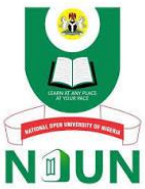
COURSE GUIDE

CYB 201
INTRODUCTION TO CYBERSECURITY STRATEGIES

Course Team NOUN (Course Developer)
Dr. Latifat A. Odeniyi. (Course Writer)-NOUN
Dr. F. A. Oladeji (Content Editor)
Awe Olaniyan Joseph (Copy Editor)



NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
University Village
Plot 91, Cadastral Zone
Nnamdi Azikiwe Expressway
Jabi, Abuja

Lagos Office
14/16 Ahmadu Bello Way
Victoria Island, Lagos

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Printed 2024

ISBN: 978-978-786-271-1

CONTENTS

INTRODUCTION

Welcome to CYB 201: Introduction to Cybersecurity Strategies. CYB 201 is a two-credit unit course that has a minimum duration of one semester. It is a compulsory course for graduate students that are enrolled in BSc Cybersecurity at the National Open University of Nigeria. The course guide through the various strategies of cybersecurity and methodologies for effective protection against cyber threats and attacks.

COURSE COMPETENCIES

- Teaching about various Cyber Attacks and threats
- Ways of identifying various means of Cyber Attacks
- System protection against all forms of attacks

COURSE OBJECTIVE

- To identify various cyber security strategies .

WORKING THROUGH THIS COURSE

To successfully complete this course, read the study units, do all assessments, open the links and read, participate in discussion forums, read the recommended books and other materials provided, prepare your portfolios, and participate in the online facilitation.

Each study unit has introduction, intended learning outcomes, the main content, conclusion, summary and references/further readings. The introduction will tell you the expectations in the study unit. Read and note the intended learning outcomes (ILOs). The intended learning outcomes tell you what you should be able to do at the completion of each study unit. So, you can evaluate your learning at the end of each unit to ensure you have achieved the intended learning outcomes. To meet the intended learning outcomes, knowledge is presented in texts, arranged into modules and units. You can print or download the texts and save in your computer or external drive. The conclusion gives you the theme of the knowledge you are taking away from the unit. Unit summaries are presented in downloadable audios and videos.

There are two main forms of assessments – the formative and the summative. The formative assessments will help you monitor your

learning. This is presented as in-text questions, discussion forums and Self-Assessment Exercises.

The summative assessments would be used by the university to evaluate your academic performance. This will be given as Computer Base Test (CBT) which serve as continuous assessment and final examinations. A minimum of three computer base test will be given with only one final examination at the end of the semester. You are required to take all the computer base tests and the final examination.

There are 23 study units in this course divided into 8 modules. The modules and units are presented as follows:

STUDY UNITS

Module 1 Introduction to Cybersecurity

Unit 1 Basic Concepts: cyber, security, confidentiality, integrity, availability, authentication, access control, non-repudiation, fault-tolerant methodologies
Unit 2 Impact of Cybersecurity on Civil and Military Institutions, Privacy, Business, and Government Applications

Module 2 Security Policies and Best Practices

Unit 1 Security Policies
Unit 2 Best Current Practices
Unit 3 Testing Security
Unit 4 Incident Response

Module 3 Risk Management and Disaster Recovery

Unit 1 Risk Management
Unit 2 Disaster Recovery
Unit 3 Access Control

Module 4 Cryptography and Secure Communication

Unit 1 Basic Cryptography and Methodologies
Unit 2 Steganography

Module 5 Cyber Attacks and Defence Mechanisms

Unit 1 Definition and Classification of Cyber-Attacks
Unit 2 Denial of Service (and other) Attack Strategies, Worms, Viruses
Unit 3 Transfer of Funds/Value Across Networks

Module 6 Operating System and Network Security

Unit 1 Operating System Protection Mechanisms
Unit 2 Intrusion Detection Systems

Module 7 Vulnerabilities and Countermeasures

Unit 1 Software Application Vulnerabilities
Unit 2 Basic Formal Models of Security
Unit 3 Countermeasures Employed by Organizations and Agencies

Module 8 Cybersecurity Policies and Regulation

Unit 1 Cybersecurity Policy and Guidelines
Unit 2 Main Actors of Cyberspace and Cyber Operations
Unit 3 Role of Standards and Frameworks
Unit 4 Trends and developments in cybersecurity

REFERENCES AND FURTHER READINGS /WEB RESOURCES

Aseem Garg (2024) Advantages and Disadvantages of Cyber Security.

Retrieved from https://trainings.internshala.com/blog/author/aseem-garg

Cyber Hub (2024). What is Cybersecurity for Governments? Retrieved from https://www.checkpoint.com/cyber-hub/cybersecurity/what-is-cybersecurity-for-governments

EC-Council University (2024). Information Security Principles. Retrieved from https://www.eccu.edu/blog/cybersecurity/fundaentals-of-information-security

Grant Collins (2024). Complete Introduction to Cybersecurity. Retrieved from **https://www.udemy.com/course/complete introduction-to-cybersecurity**

https://saltcommunications.com/news/the-importance-of-cybersecurityin-military/

Mia Smith (2019). Principle of Cybersecurity. Retrieved from **https://www.quora.com/What-are-the-10-principles-ofcybersecurity**

Mohammad J Sear (2023). The Importance of Cybersecurity for Governments.Retrieved fromhttps://www.linkedin.com/pulse/importance-cybersecurity-governments-mohammad-j-sear

NextZen Minds (2024). What is the Impact of Cyber Security on Business?Retrievedfromhttps://www.linkedin.com/pulse/what impact-cyber-security-business-nextzen-minds-jp8ac

Safecore (2024). Cyber security in the government sector: the scenario, risks and future challenges. Retrieved fromhttps://safecore.io/en/ndustries/la-cyber-security-nel-settore-governativo-lo-scenario-irischi-e-le-sfide-future

Shivanshu (2024). Advantages and Disadvantages of Cyber Security. Retrievedfromhttps://intellipaat.com/blog/advantages-anddisadvantages-of-cyber-security

PRESENTATION SCHEDULE

The presentation schedule gives you the important dates for the completion of your computer-based tests, participation in forum discussions and participation at facilitation. Remember, you are to submit all your assignments at the appropriate time. You should guard against delays and plagiarisms in your work. Plagiarism is a criminal offence in academics and is highly penalized.
Assessment

There are two main forms of assessments in this course that will be scored. The Continuous Assessments and the final examination. The continuous assessment shall be in three-fold. There will be two Computer Based Assessment(s). The computer-based assessments will be given in accordance to university academic calendar. The timing

must be strictly adhered to. The Computer Based Assessments shall be scored a maximum of 10% each, while your participation in discussion forums and your portfolio presentation shall be scored maximum of 10% if you meet 75% participation. Therefore, the maximum score for continuous assessment shall be 30% which shall form part of the final grade.

The final examination for CYB 201 will be maximum of two hours and it takes 70 percent of the total course grade. The examination will consist of 70 multiple choice questions that reflect cognitive reasoning.
Note: You will earn 10% score if you meet a minimum of 75% participation in the course forum discussions and in your portfolios otherwise you will lose the 10% in your total score. You will be required to upload your portfolio using Google Doc. What are you expected to do in your portfolio? Your portfolio should be note or jottings you made on each study unit and activities. This will include the time you spent on each unit or activity.

HOW TO GET THE MOST FROM THE COURSE

To get the most in this course, you need to have a personal laptop and internet facility. This will give you adequate opportunity to learn anywhere you are in the world. Use the Intended Learning Outcomes (ILOs) to guide your self-study in the course. At the end of every unit, examine yourself with the ILOs and see if you have achieved what you need to achieve.

Carefully work through each unit and make your notes. Join the online real time facilitation as scheduled. Where you missed the scheduled online real time facilitation, go through the recorded facilitation session at your own free time. Each real time facilitation session will be video recorded and posted on the platform.

In addition to the real time facilitation, watch the video and audio recorded summary in each unit. The video/audio summaries are directed to salient part in each unit. You can assess the audio and videos by clicking on the links in the text or through the course page.
Work through all self-assessment exercises. Finally, obey the rules in the class.

FACILITATION

You will receive online facilitation. The facilitation is learner centred. The mode of facilitation shall be asynchronous and synchronous. For the asynchronous facilitation, your facilitator will:

- Present the theme for the week;
- Direct and summarise forum discussions;
- Coordinate activities in the platform;
- Score and grade activities when need be;
- Upload scores into the university recommended platform;
- Support you to learn. In this regard personal mails may be sent.
- Send you videos and audio lectures; and podcast

For the synchronous:

There will be eight hours of online real time contact in the course. This will be through video conferencing in the Learning Management System. The eight hours shall be of one-hour contact for eight times.
At the end of each one-hour video conferencing, the video will be uploaded for view at your pace.

