designs
- Titles, names, short phrases, and slogans
- Mere variations of typographic or namentation, lettering, or coloring.

4. Patent Law

Patent law is a law that deals with new inventions. Traditional patent law protect tangible scientific inventions, such as circuit boards, heating coils, car engines, or zippers. As time increases patent law have been used to protect a broader variety of inventions such as business practices, coding algorithms, or genetically modified organisms. It is the right to exclude others from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.

In general, a patent is a right that can be granted if an invention is:

- Rights of copyright owners
- Works eligible for protection
- Duration of copyright
- Who can claim copyright

The copyright act does not covers the following-

- Ideas, procedures, methods, processes, concepts, systems, principles, or discoveries
- Works that are not fixed in a tangible form (such as a choreographic work that has not been notated or recorded or an improvisational speech that has not been written down)
- Familiar symbols or designs
- Titles, names, short phrases, and slogans
- Mere variations of typographic or namentation, lettering, or coloring.

5.1.6 The indian cyber space

Q6. What is the aim of Indian cyber space? Why Indian cyber space is more vulnerable for attacks.

Ans :

Indian cyber space was born in 1975 with the establishment of National Informatics Centre (NIC) with an aim to provide govt with IT solutions.

Three networks (NWs) were set up between 1986 and 1988 to connect various agencies of govt. These NWs were, INDONET which connected the IBM mainframe installations that made up India's computer infrastructure, NICNET (the NIC NW) a nationwide very small aperture terminal (VSAT) NW for public sector organizations as well as to connect the central govt with the state govts and district administrations, the third NW setup was ERNET (the Education and Research Network), to serve the academic and research communities.

New Internet Policy of 1998 paved the way for services from multiple Internet service providers (ISPs) and gave boost to the Internet user base grow from 1.4 million in 1999 to over 150 million by Dec 2012. Exponential growth rate is attributed to increasing Internet access through mobile phones and tablets.

Govt is making a determined push to increase broadband penetration from its present level of about 6%1. The target for broadband is 160 million households by 2016 under the National Broadband Plan.

People in India are vulnerable to cyber-attacks due to the lack of cyber hygiene. The country needs to be alert, and any laxity can have severe consequences, experts warn.

There have been attempts from time to time to launch cyber-attacks on Indian cyber space," Sanjay Dhotre, Minister of State for Electronics and Information Technology had said in a reply to the RajyaSabha on February 11, while sharing the above data.

"It has been observed that attackers are compromising computer systems located in different parts of the world and use masquerading techniques

Rahul Publications

and hidden servers to hide the identity of actual systems from which the attacks are being launched."

Official tracing and analysis reveals that the Internet Protocol or IP addresses of the computers from where the attacks originate belong to various countries, including Algeria, Brazil, China, France, Indonesia, Netherlands, North Korea, Pakistan, Russia, Serbia, South Korea, Taiwan, Thailand, Tunisia, Turkey, the US and Vietnam, Minister Dhotre said in his reply.

In 2019, 54 websites of central ministries, departments and State governments were hacked, down from 110 in 2018 and 172 in 2017.

With the recent revelations of rising cyber-attacks and attempts on government installations and utilities, experts warn that India needs to take cyber security seriously. North Korea, Russia and China are notorious in carrying out such attacks, says AtulKahate, a cryptography and network security expert.

5.1.7 National Cyber Security Policy 2013

Q7. What is the National Cyber Security Policy? Explain about it.

Ans : **(Imp.)**

The National Cyber Security Policy is a policy document drafted by the Department of Electronics and Information Technology (DeitY) in 2013 aimed at protecting the public and private infrastructure from cyber attacks.

The guideline also seeks to protect the personal information of internet users, financial and banking information, and sovereign data .

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology (DeitY) It aims at protecting the public and private infrastructure from cyber attacks.

The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". Ministry of Communications and Information Technology (India) defines Cyber space as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

Need for a cyber security policy

- Before 2013, India did not have a cybersecurity policy. The need for it was felt during the NSA spying issue that surfaced in 2013.
- Information empowers people and there is a need to create a distinction between information that can run freely between systems and those that need to be secured. This could be personal information, banking and financial details, security information which when passed onto the wrong hands can put the country's safety in jeopardy.
- This Policy has been drafted in consultation with all the stakeholders.
- In order to digitise the economy and promote more digital transactions, the government must be able to generate trust in people in the Information and Communications Technology systems that govern financial transactions.
- A strong integrated and coherent policy on cyber security is also needed to curb the menace of cyber terrorism.

National Cyber Security Policy Vision

To build secure and resilient cyber space for citizens, businesses and Government.

National Cyber Security Policy Mission

- To protect information and information infrastructure in cyber space.
- To build capabilities to prevent and respond to cyber threats.
- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

To know how Upgrading India's cyber security architecture will boost national security for India, visit the linked article.

National Cyber Security Policy Objectives

- Encouraging the adoption of IT in all sectors of the economy by creating adequate trust

Rahul Publications

in IT systems by the creation of a secure cyber ecosystem.

- Creating an assurance framework for the design of security policies and for the promotion and enabling actions for compliance with global security standards and best practices through conformity assessment.
- Bolstering the regulatory framework for ensuring a secure cyber space ecosystem.
- Enhancing and developing national and sectoral level 24 x 7 mechanisms for obtaining strategic information concerning threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.
- Operating a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC) to improve the protection and resilience of the country's critical infrastructure information.
- Developing suitable indigenous security technologies to address requirements in this field.
- Improving the visibility of the ICT (Information and Communication Technology) products/services' integrity by having testing and validation infrastructure.
- Creating a workforce of 500,000 professionals skilled in cyber security in the next 5 years.
- Providing businesses with fiscal benefits for adopting standard security practices and processes.
- Safeguarding of the privacy of citizen's data and reducing economic losses due to cybercrime or data theft.
- Enabling effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through legislative intervention.
- Developing a culture of cyber security and privacy.
- Developing effective public-private partnerships and collaborative engagements by means of technical and operational cooperation.
- Promoting global cooperation by encouraging shared understanding and leveraging relationships for furthering the cause of security of cyber space.

5.2 Cyber Forensics

5.2.1 Introduction to Cyber Forensics

Q8. What is cyber forensics ? Explain computer forensic services?

Ans : **(Imp.)**

Computer forensics is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence.

- Computer forensics also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination.
- Computer evidence can be useful in criminal cases, civil disputes, and human resources/ employment proceedings.

Use of Computer Forensics in Law Enforcement

Computer forensics assists in Law Enforcement. This can include:

- Recovering deleted files such as documents, graphics, and photos.
- Searching unallocated space on the hard drive, places where an abundance of data often resides.
- Tracing artifacts, those tidbits of data left behind by the operating system. Our experts know how to find these artifacts and, more importantly, they know how to evaluate the value of the information they find.

Rahul Publications

- Processing hidden files files that are not visible or accessible to the user that contain past usage information. Often, this process requires reconstructing and analyzing the date codes for each file and determining when each file was created, last modified, last accessed and when deleted.
- Running a string-search for e-mail, when no e-mail client is obvious.

Computer Forensics Services

Computer forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case.

For example, they should be able to perform the following services:

1. Data Seizure

- Following federal guidelines, computer forensics experts should act as the representative, using their knowledge of data storage technologies to track down evidence.
- The experts should also be able to assist officials during the equipment seizure process.