The facilitator will concentrate on main themes that are must know in the course. The facilitator is to present the online real time video facilitation time table at the beginning of the course.
The facilitator will take you through the course guide in the first lecture at the start date of facilitation

Do not hesitate to contact your facilitator. Contact your facilitator if you:

- do not understand any part of the study units or the assignment.
- have difficulty with the self-assessment exercises
- have a question or problem with an assignment or with your tutor's comments on an assignment.

Also, use the contact provided for technical support. Read all the comments and notes of your facilitator especially on your assignments, participate in the forums and discussions. This gives you opportunity to socialise with others in the programme. You can raise any problem encountered during your study. To gain the maximum benefit from

course facilitation, prepare a list of questions before the discussion session. You will learn a lot from participating actively in the discussions.

Finally, respond to the questionnaire. This will help the university to know your areas of challenges and how to improve on them for the review of the course materials and lectures.

COURSE INFORMATION

Course Code: CYB 201
Course Title: Introduction to Cybersecurity Strategies
Credit Unit: 2

COURSE STATUS: COMPULSORY

Course Blurb: This course covers various strategies in cybersecurity like Basic concepts: cyber, security, confidentiality, integrity, availability, authentication, access control, non-repudiation and fault-tolerant methodologies for implementing security. Security policies, best current practices, testing security, and incident response, Risk management, disaster recovery and access control. Basic cryptography and software application vulnerabilities. Evolution of cyber-attacks.

Operating system protection mechanisms, intrusion detection systems, basic formal models of security, cryptography, steganography, network and distributed system security, denial of service (and other) attack strategies, worms, viruses, transfer of funds/value across networks, electronic voting, secure applications.

Cybersecurity policy and guidelines. Government regulation of information technology. Main actors of cyberspace and cyber operations. Impact of cybersecurity on civil and military institutions, privacy, business and government applications; examination of the dimensions of networks, protocols, operating systems, and associated applications. Methods and motives of cybersecurity incident perpetrators, and the countermeasures employed by organisations and agencies to prevent and detect those incidences.

Ethical obligations of security professionals. Trends and development in cybersecurity. Software application vulnerabilities. Evolution of cybersecurity and national security strategies, requirements to the

typologies of cyber-attacks that require policy tools and domestic response. Cybersecurity strategies evolving in the face of big risk. Role of standards and frameworks.

Semester: First
Course Duration: 13 Weeks
Required Hours for Study: 65

ICE BREAKER

You are welcome to CYB 201: Introduction to Cybersecurity Strategies, a two-unit course. Please upload your profile such as picture, workplace address, GSM number and other details on your wall. What are your expectations in this course? I am sure you are going to enjoy the course, please fasten your seat belt as you take off. Once again you are welcome.

MAIN COURSE

MODULE 1 INTRODUCTION TO CYBERSECURITY

Introduction

Cyber-attacks have become increasingly common, targeting businesses, governments, and individuals alike. According to a report by Cyber Security ventures, global cybercrime damages could reach a staggering $10.5 trillion annually by 2025, emphasizing the importance of cybersecurity. Through this lesson note, let us delve into what cyber security entails, the properties of cyber security, its various types, key principles, and the advantages and disadvantages that come with it, threats to CIA, business scenario for cyber security.

Unit 1 Basic Concepts: cyber, security, confidentiality, integrity, availability, authentication, access control, non-repudiation, fault-tolerant methodologies

Unit 2 Impact of Cybersecurity on Civil and Military Institutions, Privacy, Business, and Government Applications

In each unit, a particular topic was explored in detail and self-assessment exercises was highlight at the end of the unit. Finally, resources for further reading were highlighted at the end of each unit.

UNIT 1 BASIC CONCEPTS OF CYBERSECURITY

Unit structure

1.1 Introduction

You will learn from this unit, the basic concepts of cybersecurity which includes the definition, key principles of cybersecurity, types and importance of cybersecurity. After studying this unit, you will be equipped with various basic concepts in cybersecurity.

1.2 Learning Outcomes

By the end of this unit, you will be able to:

- appraise that cybersecurity concept worth studying
- understand the key principles of cyber security

1.3 Basic Concepts of Cybersecurity

1.3.1 What is Cybersecurity?

Cyber-space is a platform where you can process, receive and send information. It includes computer system, network, information stored on the network, network devices that you can connect to the network, all these constitute what is called Cyber space including telephone set. This cyber space is not saved, and the process to make it save is what is called Cybersecurity.

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity.

Cybersecurity can be divided into two parts: one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data while security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called **electronic information security** or **information technology security**. The human personal, professional, social, and working space is ruled and controlled by the internet. Being surrounded by the internet makes its growth a never-ending era because it has become essential to the day-to-day human lifestyle. Now we cannot even imagine our life without the internet, and the advancement of technologies is making it fast and easy.

Some other definitions of cybersecurity are:

Cybersecurity is the set of principles and practices designed to protect our computing resources and online information against threats. Cybersecurity is the technologies and processes that is 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. After all, that is what criminal wants, *data*. The network, servers, computers are just mechanisms to get to the data. Effective cybersecurity reduces the risk of cyber-attacks and protects organizations and individuals from the unauthorized exploitation of data, systems, networks, and technologies.

1.3.2 Key Principles of Cybersecurity

There are a number of significant cybersecurity principles to learn and apply. Here are some of the pertinent points to remember about key principles of cybersecurity:

Confidentiality: This is refers to the secrecy surrounding information. It guarantees that only users with the necessary rights, privileges, and legitimate needs can access information. When unauthorized individuals or systems access information, its confidentiality is compromised. Techniques used to maintain confidentiality include data encryption, password protection, user authentication (e.g. Two-factor authentication), access controls (Biometric verification), Security tokens, and the implementation of strict privacy policies.
For example, let assume that while trying to login to your Gmail account, someone spy and gotten the password, then such password has been compromised and it's no more confidential (Confidentiality has been breached).

Integrity: means that data cannot be altered without authorization. It entails preserving the consistency, precision, and reliability of information, preventing unauthorized alterations or tampering. Integrity also ensures that authorized users can only make modifications in an approved manner. One of the measures to ensure information security is to implement privacy-preserving keyword search, which enables the retrieval of files containing specific keywords without revealing their contents through decryption

For example, if an employee leaves an organisation, then in that case, data for that employee in all departments like accounts should be

updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit the employee data.

Availability: This principle ensures that information and systems are accessible to authorized users when needed. Availability is crucial for maintaining the functionality of information systems, minimizing downtime, and ensuring that authorized users can access the data they require. Strategies for maintaining availability include redundancy, backup systems, disaster recovery planning, robust infrastructure, and network load balancing.

Authentication: The process of verifying the identity of a user, device, or process before allowing access to sensitive data or systems.
For example, if a sender sends message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side, this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the two value matches, then it is known as valid transmission with the authentic or a genuine message being received at the recipient side

Non-repudiation: The assurance that the parties involved cannot repudiate or deny an action or transaction, such as sending an email. Data Integrity and Authenticity are pre-requisites for Non repudiation.

Authorization: Authorization is the process of allowing access to resources based on user roles and permissions. Access controls and privilege management can help with this. Authorization is crucial for preventing unauthorized access to sensitive information and resources.

Accountability: Accountability refers to holding individuals and organizations responsible for their actions. This can be achieved through measures such as logging and auditing. Ensuring accountability is critical for detecting and responding to cyber-attacks and other security incidents.
Individuals and organizations can protect themselves from a wide range of cyber dangers and maintain the safe and secure operation of their systems and networks by applying these cybersecurity principles.

1.3.3 Various aspects of Cybersecurity

Cybersecurity has become an indispensable part of our daily lives and it is essential to understand its different aspects and how it can benefit the society. Here are the various aspects of cybersecurity:

i. **Network Security:** It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.
ii. **Application Security:** It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the application to ensure that they are secure from attacks. Successful security begins from the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.
iii. **Information or Data Security:** It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.
iv. **Identity management:** It deals with the procedure for determining the level of access that each individual has within an organization.
v. **Operational Security:** It involves processing and making decisions on handling and securing data assets.
vi. **Mobile Security:** It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.
vii. **Cloud Security:** It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.
viii. **Disaster Recovery and Business Continuity Planning:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.
ix. **User Education:** It deals with the processes, monitoring, alerts, and plans on how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

1.3.4 Importance of Cybersecurity

Today, we live in a digital era where all aspects of our lives depend on the network, computer and other electronic devices, and software applications. All critical organizations such as the banking system, healthcare, financial institutions, governments, and manufacturing industries use devices connected to the Internet as a core part of their operations. Some of their information, such as intellectual property, financial data, and personal data, can be sensitive for unauthorized access or exposure that could have **negative consequences**. This information gives intruders and threat actors to infiltrate them for financial gain, extortion, political or social motives, or just vandalism.