2. Data Duplication/Preservation

When one party must seize data from another, two concerns must be addressed:

- The data must not be altered in any way
- The seizure must not put an undue burden on the responding party

The computer forensics experts should acknowledge both of these concerns by making an exact duplicate of the needed data.

When experts works on the duplicate data, the integrity of the original is maintained.

3. Data Recovery

Using proprietary tools, your computer forensics experts should be able to safely recover and analyze otherwise inaccessible evidence.

The ability to recover lost evidence is made possible by the expert's advanced under standing of storage technologies.

4. Document Searches

- Computer forensics experts should also be able to search over 200,000 electronic documents in seconds rather than hours.
- The speed and efficiency of these searches make the discovery process less complicated and less intrusive to all parties involved.

5. Media Conversion

- Computer forensics experts should extract the relevant data from old and un-readable devices, convert it into readable formats, and place it onto new storage media for analysis.

6. Expert Witness Services

- Computer forensics experts should be able to explain complex technical processes in an easy-to- understand fashion.
- This should help judges and juries comprehend how computer evidence is found, what it consists of, and how it is relevant to a specific situation.

7. Computer Evidence Service Options

- Computer forensics experts should offer various levels of service, each designed to suit your individual investigative needs. For example, they should be able to offer the following services:
- **Standard service:** Computer forensics experts should be able to work on your case during normal business hours until your critical electronic evidence is found.
- **On-site service:** Computer forensics experts should be able to travel to your location to perform complete computer evidence services. While on-site, the experts should quickly be able to produce exact duplicates of the data storage media in question.
- **Emergency service:** Your computer forensics experts should be able to give your case the highest priority in their laboratories. They should be able to work on it without interruption until your evidence objectives are met.

Rahul Publications

- **Priority service:** Dedicated computer forensics experts should be able to work on your case during normal business hours (8:00 A.M. to 5:00 P.M., Monday through Friday) until the evidence is found. Priority service typically cuts your turnaround time in half.
- **Weekend service:** Computer forensics experts should be able to work from 8:00 A.M. to 5:00 P.M., Saturday and Sunday, to locate the needed electronic evidence and will continue 14 Computer Forensics, Second Edition working on your case until your evidence objectives are met.

5.2.2 Handling Preliminary Investigations

Q9. Explain about the Stages of Forensic Investigation.

Ans :

Primary Objectives of Cyber Security Forensics Investigators

1. For recovering, analyzing, reporting, and presenting computer-oriented materials so that it can be easily demonstrated and presented in the form of evidence in the court of law.
2. To identify evidence in a short time frame, and estimate the overall menace and impact of the malicious cyber activity on the victim user or organization and suggest for protection against the attack.

Steps

There are some specific ways to track cybercrime or go to a solution for how cybercrime took place. The steps are:

1. The incident occurred in any company or organization.
2. The employees or members contact the company's advocate for legal advice.
3. Advocate contact cyber forensics investigator (external or internal).
4. The forensic investigator will come and prepare the FRP, i.e., First Response Procedure documentation.
5. The investigator then seizes the evidence and other assets related to the crime scene and transports them to a forensics lab.
6. He/she will start analyzing the files and other assets.
7. Examine all the data one after another and further contact the person or group of people associated with the incident.
8. The report will be formed and concludes the investigation, where all the analyses will be written and explained.
9. The report is then handed to the organization's legal authorities.
10. The legal authority will then go through the report(s) and will press charges against the offensive in the court of law.
11. The forensic investigator will delete all the data once the entire case is closed.

Q10. What is Incident Handling?Explain

Ans :

Cybersecurity and forensics have another essential terminology that is often used in this field - incident handling. Computer security incidents are some real or suspected offensive events related to cybercrime and cybersecurity and computer networks. Forensics investigators or internal cybersecurity professionals are hired in organizations to handle such events and incidents, known as incident handlers.

Types

- **Low-level incidents**

  Where the impact of cybercrime is low.

- **Mid-level incident**s

  The impact of cybercrime is comparatively high and needs security professionals to handle the situations.

Rahul Publications

- **High-level events**

  Where the impact of cybercrime is the most serious and needs security professionals, and forensic investigators to handle the situations and analyze the scenario, respectively.

Digital Forensics Lifecycle

- **Collection**

  The first step in the forensic process is to identify potential sources of data and acquire data from them.

- **Examination**

  After data has been collected, the next phase is to examine the data, which involves assessing and extracting the relevant pieces of information from the collected data. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms.

- **Analysis**

  Once the relevant information has been extracted, the analyst should study and analyze the data to draw conclusions from it. The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the available data or determine that no conclusion can yet be drawn.

- **Reporting**

  The process of preparing and presenting the information resulting from the analysis phase. Many factors affect reporting, including the following:

  (a) Alternative Explanations

  When the information regarding an event is incomplete, it may not be possible to arrive at a definitive explanation of what happened. When an event has two or more plausible explanations, each should be given due consideration in the reporting process. Analysts should use a methodical approach to attempt to prove or disprove each possible explanation that is proposed.

  (b) Audience Consideration

  Knowing the audience to which the data or information will be shown is important.

- **Actionable Information**

  Reporting also includes identifying actionable information gained from data that may allow an analyst to collect new sources of information.

5.2.3 Controlling an Investigation

Q11. Explain how to collect and control the investigation.

Ans : **(Imp.)**

Collecting and Archiving

Logs and Logging

You should run some kind of system logging function. It is important to keep these logs secure and to back them up periodically. Because logs are usually automatically Monitoring :

Monitoring network traffic can be useful for many reasons

You can gather statistics, watch out for irregular activity (and possibly stop an intrusion before it happens), and trace where an attacker is coming from and what he is doing. Monitoring logs as they are created can often show you important information you might have missed had you seen them separately. This doesn't mean you should ignore logs later

It may be what's missing from the log that is suspicious. Information gathered while monitoring network traffic can be compiled into statistics to define normal behavior for your system. These statistics can be used as an early warning of an attacker's actions. You can also monitor the actions of your users.

This can, once again, act as an early warning system. Unusual activity or the sudden appearance

Rahul Publications

of unknown users should be considered definite cause for closer inspection. Methods of Collection:- There are two basic forms of collection: freezing the scene and honey potting. The two aren't mutually exclusive.

You can collect frozen information after or during any honey potting. Freezing the scene involves taking a snapshot of the system in its compromised state.

The necessary authorities should be notified (the police and your incident response and legal teams), but you shouldn't go out and tell the world just yet. You should then start to collect whatever data is important onto removable nonvolatile media in a standard format.

Make sure the programs and utilities used to collect the data are also collected onto the same media as the data.

All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification. Honey potting is the process of creating a replica system and luring the attacker into it for further monitoring. A related method (sandboxing) involves limiting what the attacker can do while still on the compromised system, so he can be monitored without (much) further damage.

Artifacts

Whenever a system is compromised, there is almost always something left behind by the attacker be it code fragments, trojaned programs, running processes, or sniffer log files. These are known as artifacts. Artifacts may be difficult to find; trojaned programs may be identical in all obvious ways to the originals (file size, medium access control [MAC] times, etc.).

Use of cryptographic check sums may be necessary, so you may need to know the original file's checksum. If you are performing regular file integrity assessments, this shouldn't be a problem. Analysis of artifacts can be useful in finding other systems the attacker (or his tools) has broken into.