Cyber-attack and other security attacks could endanger the global economy; hence, it is essential to have an excellent cybersecurity strategy to protect sensitive information from high-profile security breaches. Furthermore, as the volume of cyber-attacks grows, companies and organizations, especially those that deal with information related to national security, health, or financial records, need to use strong cybersecurity measures and processes to protect their sensitive business and personal information.

Self-Assessment Exercises

1.	Define Cyber Security
2.	State five (5) advantages and disadvantages of cybersecurity
3.	State the benefit of learning cyber security?

1.4 Summary

At the end of this unit, you have learnt the definition of cybersecurity, the key principles of cybersecurity and its importance.
You have learnt from this unit, how cyber-attack led to the evolution of cybersecurity and the importance of cybersecurity to our society.

1.5 References/Further Readings/Web Resources

Aseem Garg (2024) Advantages and Disadvantages of Cyber Security. Retrievedfrom https://trainings.internshala.com/blog/author/aseem-garg

EC-Council University (2024). Information Security Principles. Retrieved from https://www.eccu.edu/blog/cybersecurity/fundamentals-of-information-security

Grant Collins (2024). Complete Introduction to Cybersecurity. Retrieved from https://www.udemy.com/course/complete-introduction-to-cybersecurity

Mia Smith (2019). Principle of Cybersecurity. Retrieved from https://www.quora.com/What-are-the-10-principles-of-cybersecurity

Shivanshu (2024). Advantages and Disadvantages of Cyber Security. Retrieved from https://intellipaat.com/blog/advantages-and-disadvantages-of-cyber-security

1.4 Possible Answers to Self-Assessment Exercises

Define Cyber Security

Answer to SAE 1

Cybersecurity is the set of principles and practices designed to protect our computing resources and online information against threats.

State five (5) advantages and disadvantages of cybersecurity

Answer to SAE 2

Five (5) advantages of cyber security are:
i. Protection of Sensitive Data
ii. Business Continuity
iii. Compliance with Regulations
iv. Enhanced Customer Trust
v. Competitive Benefit and so on.

Five (5) disadvantages of cyber security are:
i. High Cost of Implementation
ii. Complexity
iii. Potential False Sense of Security
iv. Potential for Human Error
v. Limited Effectiveness Against Insider Threat

State the benefit of learning cyber security?

Answer to SAE 3

Learning cybersecurity is essential for safeguarding personal and organizational data against malicious attacks from hackers. By doing so, one can reduce exposure to potential financial and reputational risks.

Unit 2 Impact of Cybersecurity on Civil and Military Institutions, Privacy, Business, and Government Applications

Unit Structure

2.1 Introduction

You will learn the impact of cybersecurity on military institutions, on business as well as the impact on government application from this unit.

2.2 Learning Outcome(s)

At the end of this unit, you will be able to:
Identify the impact of cybersecurity on civil and military institutions
Understand the impact of cybersecurity on business and government applications

2.3 Impact of Cybersecurity on Civil and Military Institutions, Privacy, Business, and Government Applications

Cybersecurity or information technology security, protects sensitive information/data, networking systems, and programs from cyberattacks. It prevents malicious attacks designed to alter, destroy, gain access, extort, or delete a government’s or an organization's sensitive data and systems.

Government sector is frequently targeted by cyber-attacks due to the management of large amounts of sensitive data and the responsibility for safeguarding critical infrastructure. These attacks can manifest themselves in various forms, including phishing, malware, ransomware, and distributed denial of service (DDoS) attacks.

Having an effective data protection strategy and support of an expert cybersecurity company directly and indirectly support and align along with your business growth plan to protect your businesses and digital assets, cloud data from unauthorized access, hacking and threats

2.3.1 Impact of Cyber Security on Military Institutions

The military's primary mission is to provide security to all citizens. The rise in cyber-attacks can make this mission more difficult as it's becoming increasingly onerous to protect themselves, let alone the entire citizen. The widespread adoption of information technologies has increased the likelihood of cyber-attacks and the military along with every other global industry must work together with all stakeholders and experts to raise awareness and provide a secure cyberspace through the supply of resilient and robust cybersecurity technology to avert the effect on the citizen.
These cybersecurity skills are primarily focused on detecting, defending, responding to, and preventing cyber-attacks that may harm military systems and networks, which could have a negative impact on military operations. As a result, it could be argued that the military's primary responsibility in cybersecurity is to provide protection for information systems and communications.

Military's role in Cybersecurity

The military sector has been taking steps to gain a better grasp of the problems of cyber defense, which has resulted in greater operational planning integration. The overall goal of the military's cybersecurity and technology strategy is to mitigate any potential hazards. As a result, the military must fully integrate and embrace the cyber defense part of their work, as well as their overall cyber mindset.

Cybersecurity is a set of behaviours, methods, and technologies aimed at protecting systems, networks, data, computers, and program from harm, attacks, and illegal access in order to safeguard personal data and secrets. The military, like any other institution or business, relies on cybersecurity to keep itself safe.
Social security numbers and even the nation's top secrets are among the data that must be safeguarded. An example of this is when millions of troops were hit by a cyber-attack in 2015 which was able to access

social security numbers, family information, health records and even the fingerprints of 21.5 million federal employees. These pieces of data should be kept safe from any vulnerabilities or adversaries who could try to take advantage of them.

How the military can protect themselves & their citizens from Cyber Assault

Most cyber assaults target a vulnerable spot and then utilise that exploit to move to other parts of the system, implementing a combination of hardware and software attacks. Since hardware-based attacks are more challenging, the majority of cyber-attacks will be software-based. With attacks coming from all directions and employing ever-increasing degrees of stealth and sophistication, every networked device, from the personal to the most guarded government or military systems, requires some type of cyber defence.

Defense groups, such as armed forces on land, at sea, and in the air, can only execute important duties and missions if information is exchanged securely. By using Salt Communications, the military has the capability to send secure messages, broadcasts, media, reports, as well as carry out secure calls. As a result, security officers may swiftly and securely access information being sent from within the system and transmit information to relevant parties within the platform.

By providing complete ownership of Secure Communications

Salt Communications works with large military clients across the globe who require complete assurance over the security and privacy of their communications platform, from where it’s being hosted, to whom is being granted access.

Providing the capability to send secure messages and carry out secure calls, Salt supports Military clients with protected instant messaging features and a host of additional unique capabilities. Military partners can utilise message broadcasting, the ability to keep key personnel informed by pushing out real time alerts to groups of users within an organisation, and a real-time incident reporting function to ensure efficient transmission of incident details back to headquarter.

2.3.2 Impact of Cyber Security on Business

Cyber security is a must for all sized businesses. Cloud data storage made lives easier and better for business owners. A business organization’s services or business ideas or product designs, its

technologies, and customer information, user privacy data and marketing strategies are the most important and valuable assets.
As businesses run and store their business and customers data online, cloud storage infrastructure becomes increasingly vulnerable to cyber threats and attacks. Protection and dealing with cyber attackers increase cyber protection costs along with the regular business operations cost.

Is your business at Risk of a Data Breach by Cyber threats?
Many business owners think that their business is not targeted by online intruders and cyber attackers but local and abroad cyber criminals will target all sized businesses, data infrastructures and cloud assets no matter the location, country and revenue size. All types of business are victim of cyber-attack, be it technologies, business operation, financial investment, relationship with customers, and brand reputation could be at risk. Small medium corporate businesses are prone to cybersecurity threats as they do not take any serious measures to protect themselves against these cyber-attacks.

Cyber attackers and intruders always look to gain access to business' sensitive information and users' data from various sources including business, in-house employees and customers, third party applications and lots more.

Why is Cyber Security Important for Businesses?

1. Secures data from theft
2. Prevents financial losses
3. Avoid legal liability for data breaches
4. Protects the reputation of your business
5. Supports the fight against the rise in cybercrime

Ways by which Cyber-attacks can Happen/occur in businesses

- Cybersecurity for business is about monitoring and protecting technology and data or information from illegal access, accidental damage, inside threats, theft and all kinds of damage.
- Unauthorised access of computers, hardware and mobile devices
- Infecting the data storage sources with malware
- Cyber-attacks to your technology or website or digital assets
- Hacking the computers or third-party systems
- Spamming you with emails containing malware
- Unauthorised access to your business data through your employees

There are many better ways to minimise the impact of the cyber breach on businesses.

Most Common Cybersecurity Risks to Businesses

- Malware attacks
- Ransomware attacks
- Phishing attacks
- Weak passwords
- Insider threats

Types of Online Threats for Business

1. Phishing emails
2. Distribution of malware
3. Attacks of ransomware
4. Data breach
5. Cyber scams
6. Hacking
7. Identity theft
8. Denial of service

In cybersecurity impact to business, what kind of data do you think are mainly at risk?

1. Customer records
2. Email records
3. Financial records
4. Personal data
5. Business ideas
6. Business plans
7. Marketing strategy
8. Product design
9. Patent applications
10. Intellectual property
11. Employee information
12. Sales data or records
13. Banking transactions
14. Technologies

How do you think companies and organizations can benefit from cybersecurity solutions?

1. Protect your business
2. Protects personal information
3. Allows all staffs to work safely
4. Protects productivity
5. Denies spyware

6. Prevents adware
7. A Consolidated solution
8. Support your IT expert

How can a cyber threat be fixed to safeguard businesses?

1. Adopting to a Cybersecurity technology
2. Hiring a cyber security expertise
3. Notifying affected parties of a data breach
4. Public relations support
5. Disaster recovery plan
6. Business continuity
7. Data security practices

2.3.3 Impact of Cyber Security on Government Application

The government industry is a prime target of cyber-attacks for a variety of reasons. Some of the most common reasons include the fact that governments have access to highly sensitive data and they control critical infrastructure that can be disrupted by cyberattacks. Additionally, government agencies may be targeted by hacktivists with political motivations.

The government sector is frequently targeted by cyber-attacks due to the management of large amounts of sensitive data and the responsibility for safeguarding critical infrastructures. These attacks can manifest themselves in various forms, including phishing, malware, ransomware, and distributed denial of service (DDoS) attacks.

To counter such threats, several standards and guidelines have been developed. The National Institute of Standards and Technology (NIST) of the USA, for example, created the Framework for Improving Critical Infrastructure Cybersecurity, which establishes guidelines for defending critical infrastructures from cyber-attacks. The Organization for Economic Co-operation and Development (OECD) has also formulated specific guidelines for cybersecurity in public sector information systems and networks.

Governments actively collaborate with cybersecurity specialists to develop and implement advanced solutions. Technologies such as blockchain are gaining relevance in the government sector for the security of sensitive data and for the creation of reliable electronic voting systems.

However, significant challenges in government cybersecurity persist. The limited availability of funds and qualified cybersecurity personnel

can hinder the implementation of advanced security solutions in government institutions. Additionally, the increasing complexity of government IT infrastructures further complicates protection from cyber threats.

As a result, cybersecurity in the government sector is crucial to ensuring the security of sensitive information and critical infrastructure.

In recent years, cyberattacks have increasingly been used as a tool of war. The Russia-Ukraine conflict is a prime example of this, as cyber-attackers affiliated with Russia have launched attacks against Ukraine and its allies to disrupt their military operations and daily life. As these types of attacks grow more common, government organizations face increased security risks.

The Importance of Cybersecurity to Government Institutions
Government institutions are entrusted with sensitive data and important responsibilities. A data breach or disruptive cyberattack can cause significant damage not only to the organization but also to its constituents. As a result, implementing strong cybersecurity to protect against these attacks is a major responsibility of government agencies.

Technological Evolution in the Government Sector

The government sector has undergone a technological evolution which is significant in recent decades, with the adoption of advanced technologies to improve the efficiency and quality of public services offered to citizens. Below is the list of some of the main technologies that have influenced the evolution of the government sector:

Cloud Computing: Cloud computing has enabled the government sector to store and manage large amounts of data more efficiently and securely, improving the sharing of information between government agencies and citizens.

Big data analytics: Big data analytics has enabled the government sector to gain a better understanding of data, enabling governments to make more informed decisions and improve resource planning and management.

Artificial Intelligence (AI): AI is becoming increasingly important in the government sector, with applications ranging from data management to process automation and city planning. AI can improve efficiency and accuracy in managing public services.

Internet of Things (IoT): IoT can improve the efficiency of public services by enabling real-time monitoring of critical infrastructure such as bridges, roads and public transportation systems.

Blockchain: Blockchain technology is becoming increasingly important in the government sector, with applications ranging from creating secure electronic voting systems to managing digital identities.

Process automation: process automation can improve the efficiency of public services, reducing the processing time for citizens' requests and improving data and information management.

Virtual and augmented reality: virtual and augmented reality can be used in the government sector for training, simulation and public infrastructure design.

The adoption of advanced technologies has allowed governments to improve the efficiency of their operations, automating manual processes and reducing response times. It has improved the quality of the services offered, has facilitated the interaction between citizens and the government and has increased the transparency and accountability of the government sector, making it easier for citizens to monitor government activities and access information on budgets, policies and decisions.

Vulnerabilities in the Sector

The technological vulnerabilities of the government sector are numerous and can have serious consequences on national security, the economy and the privacy of citizens. Below are some of the key vulnerabilities and challenges governments face:

Old and outdated technological infrastructure: Many governments use outdated computer systems and networks that haven't been updated or replaced for years. This makes these systems more vulnerable to cyber-attacks and increases the risk of malfunctions and service interruptions.

Lack of security updates: Government organizations often do not apply security updates promptly, which leaves their systems exposed to known vulnerabilities that could be exploited by attackers.

Design and configuration flaws: Design and configuration errors in government systems and applications can create vulnerabilities that can be exploited by attackers to gain access to sensitive information or disrupt services.

Insider threats: Insider threats, such as dishonest or negligent government employees, can pose a significant risk to the security of government systems and information. They can use their knowledge and access to systems to steal information or damage infrastructure.

Phishing and Social Engineering: Phishing and social engineering attacks are common in the government sector and can be used to trick employees into gaining access to sensitive systems and information.

Ransomware: Ransomware attacks, which block access to data and systems until a ransom is paid, have become increasingly frequent and sophisticated. Governments are often targeted due to their reliance on critical services and need to quickly restore operations.

Supply chain attacks: Supply chain attacks, in which attacker's compromise software or hardware vendors to infiltrate government organizations, are on the rise and pose a significant security threat to critical infrastructure.

Cyber warfare and espionage: Nation-states can use sophisticated hacking capabilities to infiltrate government systems in order to steal sensitive information, manipulate decision-making processes or cause disruptions in services.

Lack of qualified safety personnel: Many governments struggle to recruit and retain staff with cybersecurity expertise, which can compromise their ability to adequately protect systems and information.
To address these vulnerabilities, governments must invest in training, advanced security technologies, and collaboration with private sector experts to protect the entire infrastructure.

Self-Assessment Exercises

1. Why do you think Cybersecurity is Important for Businesses?
2. Mention various ways by which cyber-attacks can happen
3. Mention some most common cybersecurity risks to businesses?

2.4 Summary

At the end of this unit, you have learnt about impact of cybersecurity to civil and military institutions, businesses and government agencies.

You have learnt from this unit that cybersecurity has great impact on civil and military institutions as well as private and government business. Therefore, it is important that you understand how best to protect systems in all areas of need against cyber threat.

2.5 References/Further Readings/Web Resources

Cyber Hub (2024). What is Cybersecurity for Governments? Retrieved from https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity-for-governments

https://saltcommunications.com/news/the-importance-of-cybersecurity-in-military/

Mohammad J Sear (2023). The Importance of Cybersecurity for Governments. Retrieved from https://www.linkedin.com/pulse/importance-cybersecurity-governments-mohammad-j-sear

NextZen Minds (2024). What is the Impact of Cyber Security on Business? Retrieved from https://www.linkedin.com/pulse/what-impact-cyber-security-business-nextzen-minds-jp8ac

Safecore (2024). Cyber security in the government sector: the scenario, risks and future challenges. Retrieved from https://safecore.io/en/industries/la-cyber-security-nel-settore-governativo-lo-scenario-i-rischi-e-le-sfide-future

2.6 Possible Answers to Self-Assessment Exercises

Why do you think Cybersecurity is Important for Businesses?

Answer to SAE 1

1. Secures data from theft
2. Prevents financial losses
3. Avoid legal liability for data breaches
4. Protects the reputation of your business
5. Supports the fight against the rise in cybercrime

Mention various ways by which cyber-attacks can happen.