Collection Steps

You now have enough information to build a step-bystep guide for the collection of the evidence. Once again, this is only a guide. You should customize it to your specific situation.

You should perform the following collection steps:

1. Find the evidence.
2. Find the relevant data.
3. Create an order of volatility.
4. Remove external avenues of change.
5. Collect the evidence.
6. Document everything.

Find the Evidence

Determine where the evidence you are looking for is stored. Use a checklist. Not only does it help you to collect evidence, but it also can be used to double-check that everything you are looking for is there.

Find the Relevant Data

Once you've found the evidence, you must figure out what part of it is relevant to the case. In general, you should err on the side of over-collection, but you must remember that you have to work fast.

System is a good guide and ensures that you minimize loss of uncorrupted evidence.

Remove External Avenues of Change

It is essential that you avoid alterations to the original data, and prevention is always better than a cure.

Preventing anyone from tampering with the evidence helps you create as exact an image as possible.

However, you have to be careful. The attacker may have been smart and left a dead-man switch. In the end, you should try to do as much as possible to prevent changes.

Collect the Evidence

You can now start to collect the evidence using the appropriate tools for the job. As you go, reevaluate the evidence you've already collected.

You may find that you missed something important. Now is the time to make sure you get it.

Rahul Publications

Document Everything

Your collection procedures may be questioned later, so it is important that you document everything you do. Time stamps, digital signatures, and signed statements are all important. Don't leave anything out.

Controlling Contamination

The Chain of Custody A good way of ensuring that data remains uncorrupted is to keep a chain of custody.

This is a detailed list of what was done with the original copies once they were collected.

Remember that this will be questioned later on, so document everything (who found the data, when and where it was transported [and how], who had access to it, and what they did with it).

You may find that your documentation ends up greater than the data you collected, but it is necessary to prove your case.

Analysis

Once the data has been successfully collected, it must be analyzed to extract the evidence you wish to present and to rebuild what actually happened.

As always, you must make sure that you fully document everything you do. Your work will be questioned and you must be able to show that your results are consistently obtainable from the procedures you performed.

Time

To reconstruct the events that led to your system being corrupted, you must be able to create a time line. This can be particularly difficult when it comes to computers. Clock drift, delayed reporting, and differing time zones can create confusion in abundance.

One thing to remember is to never, ever change the clock on an affected system. Record any clock drift and the time zone in use, as you will need this later, but changing the clock just adds in an extra level of complexity that is best avoided.

Forensic Analysis of Backups

When analyzing backups, it is best to have a dedicated host for the job. This examination host should be secure, clean (a fresh, hardened install of the operating system is a good idea), and isolated from any network.

You don't want it tampered with while you work, and you don't want to accidentally send something nasty down the line.

Reconstructing the Attack

Now that you have collected the data, you can attempt to reconstruct the chain of events leading to and following the attacker's break-in. You must correlate all the evidence you have gathered (which is why accurate timestamps are critical), so it's probably best to use graphical tools, diagrams, and spreadsheets. Include all of the evidence you've found when reconstructing the attack - no matter how small it is. You may miss something if you leave a piece of evidence out.

5.2.4 Conducting disk-based analysis

Q12. Explain dusk based forensic analysis

Ans :

Disk forensics is the science of extracting forensic information from digital storage media like Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc.. The process of Disk Forensics are

1. Identify digital evidence

First step in Disk Forensics is identification of storage devices at the scene of crime like hard disks with IDE/SATA/SCSI interfaces, CD, DVD, Floppy disk, Mobiles, PDAs, flash cards, SIM, USB/ Fire wire disks, Magnetic Tapes, Zip drives, Jazz drives etc. These are some of the sources of digital evidence.

2. Seize & Acquire the evidence

Next step is seizing the storage media for digital evidence collection. This step is performed at the scene of crime. In this step, a hash value of the storage media to be seized is computed using appropriate cyber forensics tool. Hash value is a unique signature generated by a mathematical hashing algorithm based on the content of the storage media. After computing the hash value, the storage media is securely sealed and taken for further processing.

Rahul Publications

One of the cardinal rules of Cyber Forensics is "Never work on original evidence". To ensure this rule, an exact copy of the original evidence is to be created for analysis and digital evidence collection. Acquisition is the process of creating this exact copy, where original storage media will be write protected and bit stream copying is made to ensure complete data is copied into the destination media. Acquisition of source media is usually done in a Cyber Forensics laboratory.

3. Authenticate the evidence

Authentication of the evidence is carried out in Cyber Forensics laboratory. Hash values of both source and destination media will be compared to make sure that both the values are same, which ensures that the content of destination media is an exact copy of the source media.

4. Preserve the evidence

Electronic evidences might be altered or tampered without trace. Once the acquisition and authentication have been done, the original evidence should be placed in secure storage keeping away from highly magnetic and radiation sources. One more copy of image should be taken and it needs to be stored into appropriate media or reliable mass storage. Optical media can be used as the mass storage. It is reliable, fast, longer life span and reusable.

5. Analyze the evidence

Verification of evidence before starting analysis is an important step in Cyber Forensics process. This is done in Cyber Forensics laboratory before commencing analysis. Hash value of the evidence is computed and compared it with the hash value taken at the time of acquisition. If both the values are same, there is no change in the content of the evidence. If both are different, there is some change in the content. The result of verification should be properly documented.

Analysis is the process of collecting digital evidence from the content of the storage media depending upon the nature of the case being examined. This involves searching for keywords, picture analysis, time line analysis, registry analysis, mailbox analysis, database analysis, cookies, temporary and Internet history files analysis, recovery of deleted items and analysis, data carving and analysis, format recovery and analysis, partition recovery and analysis, etc.

6. Report the findings

Case analysis report should be prepared based on the nature of examination requested by a court or investigation agency. It should contain nature of the case, details of examination requested, details of material objects and hash values, result of evidence verification, details of analysis conducted and digital evidence collected, observations of the examiner and conclusion. Presentation of the report should be in simple terms and precise way so that non-technical persons should be able to understand the content of the report.

7. Documenting

Documentation is very important in every step of the Cyber Forensics process. Everything should be appropriately documented to make a case admissible in a court of law. Documentation should be started from the planning of case investigation and continue through searching in scene of crime, seizure of material objects, chain of custody, authentication and acquisition of evidence, verification and analysis of evidence, collection of digital evidence and reporting, preservation of material objects and up to the closing of a case.

5.2.5 Investigating Information-hiding

Q13. How data can be hidden in computer forensics and explain how hidden data can be investigated in cyber forensics.

Ans : **(Imp.)**

Information hiding is a research domain that covers a wide spectrum of methods that are used to make (secret) data difficult to notice. Due to improvements in network defenses such techniques are recently gaining an increasing attention from actors like cyber criminals, terrorist and state-

Rahul Publications

sponsored groups as they allow to store data or to cloak communication in a way that is not easily discoverble.

Digital forensics are. Here are some ways that data can be hidden within storage media :

Example 1: Deleted Files and Slack Space

Recently deleted files leave slack space. The files are still there, but the area is marked unallocated. Those unallocated sectors are eventually overwritten, permanently "deleting" prior data in the sector (Olzak, 2007).