Answer to SAE 2

1. Unauthorised access of computers, hardware and mobile devices
2. Infecting the data storage sources with malware
3. Cyber-attacks to your technology or website or digital assets
4. Hacking the computers or third-party systems
5. Spamming you with emails containing malware
6. Unauthorised access to your business data through your employees

Mention some most common cybersecurity risks to businesses?

Answer to SAE 3

They are:
1. Malware attacks
2. Ransomware attacks
3. Phishing attacks
4. Weak passwords
5. Insider threats

MODULE 2 SECURITY POLICIES AND BEST PRACTICES

Introduction

Cybersecurity generally works for securing the organization's important assets, Employee details, and the operations performed from the hacker's attacks or hacks. The cybersecurity solutions are available to have a secure and less risky operation from cyber-attacks. High authorities and Information Technology (IT) professionals are more prone to cyber-attacks and thereby need to take security precautions seriously to limit loss of their data and assets. Though, not only IT experts and senior managers should be concerned about security in an organization, all staff members working with a computer system should know the cybersecurity policy for protecting their data and systems.

Unit 1 Security Policies
Unit 2 Best Current Practices
Unit 3 Testing Security
Unit 4 Incident Response

In each unit, each topic was explored in details and self-assessment was captured. Also, resources for further readings appear at the end of each unit.

Unit 1 Security Policies

Unit structure

1.1 Introduction
1.2 Learning Outcomes
1.3 Security Policies
    1.3.1 Definition of Security Policy:
    1.3.2 Need for security policy
    1.3.3 Types of security policy
    1.3.4 Key elements of security policy
    1.3.5 How to create security policy
1.4 Summary
1.3 References/Further Readings/Web Resources
1.6 Possible Answers to Self-Assessment Exercise(s

1.1 Introduction

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.

1.2 Learning Outcomes

BY the end of this unit, you will be able to:

- explore reasons for security policy
- state ways to create security policy
- explain the various types of security policy

1.3 Security Policies

1.3.1 Definition of security policy?

security policy is a document that states in writing how a company plans to protect its physical and information technology (IT) assets.
Security policies are living documents that are continuously updated and changing as technologies, vulnerabilities and security requirements change.

A company's security policy may include an acceptable use policy which describe how the company plans to educate its employees about protecting the company's assets. It also includes an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the policy to ensure that necessary corrections are made to safeguard organization’s data.

1.3.2 Needs for Security Policies

Needs for security policy are highlighted below:

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 data and information.

2. It upholds discipline and accountability: When any human mistake occurs, system security is compromised, then the security policy of the organization will back up any disciplinary action and 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.

1.3.3 Types of Cybersecurity Policies

An organization may implement various cybersecurity policies. Some of the most common ones include the following:

1. Internet Policy: Computer Systems for both personnel and professionals use the Internet as the main source. Employees, Clients, and Stakeholders have to follow certain policies and regulations on how to use the Internet.
2. Internet of Things (IoT) Policy: IoT cyber security deals with technology that safeguards networks and connected devices in the Internet of things (IoT). This strategy creates an IoT structure flow that ensures its security and efficient operation. The Organization needs a specific standard to protect the policy against the IoT using devices.
3. Server Security Policy: The server contains all the information of the network in the organization and using the server security policy can protect it. It provides the steps needed to secure the system from attacks, data breaches, and any illegal activities. It

outlines the requirements and standards for internal server base configuration.

4. Password Policy: Companies are prohibited to use simple passwords under this policy and must develop strong passwords and update them frequently to prevent security breaches.
5. Email Security Policy: An email security policy defines the acceptable use of corporate email systems to help protect the organization against spam, phishing, and malware (such as ransomware) and to prevent misuse of corporate email. This type of policy may include general rules for how corporate email can and should be used, as well as specific guidance on how to handle suspicious links and email attachments.
   The Protocol used for the Email is a Simple Mail Transfer Protocol and it does not provide any security. So, using the electronic mail policy, people can come to know the list of rules followed. It reduces the possibilities of risk and makes people to understand how to interact with other users.
6. Firewall Policy: Every Organization network has a firewall, and firewall policy keeps track of its traffic. It makes sure that any incoming internet traffic is safe and doesn't endanger the organization.
7. E-Commerce Policy: Companies with a significant online presence must adhere to this guideline. It makes ensuring that these services are managed and run by the prescribed criteria.
8. Account Information Policy: The Account information policy specifies a procedure for setting up and managing accounts with access to the data. The policy must be followed while using the account and upon removing it, whether it belongs to an employee or a client.
9. Wireless Connection Policy: The wireless Fidelity (Wi-Fi) networks that businesses and their employees utilize are quite specific. And a big reason for that is this policy. It outlines the policies that businesses must adhere to when using unprotected, public Wi-Fi to safeguard data.
10. Remote Access System Policy: The Remote policy specifies how the internal networks of an organization can be connected remotely. The company's network frequently accesses vulnerable network areas where they slip under the radar. Safety is ensured by this policy in certain circumstances.
11. IT Security Policy: An organization’s IT security policy defines the rules and procedures for protecting the organization against cyber threats. Some of the aspects of an IT security policy include acceptable use of corporate assets, incident response plans, business continuity strategies, and the organization’s plan for achieving and maintaining regulatory compliance.

12. BYOD Policy: A BYOD policy defines rules for personal devices that are used for work. These policies commonly define security requirements for these devices, such as the use of an endpoint security solution, strong passwords, and a virtual private network (VPN) when connecting to corporate networks and IT assets via an untrusted network.
13. Physical Security Policies: Physical security policies protect all physical assets in an organization, including buildings, vehicles, inventory and machines. These assets include IT equipment, such as servers, computers and hard drives.

Protecting IT physical assets is particularly important because the physical devices contain company data. If a physical IT asset is compromised, the information it contains and handles is at risk. In this way, information security policies are dependent on physical security policies to keep company data safe.

Physical security policies include the following information:
sensitive buildings, rooms and other areas of an organization;
who is authorized to access, handle and move physical assets;
procedures and other rules for accessing, monitoring and handling these assets; and responsibilities of individuals for the physical assets they access and handle.

Security guards, entry gates, and door and window locks are all used to protect physical assets. Other, more high-tech methods are also used to keep physical assets safe. For example, a biometric verification system can limit access to a server room. Anyone accessing the room would use a fingerprint scanner to verify they are authorized to enter.

1.3.4 Key Elements of Security policy

Some of the key elements of an organizational information security policy include the following:

- statement of the purpose;
- statement that defines who the policy applies to;
- statement of objectives, which usually encompasses the CIA triad;
- authority and access control policy that delineates who has access to which resources;
- data classification statement that divides data into categories of sensitivity -- the data covered can range from public information to information that could cause harm to the business or an individual if disclosed;

- data use statement that lays out how data at any level should be handled -- this includes specifying the data protection regulations, data backup requirements and network security standards for how data should be communicated, with encryption, for example;
- statement of the responsibilities and duties of employees and who will be responsible for overseeing and enforcing policy; security awareness training that instructs employees on security best practices -- this includes education on potential security threats, such as phishing, and computer security best practices for using company devices; and
- effectiveness measurements that will be used to assess how well security policies are working and how improvements will be made.

1.3.5 How to Create a Cybersecurity Policy

Creating a cybersecurity policy is a multi-stage process with the following key steps:

Determine the Threat Surface: Different policies are designed to address different threats and risks to the organization. The first step in writing a policy is to gain a clear understanding of the systems and processes to be regulated, such as the use of personal devices for business.

Identify Applicable Requirements: Corporate cybersecurity policies may have both internal and external drivers, such as corporate security goals and regulatory requirements (HIPAA, PCI DSS, etc.). To develop a cyber security policy, the next step is to define the requirements that the policy should fulfill.

Draft the Policy: After identifying requirements, the next step is to draft the policy. This should be accomplished by a team with stakeholders from IT, legal, HR, and management.

Solicit Feedback: A cyber security policy is most effective if it is clear and comprehensible to employees. Soliciting feedback from employees outside the policy group can help to avoid misunderstandings and similar issues.

Train Employees: After the policy has been developed, it needs to be disseminated through the organization. Also, employees will need to be trained on these policies to follow their requirements.

Regularly Update the Policy: Policies can go out of date, and their requirements may change. They should be regularly reviewed and updated to keep them up-to-date.

Self- Assessment Exercise(s)

1. Discuss the important of security policies.
2. What to consider when creating a security policy?
3. What is the main purpose of a security policy?

1.4 Summary

At the end of this unit, you have learnt the various classifications of security policy. In the next unit you will learn about current practices.

You have learnt from this unit how to develop a security policy ant its importance in organizations.

1.5 References/Further Readings/Web Resources

Ani Khachatryan (2024). Information Security Policies Every Organization Should Implement.Origin: https://www.ekransystem.com/en/blog/information-security-policies

Ben Lutkevich (2024). Security Policies. Retrieved from https://www.techtarget.com/searchsecurity/definition/security-policy

Cyber Security Policies. Retrieved from Javapoint https://www.javatpoint.com/cyber-security-policies

Robert Grimmick (2023) What is a Security Policy? Definition, Elements, and Examples. Retrieved from https://www.varonis.com/blog/what-is-a-security-policy

1.5 Possible Answers to Self- Assessment Exercise(s)

Discuss the important of security policies.

Answer to SAE 1

Important of security policies - Security policies are important because they protect an organizations' assets, both physical and digital. They identify all company assets and all threats to those assets.

What to consider when creating a security policy?

Answer to SAE 2

The factors considered when creating a security policy are:

1. Cloud and mobile
2. Data classification
3. Continuous updates
4. Policy frameworks

What is the main purpose of a security policy?

Answer to SAE 3

A security policy serves to communicate the intent of senior management with regards to information security and security awareness. It contains high-level principles, goals, and objectives that guide security strategy.

Unit 2 Cybersecurity Best Practices

Unit Structure

2.1 Introduction

Cybersecurity Best Practices Guideline (Guideline) seeks to provide companies with guiding principles that are consistent with international best practices, for establishing adequate cybersecurity frameworks to ensure cyber resilience. The cyber security framework to be established should be proportional to the company's business model, complexity of operations and risks.

2.2 Learning Outcomes

At the end of this unit, you should be able to:
State the best practices for protecting your company from cyber threat
Understand various cybersecurity best practices guideline

2.3 Cybersecurity Best Practices

3.3.1 Definition of cybersecurity best practices

Best practices in cybersecurity are the principles and practices that guide the use of computer applications again threats and attacks. These practices along with many other cybersecurity frameworks and tools will

help increase security posture through implementing a strong cybersecurity program.

2.3.2 List of Cybersecurity Best Practices

Among the list of best practices in cybersecurity are:

1. General Computer Usage
2. General Internet Browsing
3. Malware Defense
4. Removable Information Storage Media (Pen Drive/External Hard Disk etc.)
5. Smart Device (Smart Phone, Tabs, etc.)

2.3.3 General Computer Usage

1. Use account with limited privileges on systems and avoid accessing with administrator privileges for day-to-day usage.
2. Keep Operating System, Application software and Anti-Virus software updated by applying the latest service packs and patches.
3. Backup of important files at regular intervals.
4. Do not leave system unattended. Log out of or lock your computer when stepping away, even for a moment
5. Supervise maintenance or rectification of faults in the system by service engineers.
6. Do not download unfamiliar software off the Internet.
7. Remove unnecessary programs or services from computer: Uninstall any software and services you do not need
8. Restrict remote access. If file sharing is not required in your day-to-day work, disable file and print sharing.
9. Treat sensitive data very carefully.
10. Remove data securely: Remove files or data you no longer need to prevent unauthorized access to them. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system
11. If your networking devices are not using IPv6, disable IPv6 from computer.
12. Use system’s screen locking functionality to protect against physical access, such as a screen saver that won’t deactivate without a password, or just log out of everything so anyone that wants access has to log in again. The systems should be placed in a room which is dust free and has a good ventilation to avoid overheating of CPU.

13. Do not plug the computer directly to the wall outlet as power surges may damage computer. Instead use a genuine surge protector to plug a computer.
14. Don't eat food or drink near the PC.
15. There should be no magnets near to your PC.
16. Scan all the files after you download whether from websites or links received from e-mails.

2.3.4 General Internet Browsing

1. Always use updated anti-virus, Operating System applications and browser.
2. Use a web browser with sandboxing capability (like Google chrome, safari, etc.). Sandboxing usually contains malware during execution.
3. Download software from trusted source only.
4. Be wary of storing personal information on Internet.
5. Do not store any information you want to protect on any device that connects to the Internet.
6. Verify those you correspond with. It is easy for people to fake identities over the Internet.
7. Make a habit of clearing history from the browser after each logout sessions.
8. Delete Windows "Temp" and "Temporary Internet files" regularly.
9. Avoid using services that require location information.
10. Remember search engines track your search history and build profiles on you to serve you personalised results based on your search history.
11. Be conscious of what you are clicking on/downloading.
12. Some pop-ups have what appears to be a close button, but will actually try to install spyware when you click on it.
13. Remember that things on the internet are rarely free. "Free" Screensavers, etc. generally contain Malware.
14. Be wary of free downloadable software - There are many sites that offer customized toolbars or other features that appeal to users, which are likely to have backdoors.
15. Avoid Internet access through public Wi-Fi.
16. Never exchange home and office work related contents.
17. Avoid posting of photos with GPS coordinates.
18. Don't respond to email, instant messages (IM), texts, phone calls, etc., asking you for your password.
19. Only click on links from trusted sources. Never click on a mystery link unless you have a way to independently verify that it is safe. This includes tiny URLs.

20. Be extremely careful with file sharing software. File sharing opens your computer to the risk of malicious files and attackers. Also, if you share copyrighted files, you risk serious legal consequences.

2.3.5 Malware Defense

Always set automatic updates for Operating System, Antivirus and Applications.

Enable hidden file & system file view to find any unusual or hidden files. (My computer -> tools -> folder options -> view -> select enabled with “Show hidden file and folders” option and disable “Hide protected operating system files”)
Turn off auto play

(Win XP: Start -> Run -> type gpedit.msc -> Computer Configuration -> Administrative Templates -> System -> Double Click at Turn off Auto play -> Select Enabled -> Select “Turn off Auto play on:” to “All drives” and Click OK.

Windows 7: Start -> Run -> type gpedit.msc -> Computer Configurations -> Administrative Templates -> Windows Components -> Select “AutoPlay Policies” -> Double Click at “Turn off Auto play” -> Select Enabled -> Set “Turn off Auto play on:” to “All drives” and Click OK.)

Type: dir %temp% in “run” and delete all entries after opening any suspicious attachments.

Type “msconfig” in “run” and check for any unusual executable running automatically.

Check Network icon (for packets received and sent) / ADSL lights for data in non- browsing mode. Check data usage pattern in Mobile. If the outgoing is unusually high, then it is very likely that the system is compromised.

Type “ ipconfig/displaydns” in command prompt and look out for any URLs which you have not accessed recently.

Always be cautious while opening attachments even from the known sources. Try to use non-native applications for opening attachments.

Example for word document use, WordPad to open the attachment.

When in doubt, it's better to format the Internet connected with computer system rather than doing some "patch works".

2.3.6 Removable Information Storage Media (Pen Drive/External Hard Disk etc.)

Removable Information Storage Media (RISM) means any device which is capable of storing electronic information in any form. Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer.

For example, CDR (multi sessions), CD-RW, DVD-RW, BluRay Disk, MOD, USB Storage devices (Pen Drives, Media Cards, etc.), MP3 Players, MP4 Players, Smart Phones, Digital Camera, Watches with memory, Various types of Memory cards, Internet Data Card, External Hard Disk, or any other gadget having memory space and could be connected to a system through USB or any other ports or device connected through Network Share falls under Removable Information Storage Media.

Damaged /faulty RISM should never be handed over to outsiders / manufacturer for repair.

Sensitive information should be stored on removable media only when required in the cases of assigned duties.

All media must be stored in a safe and secure environment
All media must be handled with care and must be ensured that it is not kept near magnetic material and not exposed to extreme heat or pollution;

The computers should be enabled with "Show hidden file and folders" option and "Hide protected operating system files" should be disabled to view hidden malicious files in USB storage devices

Make sure there is no hidden file and folders present in the Media.
Autorun/Autoplay feature should be disabled in all the computers.
Avoid Baiting. (Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope that you will use the device and enable them to hack your computer). Do not use any electronic storage device unless you know its origin is legitimate and safe.
Scan all electronic media for Malware before use.

2.3.7 Smart Device (Smart Phone, Tabs, etc.)

Smart device is a device having any of the features like computation power, Internet access, storage capability, camera, recordings, GPS, etc. Smart phone, Tablets and so on falls under this category.