Example 2: Hiding data in HPA on disk

Host Protected Areas on disks are not visible to the operating system. Boot diagnostics, BIOS support, and other manufacturer tools are generally loaded there in the host protected area. Rootkits can write to that space, which makes them difficult to detect because the operating system and anti-virus cannot see those rootkits either (Volonino, 2017).

Example 3: Hiding data by marking sectors that contain data as "bad" and therefore unreadable by end user software

This process forces the operating system to think a sector is bad, and therefore it will ignore it. It requires creating bad blocks on the file system where data is logically located to "hide" it. This is generally reversible by unmarking bad blocks and making them visible to the operating system (Cisar et al., 2014).

How is Computer Forensics Used to Gather Evidence?

The usual procedure to gathering evidence from the computer of someone who is suspected of a crime is to first, take the computer and physically isolate it.

After the investigators have the computer, they will make a digital copy of everything that is in the drive. They will then analyze the copy they made to find evidence of any wrong doing.

In order to analyze the data found on the hard drive, they use a variety of techniques and employ data recovery software to find any hidden or recently deleted files and folders.

Anything that the investigators turn up that could be used as evidence in court are documented and presented in a finding report.

The type of evidence that can be recovered through computer forensics include documents, videos, photos, messages, audio, and even the Internet search history of a suspect. They can even find and search deleted e-mails with a program like DataNumen Outlook Repair and DataNumen Exchange Recovery.

How is Data Recovery Used in Computer Forensics?

Digital forensics is a branch of computer forensics that focus on recovering material from digital devices such as computers and mobile devices. Digital forensic investigators use advanced data recovery software to recover data that suspects tried to hide.

While criminals might initially store incriminating data on their computers or mobile devices, they might delete or hide this data when they suspect that they are being monitored by law enforcement agencies. They might also try to hide the data by getting rid of their hard drives or physically damaging them in the hope that the data inside will not be accessible. This is when digital forensics steps in.

One of the basic techniques employed by computer forensic investigators is to scan and identify and deleted files and folders on a seized computer. They will then try to restore the data in these deleted files and often find valuable data that can help build the case against the suspects.

5.2.6 Scrutinizing E-mail

Q14. What are the various approaches to use for Email forensic?

Ans :

E-mail forensics refers to the study of source and content of e-mail as evidence to identify the

actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc. This study involves investigation of metadata, keyword searching, port scanning, etc. for authorship attribution and identification of e-mail scams.

Rahul Publications

Various approaches that are used for e-mail forensic are:

Header Analysis

Meta data in the e-mail message in the form of control information i.e. envelope and headers including headers in the message body contain information about the sender and/or the path along which the message has traversed. Some of these may be spoofed to conceal the identity of the sender. A detailed analysis of these headers and their correlation is performed in header analysis.

Bait Tactics

In bait tactic investigation an e-mail with http: "<imgsrc>" tag having image source at some computer monitored by the investigators is send to the sender of e-mail under investigation containing real (genuine) e-mail address. When the e-mail is opened, a log entry containing the IP address of the recipient (sender of the e-mail under investigation) is recorded on the http server hosting the image and thus sender is tracked. However, if the recipient (sender of the e-mail under investigation) is using a proxy server then IP address of the proxy server is recorded. The log on proxy server can be used to track the sender of the e-mail under investigation. If the proxy server's log is unavailable due to some reason, then investigators may send the tactic e-mail containing a) Embedded Java Applet that runs on receiver's computer or b) HTML page with Active X Object. Both aiming to extract IP address of the receiver's computer and e-mail it to the investigators.

Server Investigation

In this investigation, copies of delivered e-mails and server logs are investigated to identify source of an e-mail message. E-mails purged from the clients (senders or receivers) whose recovery is impossible may be requested from servers (Proxy or ISP) as most of them store a copy of all e-mails after their deliveries. Further, logs maintained by servers can be studied to trace the address of the computer responsible for making the e-mail transaction. However, servers store the copies of e-mail and server logs only for some limited periods and some may not co-operate with the investigators. Further, SMTP servers which store data like credit card number and other data pertaining to owner of a mailbox can be used to identify person behind an e-mail address.

Network Device Investigation

In this form of e-mail investigation, logs maintained by the network devices such as routers, firewalls and switches are used to investigate the source of an e-mail message. This form of investigation is complex and is used only when the logs of servers (Proxy or ISP) are unavailable due to some reason, e.g. when ISP or proxy does not maintain a log or lack of co-operation by ISP's or failure to maintain chain of evidence.

Software Embedded Identifiers

Some information about the creator of e-mail, attached files or documents may be included with the message by the e-mail software used by the sender for composing e-mail. This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF). Investigating the e-mail for these details may reveal some vital information about the senders e-mail preferences and options that could help client side evidence gathering. The investigation can reveal PST file names, Windows logon username, MAC address, etc. of the client computer used to send e-mail message.

Sender Mailer Fingerprints

Identification of software handling e-mail at server can be revealed from the Received header field and identification of software handling e-mail at client can be ascertained by using different set of headers like "X-Mailer" or equivalent. These headers describe applications and their versions used at the clients to send e-mail. This information about the client computer of the sender can be used to help investigators devise an effective plan and thus prove to be very useful.

5.2.7 Validating E-mail header information

Q15. Explain about email headers.

Ans :

Email headers contain important information about the origin and path an email took before arriving at its final destination, including the sender's IP address, internet service provider, email client, and even location. The information could be used to block future emails from the sender (in the case of spam) or to determine the legitimacy of a

Rahul Publications

suspicious email. A review of the headers can also help to identify "header spoofing," a strong indication the email was sent with malicious intent.

Understanding the Header Fields

Email headers are read chronologically from the bottom up and can be broken down into three main categories: 1) Message Information 2) X-Headers and 3) Server Relay Information.. Simply copy and paste the headers into the tool, and it will analyze the server relays and convert the headers into an easy to read format.

Message Information

Includes commonly recognized email header fields, such as To:, From:, Subject:, Date:, To:, as well as useful fields like Message-ID:, Return-Path:, Reply To:, among others. These fields are the most easily spoofed because they are specified by the sender's mail client. They are usually found near the bottom of the headers as they are the first to be added.

```
Return-Path: mmcduck***@outlook.com
Content-Type: multipart/mixed;
       boundary="_dc53e542-2fb7-4d92-a5af-eb8a0709fddb_"
From: Mike McDuck <mmcduck***@outlook.com>
To: "buggln***@gmail.com" <buggln***@gmail.com>
Subject: New Update!
Date: Tue, 24 Apr 2016 08:59:23 -0700
Importance: Normal
MIME-Version: 1.0
X-OriginalArrivalTime: 24 Apr 2016 15:59:24.0506 (UTC) FILETIME=[3E1ACBA0:01D1B5D5]
```

Fig.1: Headers – Message Info

X-Headers

These fields are added to the email by security devices such as email anti-virus scanners as it traverses the internet and internal networks. The X-Headers may not be in order and are often intermixed within the Message Info and Server Relay headers. Not all X-Headers will be present in every case. In the example below there is an X-Originating-Email: that reveals the true sender was bad_guy_spammer@spammy.com and not mmcduck***@outlook.com. Sometimes there is an X-Originating-IP as well. The headers below also show that the email was scanned by Agari Email Security and Iron Port devices.

```
X-Originating-Email: [bad_guy_spammer@spammy.com]
X-Originating-IP: [192.168.1.25]
X-Agari-Original-From: bad_guy_spammer@spammy.com
X-Agari-Original-To: buggln***@gmail.com
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-AV: E=Sophos;i="5.26,359,1459832400";
   d="scan'208,217";a="15091714"
From: Mike McDuck <mmcduck***@outlook.com>
To: "buggln***@gmail.com" <buggln***@gmail.com>
Subject: New Update!
Date: Tue, 24 Apr 2016 08:59:23 -0700
Importance: Normal
MIME-Version: 1.0
X-OriginalArrivalTime: 24 Apr 2016 15:59:24.0506 (UTC)
FILETIME=[3E1ACBA0:01D1B5D5]
```

Fig. 2: Headers – X-Headers

Server Relay Information

Each time a server relay receives an SMTP message, it will add a new Received: line at the beginning of the header block. A typical email received by a user on a corporate network will show many server relays both before and after being delivered to the corporate email servers (company server.com). These will be in chronological order starting from the bottom up.