Most of the Smart Phones and Tablets (Tabs) are having equal computing power of a normal Desktop / Laptop systems. These gadgets are capable of delivering many services on Video, Voice, GPS and other computational applications like any other computer. Therefore, all cybersecurity issues related to computers are also applicable to these devices. Following are some of the security concerns of smart devices:

These are equally vulnerable to malware attacks and data leakages as ordinary Internet connected computers.
More application, features and service are available on Smart device for exploits than ordinary feature phones.

These gadgets are known to be used for bugging (audio and video), monitoring call details, contents, SMS monitoring, sending malicious SMS, Emails, spoofing, and other malicious activities without the knowledge of the user.

Android and IOS platform based Smart Phones and Tabs are known to have multiple vulnerabilities, which are being widely exploited by the attackers and adversaries.

Smart device must not be used for sensitive telephonic conversation.
The Wi-Fi and blue-tooth should be kept in turned-off mode.
A low-end basic mobile phone without camera / internet / Wi-Fi may be carried for sensitive voice conversation and contact details.
Internet connection in the Smart device will normally be kept in off-mode and it will be made 'on' on need basis to access internet.
No free applications should be loaded in the Smart device.

During repairs, do not leave Smart device unattended to deny the possibility of installation of malware.
Relevant anti-virus software should be installed in the smart device.
If the Smart device gets de-activated for any reason for few hours / a day, the service provider should be contacted immediately to ascertain the reason for deactivation.

If the battery gets unusually discharged very fast or device gets heated up without any user activity, then it is very likely some malicious traffic is consuming battery.

Free Wi-Fi should not be used at public places such as Airport. Turn off blue-tooth and Wi-Fi when use of the same is not required for operational purposes. Even when the same is in use, set default blue-tooth / Wi-Fi configuration to "non-discoverable".
Compromised smart device should not be connected with computer even for the purpose of charging.

Self-Assessment Exercises

1.	What is the basic cyber security best practices?
2.	What is the biggest problem in cybersecurity?
3.	What is the biggest weakness in cyber security?

2.4 Summary

At the end of this unit, you have learnt the definition of cybersecurity best practices and the different types of best practices to keep tract of.

At the end of this unit, you have learnt that cybersecurity best practice is important every system user to keep track of to avoid cyber theat. Therefore, it is important to understand how to reduce or guide against cyber threats using these best
practices.

2.5 Reference/Further Readings/Web Resources

Cycord (2024). Cyber Security Best Practices. Retrieved from https://www.iitbbs.ac.in/wp-content/uploads/2023/11/CyberSecurityBestPractices141123.pdf

Open Source (2024). Best Practices for Information Technology Security.pdf Retrieved from https://tourism.gov.in/sites/default/files/2019-10/Best%20Practices%20for%20Information%20Technology%20Security.pdf

2.6 Possible Answers to Self-Assessment Exercises

What is the basic cyber security best practices?

Answer to SAE 1

Using strong passwords, updating your software, thinking before you click on suspicious links, and turning on multi-factor authentication are the basics of what we call “cyber hygiene” and will drastically improve your online safety.

What is the biggest problem in cybersecurity?

Answer to SAE 2

i. Top Cybersecurity Threats are:
ii. Social Engineering.
iii. Third-Party Exposure.
iv. Configuration Mistakes.
v. Poor Cyber Hygiene.
vi. Cloud Vulnerabilities.
vii. Mobile Device Vulnerabilities.
viii. Internet of Things.
ix. Ransomware

What is the biggest weakness in cyber security?

Answer to SAE 3

i. Top Cybersecurity Vulnerabilities
ii. Zero-Day Vulnerabilities.
iii. Unpatched Software.
iv. Application Misconfiguration.
v. Remote Code Execution.
vi. Credential Theft.
vii. Security-Based Software.
viii. Wi-Fi Security.
ix. Firewalls.

Unit 3 Security Testing

Unit Structure

3.1 Introduction

Security testing is usually performed to ensure that the software is safe and secure by checking whether there is any information leakage by encrypting the application or using a wide range of software, hardware and firewalls. This testing makes sure that the software is not easily hacked by malicious codes and helps software developers to identify and remove loopholes in the software and to ensure that the system will not be attacked by hackers and other third-party intruders.

3.2 Learning Outcomes

By the end of this unit, you will be able to:

- define security testing.
- mention the goal of security testing
- describe the principle of security testing
- state the key areas in security testing.

3.3 Security Testing

3.3.1 What is Security Testing?

Security testing is an integral part of software testing, which is used to discover the weaknesses, risks, or threats in the software application and also help to stop the nasty attack from the intruders and make sure the

security of software applications is taken care of. It is the type of software testing that ensures security to software systems and applications.

The primary objective of security testing is to find all the potential ambiguities and vulnerabilities of the application so that the software does not stop working as a result of vulnerability. Security testing helps to identify all the possible security threats and also help the programmer to fix those errors and threats. It is a testing procedure, which is used to ensure that the data will be safe and also continue the working process of the software.

The Goal of Security Testing

The goal of security testing is to:

i. identify the threats in the system.
ii. measure the potential vulnerabilities of the system.
iii. help in detecting every possible security risk in the system.
iv. help developers fix security problems through coding.

In a nut-shell, the goal of security testing is to identify vulnerabilities and potential threats in a system or application and to ensure that the system is protected against unauthorized access, data breaches, and other security-related issues.

The main objectives of security testing are to:

1. Identify vulnerabilities: Security testing helps identify vulnerabilities in the system, such as weak passwords, unpatched software, and misconfigured systems, that could be exploited by attackers.
2. Evaluate the system's ability to withstand an attack: Security testing evaluates the system's ability to withstand different types of attacks, such as network attacks, social engineering attacks, and application-level attacks.
3. Ensure compliance: Security testing helps ensure that the system meets relevant security standards and regulations, such as HIPAA, PCI DSS, and SOC2.
4. Provide a comprehensive security assessment: Security testing provides a comprehensive assessment of the system's security posture, including the identification of vulnerabilities, the evaluation of the system's ability to withstand an attack, and compliance with relevant security standards.
5. Help organizations prepare for potential security incidents: Security testing helps organizations understand the potential

risks and vulnerabilities that they face, enabling them to prepare for and respond to potential security incidents.

6. Identify and fix potential security issues before deployment to production: Security testing helps identify and fix security issues before the system is deployed to production. This helps reduce the risk of a security incident occurring in a production environment.

3.3.2 How to Perform Security Testing

The security testing is needed to be done in the initial stages of the software development life cycle (SDLC) in order to save cost. Stages involved in the development of security testing are:

Step1
SDLC: Requirement stage
Security Procedures: In the requirement phase of SDLC, the security analysis of the business needs will be done and also verification to know which cases are manipulative and waste.

Step2
SDLC: Design stage
Security Procedures: In the design phase of SDLC, the security testing for risk exploration of the design will be done and also embraces the security tests at the development of the test plan.

Step3
SDLC: Development or coding stage
Security Procedures: In the coding phase of SDLC, the white box testing along with static and dynamic testing will be performed.

Step4
SDLC: Testing (functional testing, integration testing, system testing) stage
Security Procedures: In the testing phase of SDLC, one round of vulnerability scanning along with black-box testing will be done.

Step 5
SDLC: Implementation stage
Security Procedures: In the implementation phase of SDLC, **vulnerability scanning** will be done again and also perform one round of penetration testing**.**

Step 6
SDLC: Maintenance stage

Security Procedures: In the Maintenance phase of SDLC, impact analysis of impact areas will be performed. The test plan should contain the following:

1. The test data should be linked to security testing.
2. For security testing, test tools will be needed.
3. With the help of various security tools, analyze several test outputs.
4. Write the test scenarios or test cases that rely on security purposes, Example of security testing
5. Generally, the type of security testing includes the problematic steps based on overthinking, but sometimes the simple tests will help us to uncover the most significant security threats.

An example to understand how to do security testing on a web application:

1. First log in to the web application.
2. then log out of the web application.
3. then click the BACK button of the browser to verify that it was asking us to log in again, or we are already logged-in the application.

3.3.3 Techniques for Security Testing

Techniques/Methodologies followed in Security Testing are as follows.

i. **Black Box Testing:** In Black Box, testers are authorized to do testing on everything about the network topology and the technology.
ii. **Grey Box Testing:** In Grey Box, testers are provided with partial information about the system. It is a hybrid of white and black box models.
iii. **Tiger Box Testing:** It is done in a system that has a collection of operating systems and hacking tools. It helps security testers to conduct vulnerabilities assessment and attacks.