Rahul Publications

➢ **View Larger Imag**

```
Received: from msg2.companyserver.com (0.0.0.161) by dity043.ds.somewhere.com
(10.132.213.109) with Microsoft SMTP Server id 14.3.279.2; Sat, 21 Apr 2016 08:19:02 -
0500

Received: from fireeye001.companyserver.com (HELO fe-ctc msg10.companyserver.com)
([0.0.0.151])by mail24.companyserver.com with ESMTP; 21 Apr 2016 08:19:02 -0500

Received: from localhost.localdomain (localhost [127.0.0.1]) by me-ctd-
msg10.companyserver.com (Postfix) with SMTP id 3rDlkZ4vHdz7Wjk for
<user.mchappy@company.com>; Sat, 21 Apr 2016 08:19:02 -0500 (CDT)

Received: from msg2.companyserver.com (msg2.companyserver.com [0.0.0.161])by me-ctd-
msg10.companyserver.com (Postfix) with ESMTP id 3rDlkY6VFszPjdW for
<user.mchappy@company.com>; Sat, 21 Apr 2016 08:19:01 -0500 (CDT)

Received: from col004-omc1s19.hotmail.com ([65.55.34.29])by msg2.companyserver.com with
ESMTP/TLS/AES256-SHA; 21 Apr 2016 08:19:01 -0500

Received: from NAM01-BN3-obe.outbound.protection.outlook.com ([65.55.34.7]) by COL004-
OMC1S19.hotmail.com over TLS secured channel with Microsoft SMTPSVC(7.5.7601.23008); Sat,
21 Apr 2016 06:19:00 -0700
```

Fig. 3: Headers: Server Relay

Analyzing Headers

By analyzing the server relay information in chronological order from the bottom-up, you can get a picture of where the message travelled. Each receiving mail server adds the name and IP address of the server that delivered the message. The server name may reveal the domain of the sender relay, and a Who-Is lookup of the IP may give you a geographic location. In the case of messages sent via Gmail and other large email service providers, this may only lead you back to the location of the email servers or even the corporate headquarters of the provider (i.e. Mountain View, CA). If you are lucky, the headers will include an X-Originating-IP that may reveal the sender's internet service provider and narrow down the sender's location.

If you are looking at spam email headers from a network security perspective, it is important to identify the IP address/domain that delivered the email to your frontline email server, the security device in front of your email server. The server relay header will read "Received: from some.external.domain ([some.IP]) by your.company.device ([your.IP])." Potentially, everything before this entry could be spoofed, but, as your server is reporting it received an email from some.external.domain ([some.IP]) and is the one adding it to the headers, you should be able to trust it.

```
Received: from msg2.companyserver.com (msg2.companyserver.com [0.0.0.161])by me-ctd-
msg10.companyserver.com (Postfix) with ESMTP id 3rDlkY6VFszPjdW for
<user.mchappy@company.com>; Fri, 29 Apr 2016 10:09:02 -0500 (CDT)

Received: from unknown (HELO nuxos.us) ([184.83.22.146]) by msg2.companyserver.com with
ESMTP; 29 Apr 2016 10:08:14 -0500
Subject: Sponsored Promotions >> Insurance Deals!
```

Figure 4: Headers – Originating IP

Figure 5: SenderBase.org – Reputation Rating

It is important to look for evidence of spoofing or alteration of header data in the Message Information headers. The spammer can easily alter these headers within their email client or by using specialized software. The most common field to spoof is the From: field. In the example in Figure 2, the sender changed the From: field to display "Mike McDuck<mmcduck***@outlook.com>" but the true sender was revealed by the X-Originating-Email field. It is not uncommon for spammers to use the recipient's own name and email address in the From: field in order to increase the chances the recipient will open the

The Message-ID is another good place to identify spoofing. The Message-ID is a unique identifier of digital messages and is difficult to alter as it is added by the mail server that processes the email. Because it has to be unique, it is common for message systems to use a date/time stamp followed by the sender's domain name (example: CAF4Ths+hsd84G9sedaD@mail.gmail.com). If the sender domain in the From: field does not match the Message-ID, you might be dealing with a spoofed message.

The majority of spam emails are generated by servers capable of producing millions of messages per day. Sometimes those servers are running programs that populate the "X-Mailer" field with the name of the mail client that was used. Legitimate emails will usually include a known mail client (i.e. Microsoft Outlook 16.0, Outlook Express, iPad Mail), but the spammer mail clients may be something less common (see Figure 6) or even obscured through random, nonsense characters.

```
From: Mike McDuck <mmcduck***@outlook.com>
To: "'Jim B'" <bugg1n***@gmail.com>
Subject: Super Cheap Diet Pills!
Date: Tue, 24 Apr 2016 08:56:34 -0700
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_000_03F6_01D1B59A.2CC98390"
X-Mailer: MonkeyMailer v.22
Thread-Index: AdG11Nj/KhXi2dH1T+emsUToVVc5nQ==
Content-Language: en-us
X-OriginalArrivalTime: 24 Apr 2016 15:56:41.0879 (UTC) FILETIME=[DD2BE270:01D1B5D4]
```

Figure 6: Headers – Mail Client

5.2.8 Tracing Internet access

Q16. How internet tracing can be done? Explain various methods to track internet access.

Ans : **(Imp.)**

The information that resides on the Internet can be tracked and traced, and so can be valuable in forensics.

Tracing is a process that follows the Internet activity backwards, from the recipient to the user. As well, a user's Internet activity on web sites can also be tracked on the recipient site (i.e., what sites are visited and how often, the activity at a particular site). Sometimes this tracking and tracing ability is used to generate e-mail to the user, promoting a product that is related to the sites visited. User information, however, can also be gathered covertly.

Techniques of Internet tracking and tracing can also enable authorities to pursue and identify those responsible for malicious Internet activity.

Cookies are computer files that are stored on a user's computer during a visit to a web site. When the user electronically enters the web site, the host computer automatically loads the file(s) to the user's computer.

The cookie is a tracking device, which records the electronic movements made by the user at the site, as well as identifiers such as a username and password. Commercial web sites make use of cookies to allow a user to establish an account on the first visit to the site and so to avoid having to enter account information (i.e., address, credit card number, financial activity) on subsequent visits. User information can also be collected unbeknownst to the user, and subsequently used for whatever purpose the host intends.

Cookies are files, and so can be transferred from the host computer to another computer. This can occur legally (i.e., selling of a subscriber mailing list) or illegally (i.e., "hacking in" to a host computer and copying the file). Also, cookies can be acquired as part of a law enforcement investigation.

Stealing a cookie requires knowledge of the file name. Unfortunately, this information is not difficult to obtain.

Here are a few other commonly used data tracking methods today, including what user data they collect:

- Web beacons, AKA web bugs or tracking beacons, track how you engage with a specific webpage, including content you click. They also can be used in email exchanges to determine if a message has been received or opened.
- IP addresses are attached to all internet-connected devices and required to visit a website, which might remember yours and use it to track your activity.
- Session replay scripts are programs that record a website visitor's activity on a website, including their mouse movement, clicks, and scrolls.
- Favicons are considered supercookies in that they operate similarly but are much more difficult to decline or remove.
- Account tracking keeps tabs on your online activity while logged into a specific online account or platform and is often an internet tracking method that online users must grant permission for.
- Mouse tracking, AKA cursor tracking, is a data tracking software that records online users' mouse movements to analyze how they interact with a website.
- Browser fingerprinting stitches together information about your device — including its operating system, language preferences, time zone, etc. — to create a unique identifier that's used to trace all of your online activity. This can also be conducted through canvas fingerprinting, which recognizes your HTML5 canvas elements.
- Cross-device tracking, also considered deterministic or probabilistic tracking, matches up your browsing habits across devices.
- Click-through rate is a measure of times an online user clicks on and visits a piece of content suggested or advertised to them. Websites use the metric to inform their content strategies or advertiser opportunities.

5.2.9 Tracing memory in real-time

Q17. Explain about the importance of memory forensic to trace real time data.

Ans :

Memory forensics is a vital form of cyber investigation that allows an investigator to identify unauthorized and anomalous activity on a target computer or server. This is usually achieved by running special software that captures the current state of the system's memory as a snapshot file, also known as a memory dump. This file can then be taken offsite and searched by the investigator. This is useful because of the way in which processes, files and programs are run in memory, and once a snapshot has been captured, many important facts can be ascertained by the investigator, such as:

- Processes running
- Executable files that are running
- Open ports, IP addresses and other networking information
- Users that are logged into the system, and from where
- Files that are open and by whom

Rahul Publications

The Importance of Memory Forensics

Memory forensics can provide unique insights into runtime system activity, including open network connections and recently executed commands or processes. In many cases, critical data pertaining to attacks or threats will exist solely in system memory – examples include network connections, account credentials, chat messages, encryption keys, running processes, injected code fragments, and internet history which is non-cacheable. Any program – malicious or otherwise – must be loaded in memory in order to execute, making memory forensics critical for identifying otherwise obfuscated attacks.

As attack methods become increasingly sophisticated, memory forensics tools and skills are in high demand for security professionals today. Many network-based security solutions like firewalls and antivirus tools are unable to detect malware written directly into a computer's physical memory or RAM. Security teams should look to memory forensics tools and specialists to protect invaluable business intelligence and data from stealthy attacks such as fileless, in-memory malware or RAM scrapers

Memory Forensics Tools

Traditional network and endpoint security software has some difficulty identifying malware written directly in your system's RAM. Traditional security systems typically analyze input sources like network, email, CD/DVD, USB drives, and keyboards, yet lack the ability to analyze volatile data that is stored in memory. These systems are viable options for protecting against malware in ROM, BIOS, network storage, and external hard drives. However, your data in execution might still be at risk due to attacks that upload malware to memory locations reserved for authorized programs. The most sophisticated enterprise security systems now come with memory forensics and behavioral analysis capabilities which can identify malware, rootkits, and zero days in your system's physical memory.

Memory forensics tools also provide invaluable threat intelligence that can be gathered from your system's physical memory. Physical memory artifacts include the following:

- **Usernames and Passwords**

  Information users input to access their accounts can be stored on your system's physical memory.

- **Decrypted Programs**

  Any encrypted malicious file that gets executed will have to decrypt itself in order to run. This threat intelligence is valuable for identifying and attributing threats.

- **Open Clipboard or Window Contents**

  This may include information that has been copied or pasted, instant messenger or chat sessions, form field entries, and email contents.

Rahul Publications

Short Question and Answers

1. Define Cyber space.

Ans :

Cyber space can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyber space today has become a common pool used by citizens, businesses, critical information infrastructure, military and govern- ments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyber space is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

2. Cyber law

Ans :

Cyber law is the type of law that deals with the relationship of the internet to the technological and electronic elements such as software, information system (IS), hardware, and computers. It is nothing but a part of a legal system that deals with the cyber space, internet and their legal issues.

Importance

Cyber law is used by smaller business organizations which are extremely vulnerable because of the ineffective cyber security. It is very important to all types of business organizations, particularly when you think about the importance or advantages of the internet as well as digital systems are for your day-to-day operations. There are various reasons for which Cyber Law, is very important, are listed below;

- **It allows employees to work safely**

  With the help of cyber law, you and the employees of your company haven't got any risk from a potential cyber attack. If your system becomes infected than that can really hamper their productivity.

- **It can protect your business**

  This is one of the biggest factors, because of which cyber law is very important. It allows the employees to surf the internet as and when they require it. You have to ensure that they can't at risk from potential threats.

- **It protects the personal information of the user**

  One of the most important factors in the digital world is to keep your personal information secret. It is very essential for the customer that they are quite capable of selling the information.

3. Roles of international cyber law.

Ans :

In various countries, areas of the computing and communication industries are regulated by governmental bodies

- There are specific rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming
- There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes
- There are laws governing trade on the Internet, taxation, consumer protection, and advertising
- There are laws on censorship versus freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies
- Some states limit access to the Internet, by law as well as by technical means.

4. Cyber security standards

Ans :

To make cyber security measures explicit, the written norms are required. These norms are known as cyber security standards: the generic sets of prescriptions for an ideal execution of certain measures. The standards may involve methods, guidelines, reference frameworks, etc. It ensures efficiency of security, facilitates integration and interoperability, enables meaningful comparison of measures, reduces complexity, and provide the structure for new developments.

A security standard is "a published specification that establishes a common language, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline,

Rahul Publications

or a definition." The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. The Well-Written cyber security standards enable consistency among product developers and serve as a reliable standard for purchasing security products.

Security standards are generally provided for all organizations regardless of their size or the industry and sector in which they operate. This section includes information about each standard that is usually recognized as an essential component of any cyber security strategy.

5. What is the aim of Indian cyber space?

Ans :

Indian cyber space was born in 1975 with the establishment of National Informatics Centre (NIC) with an aim to provide govt with IT solutions.

Three networks (NWs) were set up between 1986 and 1988 to connect various agencies of govt. These NWs were, INDONET which connected the IBM mainframe installations that made up India's computer infrastructure, NICNET (the NIC NW) a nationwide very small aperture terminal (VSAT) NW for public sector organizations as well as to connect the central govt with the state govts and district administrations, the third NW setup was ERNET (the Education and Research Network), to serve the academic and research communities.

New Internet Policy of 1998 paved the way for services from multiple Internet service providers (ISPs) and gave boost to the Internet user base grow from 1.4 million in 1999 to over 150 million by Dec 2012. Exponential growth rate is attributed to increasing Internet access through mobile phones and tablets.

Govt is making a determined push to increase broadband penetration from its present level of about 6%1. The target for broadband is 160 million households by 2016 under the National Broadband Plan.

People in India are vulnerable to cyber-attacks due to the lack of cyber hygiene. The country needs to be alert, and any laxity can have severe consequences, experts warn.

6. National Cyber Security Policy.

Ans :

The National Cyber Security Policy is a policy document drafted by the Department of Electronics and Information Technology (DeitY) in 2013 aimed at protecting the public and private infrastructure from cyber attacks.

The guideline also seeks to protect the personal information of internet users, financial and banking information, and sovereign data .

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology (DeitY) It aims at protecting the public and private infrastructure from cyber attacks.

The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". Ministry of Communications and Information Technology (India) defines Cyber space as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

7. What is cyber forensics?

Ans :

Computer forensics is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence.

- Computer forensics also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer exami- nation.
- Computer evidence can be useful in criminal cases, civil disputes, and human resources/ employment proceedings.

8. What is Incident Handling? Explain.

Ans :

Cybersecurity and forensics have another essential terminology that is often used in this field - incident handling. Computer security incidents are some real or suspected offensive events related to cybercrime and cybersecurity and computer networks. Forensics investigators or internal cybersecurity professionals are hired in organizations to handle such events and incidents, known as incident handlers.

Types

- **Low-level incidents**

  Where the impact of cybercrime is low.

- **Mid-level incident**s

  The impact of cybercrime is comparatively high and needs security professionals to handle the situations.

Rahul Publications

- **High-level events**

  Where the impact of cybercrime is the most serious and needs security professionals, and forensic investigators to handle the situations and analyze the scenario, respectively.

Digital Forensics Lifecycle

- **Collection**

  The first step in the forensic process is to identify potential sources of data and acquire data from them.

- **Examination**

  After data has been collected, the next phase is to examine the data, which involves assessing and extracting the relevant pieces of information from the collected data. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms.

- **Analysis**

  Once the relevant information has been extracted, the analyst should study and analyze the data to draw conclusions from it. The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the available data or determine that no conclusion can yet be drawn.

9. How internet tracing can be done?

Ans :

The information that resides on the Internet can be tracked and traced, and so can be valuable in forensics.

Tracing is a process that follows the Internet activity backwards, from the recipient to the user. As well, a user's Internet activity on web sites can also be tracked on the recipient site (i.e., what sites are visited and how often, the activity at a particular site). Sometimes this tracking and tracing ability is used to generate e-mail to the user, promoting a product that is related to the sites visited. User information, however, can also be gathered covertly.

Techniques of Internet tracking and tracing can also enable authorities to pursue and identify those responsible for malicious Internet activity.

Cookies are computer files that are stored on a user's computer during a visit to a web site. When the user electronically enters the web site, the host computer automatically loads the file(s) to the user's computer.

The cookie is a tracking device, which records the electronic movements made by the user at the site, as well as identifiers such as a username and password. Commercial web sites make use of cookies to allow a user to establish an account on the first visit to the site and so to avoid having to enter account information (i.e., address, credit card number, financial activity) on subsequent visits. User information can also be collected unbeknownst to the user, and subsequently used for whatever purpose the host intends.

Cookies are files, and so can be transferred from the host computer to another computer. This can occur legally (i.e., selling of a subscriber mailing list) or illegally (i.e., "hacking in" to a host computer and copying the file). Also, cookies can be acquired as part of a law enforcement investigation.

Stealing a cookie requires knowledge of the file name. Unfortunately, this information is not difficult to obtain.

10. Tracing memory in real-time.

Ans :

Memory forensics is a vital form of cyber investigation that allows an investigator to identify unauthorized and anomalous activity on a target computer or server. This is usually achieved by running special software that captures the current state of the system's memory as a snapshot file, also known as a memory dump. This file can then be taken offsite and searched by the investigator. This is useful because of the way in which processes, files and programs are run in memory, and once a snapshot has been captured, many important facts can be ascertained by the investigator, such as:

- Processes running
- Executable files that are running
- Open ports, IP addresses and other networking information
- Users that are logged into the system, and from where
- Files that are open and by whom

The Importance of Memory Forensics

Memory forensics can provide unique insights into runtime system activity, including open network connections and recently executed commands or processes. In many cases, critical data pertaining to attacks or threats will exist solely in system memory – examples include network connections, account credentials, chat messages, encryption keys, running

Rahul Publications

processes, injected code fragments, and internet history which is non-cacheable. Any program malicious or otherwise must be loaded in memory in order to execute, making memory forensics critical for identifying otherwise obfuscated attacks.

As attack methods become increasingly sophisticated, memory forensics tools and skills are in high demand for security professionals today. Many network-based security solutions like firewalls and antivirus tools are unable to detect malware written directly into a computer's physical memory or RAM. Security teams should look to memory forensics tools and specialists to protect invaluable business intelligence and data from stealthy attacks such as fileless, in-memory malware or RAM scrapers

Memory Forensics Tools

Traditional network and endpoint security software has some difficulty identifying malware written directly in your system's RAM. Traditional security systems typically analyze input sources like network, email, CD/DVD, USB drives, and keyboards, yet lack the ability to analyze volatile data that is stored in memory. These systems are viable options for protecting against malware in ROM, BIOS, network storage, and external hard drives. However, your data in execution might still be at risk due to attacks that upload malware to memory locations reserved for authorized programs. The most sophisticated enterprise security systems now come with memory forensics and behavioral analysis capabilities which can identify malware, rootkits, and zero days in your system's physical memory.

Rahul Publications

Choose the Correct Answers

1. Which of the following is not a type of cyber crime? [d]

   (a) Data theft (b) Forgery

   (c) Damage to data and systems (d) Installing antivirus for protection

2. Which of the following refers to stealing one's idea or invention of others and use it for their own benefits? [b]

   (a) Piracy (b) Plagiarism

   (c) Intellectual property rights (d) All of the above

3. Which of the following is not an example of a computer as weapon cyber-crime? [b]

   (a) Credit card fraudulent (b) Spying someone using keylogger

   (c) IPR Violation (d) Pornography

4. What type of cyber-crime, its laws and punishments does section 66 of the Indian IT Act holds? [a]

   (a) Cracking or illegally hack into any system (b) Putting antivirus into the victim

   (c) Stealing data (d) Stealing hardware components

5. Download copy, extract data from an open system done fraudulently is treated as _____. [b]

   (a) cyber-warfare (b) cyber-security act

   (c) data-backup (d) cyber-crime

6. What is not the definition of Hacking? [c]

   (a) The gaining of unauthorized access to data in a system or computer.

   (b) Breaking into computer system

   (c) Deliberate deception to secure unfair or unlawful gain

   (d) valid concept

7. What type of cyber-crime, its laws and punishments does section 66 of the Indian IT Act holds? [c]

   (a) Putting antivirus into the victim (b) Stealing data

   (c) Cracking or illegally hack into any system (d) Stealing hardware components

8. Cracking digital identity of any individual or doing identity theft, comes under _____ of IT Act. [b]

   (a) Section 65 (b) Section 66

   (c) Section 68 (d) Section 70

Rahul Publications

9. Among the following which is not suitable in terms of cyber forensics _____. [b]

(a) Recovering deleted files (b) Developing security

(c) Processing hidden files (d) Tracing artifacts

10. Which of the following techniques are used during computer forensics investigations? [d]

(a) Cross-drive analysis (b) Live analysis

(c) Deleted files (d) All of the above

Rahul Publications

Fill in the blanks

1. _____ is an intricate environment that involves interactions between people, software, and services.
2. The principal impetus of Information Technology Act, 2000 is _____.
3. _____ encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly
4. Full form of ICERT _____.
5. _____ is an application of information and communication technology (ICT) for delivering Government Service.
6. The aim of indian cyber space is _____.
7. The National Cyber Security Policy is formed in _____ year.
8. _____ is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence.
9. _____ is the science of extracting forensic information from digital storage media like Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc.,
10. _____ is a process that follows the Internet activity backwards, from the recipient to the user.

Rahul Publications

ANSWERS

1. Cyber space.
2. To offer reliable legal inclusiveness to eCommerce, facilitating registration of real-time records with the Government.
3. NIST Cybersecurity Framework
4. Indian Computer Emergency Response Team
5. Electronic Governance
6. To provide govt with IT solutions.
7. 2013.
8. Computer forensics
9. Disk forensics
10. Tracing

FACULTY OF COMMERCE

B.Com. III Year VI - Semester(CBCS) Examination

Model Paper - I

CYBER SECURITY

Time: 1½ Hours] [Max. Marks : 50

PART – A (5 × 2 = 10 Marks)

Note: Answer any five of the following questions not exceeding 20 lines each.

ANSWERS

1. What is cyber security? **(Unit-I, SQA.1)**
2. What is cyber terrorism? **(Unit-I, SQA.5)**
3. Hypertext Transfer Protocol Secure(HTTPS). **(Unit-II, SQA.2)**
4. Types of Malware **(Unit-III, SQA.5)**
5. Detection Method of IDS. **(Unit-III, SQA.10)**
6. Data Encryption Standard **(Unit-IV, SQA.1)**
7. What is digital signature? **(Unit-IV, SQA.4)**
8. Define Cyber space. **(Unit-V, SQA.1)**

PART – B (5 × 8 = 40 Marks)

Note: Answer all the questions in not exceeding four pages each.

9. (a) What is deception technology? Explain about it. **(Unit-I, Q.No.29)**

OR

(b) What is Vulnerability in Cyber Security? Explain about it. **(Unit-I, Q.No.13)**

10. (a) What are the various issues in securing web applications? **(Unit-II, Q.No.1)**

OR

(b) Explain the challenges for web security. **(Unit-II, Q.No.7)**

11. (a) Explain various types of malware infection and attacks. Write about how to remove malware from the devices. **(Unit-III, Q.No.5)**

OR

(b) Write about system integrity validataion. **(Unit-III, Q.No.14)**

12. (a) What is Cryptography? Explain briefly. **(Unit-IV, Q.No.1)**

OR

(b) Write about security protocols at application layer. **(Unit-IV, Q.No.13)**

13. (a) Explain cyber security regulations. **(Unit-V, Q.No.2)**

OR

(b) How data can be hidden in computer forensics and explain how hidden data can be investigated in cyber forensics. **(Unit-V, Q.No.13)**

FACULTY OF COMMERCE

B.Com. III Year VI - Semester(CBCS) Examination

Model Paper - II

CYBER SECURITY

Time: 1½ Hours] [Max. Marks : 50

PART – A (5 × 2 = 10 Marks)

Note: Answer any five of the following questions not exceeding 20 lines each.

ANSWERS

1. What are cyber security safe guards? **(Unit-I, SQA.9)**
2. What is Biometrics in Cybersecurity? **(Unit-I, SQA.13)**
3. OAP Communication Model **(Unit-II, SQA.5)**
4. HIPS. **(Unit-III, SQA.12)**
5. Network Intrusion Detection System(NIDS) **(Unit-III, SQA.7)**
6. What is firewall management? **(Unit-IV, SQA.8)**
7. Pretty Good Privacy (PGP) **(Unit-IV, SQA.10)**
8. What is cyber forensics? **(Unit-V, SQA.7)**

PART – B (5 × 8 = 40 Marks)

Note: Answer all the questions in not exceeding four pages each.

9. (a) What is a Threat in Cyber security? Explain the types of Cyber security threats. **(Unit-I, Q.No.4)**

OR

(b) What is open data? Explain how can we openly access to organizational data. **(Unit-I, Q.No.17)**

10. (a) What is SOAP? Explain about SOAP protocol structure. **(Unit-II, Q.No.3)**

OR

(b) Explain various security considerations in web security. **(Unit-II, Q.No.6)**

11. (a) Explain what are Internal Data Security Threats and How to deal with them. **(Unit-III, Q.No.2)**

OR

(b) Explain about Network based Intrusion detection system. **(Unit-III, Q.No.8)**

12. (a) Explain about the function of asymmetric key cryptography. **(Unit-IV, Q.No.5)**

OR

(b) Explain how security in the network layer managed using IPSec protocol. **(Unit-IV, Q.No.21)**

13. (a) How internet tracing can be done? Explain various methods to track internet access. **(Unit-V, Q.No.16)**

OR

(b) What is cyber forensics ? Explain computer forensic services? **(Unit-V, Q.No.8)**

FACULTY OF COMMERCE

B.Com. III Year VI - Semester(CBCS) Examination

Model Paper - III

CYBER SECURITY

Time: 1½ Hours] [Max. Marks : 50

PART – A (5 × 2 = 10 Marks)

Note: Answer any five of the following questions not exceeding 20 lines each.

ANSWERS

1. What is cryptography? **(Unit-I, SQA.14)**
2. What is Vulnerability in Cyber Security? **(Unit-I, SQA.7)**
3. What is authorization process? **(Unit-II, SQA.6)**
4. Protocol-based Intrusion Detection System(PIDS) **(Unit-III, SQA.9)**
5. Intrusion Detection System. **(Unit-III, SQA.6)**
6. Types of Firewall **(Unit-IV, SQA.7)**
7. Explain briefly about TLS Protocol. **(Unit-IV, SQA.12)**
8. Tracing memory in real-time. **(Unit-V, SQA.10)**

PART – B (5 × 8 = 40 Marks)

Note: Answer all the questions in not exceeding four pages each.

9. (a) Define cyber crime? What are the various methods in cyber crime? How to prevent them. **(Unit-I, Q.No.7)**

OR

(b) What is a software vulnerability? Explain about the most common security vulnerabilities. **(Unit-I, Q.No.14)**

10. (a) What is authorization process? Explain about various patterns of authorization process. **(Unit-II, Q.No.5)**

OR

(b) Explain about the security protocols in HTTPS. **(Unit-II, Q.No.2)**

11. (a) What is privilege abuse? Explain how to handle them. **(Unit-III, Q.No.3)**

OR

(b) What Is a Network Intrusion Prevention System and How Does it Work? **(Unit-III, Q.No.10)**

12. (a) Explain working mechanism of PGP. **(Unit-IV, Q.No.14)**

OR

(b) Explain briefly about TLS Protocol. **(Unit-IV, Q.No.18)**

13. (a) What is the National Cyber Security Policy? Explain about it. **(Unit-V, Q.No.7)**

OR

(b) Explain about email headers. **(Unit-V, Q.No.15)**