3.3.4 Security Testing Tools

To find the flaws and vulnerabilities in a web application, there are many free, paid, and open-source tools available in the market. The advantage of open-source tools is that it can bd easily customize to match the requirements. Some of the open-source tools are Zed Attack Proxy, Wfuzz, Wapiti, etc.,
Popular security testing tools available in the market, are as follows:

i. SonarQube
ii. ZAP
iii. Netsparker
iv. Arachni
v. IronWASP

Self-Assessment Exercise(s)

What is security testing? Give an example What are the three types of security test? Why is security testing used?

3.4 Summary

At the of this unit, you have learnt the meaning of security testing, the goal and key areas of security testing and its various categories.

You have learnt from this unit that security testing is important aspect of cybersecurity that helps and guides against attacks. Therefore, it is quite necessary to understand the basic ways to perform security testing.

3.5 Reference/ Further Readings/Web Resources

Rajkumar S. M (2024). Security Testing Tutorial | Software Testing Material. Retrieved from https://www.softwaretestingmaterial.com/security-testing-tutorial

Reddy G. C (2021). Introduction to Security Testing. Retrieved from https://www.gcreddy.com/2021/09/introduction-to-security-testing.html

Jason Chavarría (2023). Security Testing Fundamentals. Retrieved from https://fluidattacks.com/blog/security-testing-fundamentals

3 Possible Answers to Self-Assessment Exercises

What is security testing? Give an example

Answer

Security testing is vital for evaluating a system's resistance to unauthorized access and data breaches. For instance, it verifies the encryption of passwords, prevents access for invalid users, and evaluates the security of cookies and sessions

What are the three types of security test?

Answer

There are three distinct types of security assessment: security audits, vulnerability assessments, and penetration tests. Although these terms are sometimes used interchangeably and they represent different approaches to evaluating security

Why is security testing used?

Answer

Security testing serves the purpose of identifying vulnerabilities in an information system's security measures, thereby ensuring data protection and the system's intended functionality.

Unit 4 Incident Response

Unit Structure

4.1 Introduction

An effective cyber incident response plan might be the difference between your organisations suffering a slight disruption following a data breach and it collapsing into financial ruin. Security incidents are increasing in size and sophistication each year, with organisations across all sectors coming under attack. Many have failed to control the damage in time and faced insurmountable costs addressing compromised data, customer loss and regulatory penalties. But with a cyber incident response plan, you have a blueprint for a swift and effective response.

4.2 Learning Outcomes

By the end of this unit, you should be able to:

- explain cybersecurity incident response.
- understand the important of incident response
- describe types of cybersecurity incidents response
- state the lifecycle of an incident response tools and technology.

4.3 Incident Response

4.3.1 Definition of Cybersecurity Incident Response

Incident response (IR) is the process by which an organization handles a data breach or cyberattack. It is an effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents.

Incident response is a term used to describe the process by which an organization handles a data 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. Additionally, it's advisable to specify the teams, employees, or leaders responsible for both managing the overall incident response initiative and those tasked with taking each action specified in the incident response plan.

4.3.2 Importance of Incident Response Important?

Incident activity that is not properly controlled can escalate into a bigger problem, ultimately leading to data breaches, high costs, or system outages. By responding quickly to incidents, organizations can minimize losses, mitigate exploited vulnerabilities, restore services and processes, and mitigate the risk of future incidents.

Having a robust incident response plan allows businesses to swiftly detect, contain, and mitigate security breaches. This proactive approach ensures that the incident is isolated, preventing it from spreading and causing further damage.

Incident response enables organizations to do the following:

1. Prepare for the known and the unknown incidents
2. Immediately identify security incidents
3. Establish best practices to block intrusions before they cause damage

Incident response is critical to business, as most organizations' operations rely on mission critical computing systems and store sensitive information. Security incidents can have short- and long-term impacts that affect the success of the entire organization. These can include downtime and service disruption, regulatory fines, legal fees, and data recovery costs.

Beyond these direct impacts, failure to effectively respond to incidents hurts the organization's business performance. Unhandled incidents are associated with negative brand reputation and low levels of customer loyalty and satisfaction.

Although an organization cannot completely eliminate incidents, incident response can help minimize their occurrence. Organizations should focus on preparing for the impact of a security incident. Attackers will always be out there, but any organization can prepare for an attack with a functionally effective approach to incident response.

4.3.3 Types of Cybersecurity Incidents

There are many types of cybersecurity incidents that could result in intrusions on an organization's network:

Unauthorized Attempts to Access Systems or Data: Occurs when an individual or group attempts to gain unauthorized access to an organization's systems or data. Examples include hacking attempts, brute force attacks, and social engineering.

Privilege Escalation Attack: Occurs when an attacker is able to gain access to a system with limited privileges and then uses that access to gain higher-level privileges. This can be done by exploiting vulnerabilities in the system or using stolen credentials.

Insider Threat: Occurs when a current or former employee, contractor, or other insider uses their access to an organization's systems or data for malicious purposes. Examples include stealing sensitive information or sabotaging systems.

Phishing Attack: Occurs when an attacker sends an email or message that appears to be from a legitimate source, but is actually a trap to steal sensitive information or spread malware.

Malware Attack: Occurs when an attacker uses malware, such as a virus or trojan horse, to gain access to an organization's systems or data or perform other malicious activities. Different types of malwares can

perform different activities. For example, ransomware can prevent access to data until a ransom has been paid.

Denial-of-Service (DoS) Attack: Occurs when an attacker floods a system or network with traffic, causing it to become unavailable to legitimate users.

Man-in-the-Middle (MitM) Attack: Occurs when an attacker intercepts and alters communications between two parties. The attacker can steal sensitive information or spread malware this way.

Advanced Persistent Threat (APT): A sophisticated and targeted attack designed to gain access to an organization's systems or data, often with the goal of stealing sensitive information or maintaining a long-term presence.

4.3.4 Incident Response Lifecycle

The most common cyber incident response framework is National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide. It contains six phases that guide organisations through the process:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned

Although each of these stages contains complex and interrelated actions, the documented plan should provide simple and precise guidance, free from jargons. This enables stakeholders to make decisions quickly and identify a plan of action without having to sift through lengthy technical details.

1. **Preparation**
   An effective incident response plan provides guidelines for the steps an organization should take well before a disruptive incident occurs. The plan begins by outlining how an Organisation should mitigate the risk of a data breach. The preparation phase should align with the organizational policies on data protection with security goals and technological defenses. At a minimum, you must ensure that employees have received information security staff awareness training. Ideally, they should also receive specific training on incident response. Likewise, you

should perform an audit of your systems to ensure that your sensitive data is adequately protected.

2. **Identification**

The second phase of incident response planning relates to the steps an organisation takes to identify when its systems have been compromised. If you can spot an intrusion quickly, you are better equipped to thwart the attack. Even if that's not possible, you can expedite the response effort and minimize the damage, saving you time and money. When identifying a security incident, you should answer the following questions:

i. Who discovered the breach?
ii. What is the extent of the breach?
iii. Is it affecting our operations?
iv. What is the source of the compromise?

3. **Containment**

The third phase covers the steps you should take to mitigate the damage once you have been breached. Depending on the nature of the incident, this could mean taking actions to remove the criminal hacker from your systems or to isolate the already compromised data. During this phase, you should consider whether systems need to be taken offline or deleted, and whether there are immediate steps you can take to close vulnerabilities.

4. **Eradication**

Phase four of a cyber incident response plan is about rectifying the weakness that enabled the data breach to occur. The specifics will depend on how the type of incident, but during this stage, you must identify how the information was compromised and how you can eradicate the risk. If you were infected by malware, for example, you would remove the malicious software and isolate the affected parts of your organisation. Meanwhile, if the attack occurred because a criminal hacker compromised an employee's login credentials, you would freeze their account.

5. **Recovery**

Once you have eradicated the threat, you can move on to the penultimate stage of cyber incident response, which is to get your systems back online. This will be more complex in some instances than others, but it's an essential part of the process and should be treated carefully. Without a proper recovery process, you could remain vulnerable to similar attacks, which will compound the damage. As part of the recovery process, you should test and monitor the affected systems once you have

remediated the situation. This ensures that the measures you put in place work as intended, and it gives you the opportunity to correct any mistakes.

6. **Lessons learned**
   The final phase of the cyber incident response plan is to review the incident and to identify opportunities for improvement. Everyone in your incident response team should meet to evaluate parts of the plan that worked and problems that was encountered. You should assess every step of the process, discuss what happened, why it happened, what you did to curtail the situation and what could have been done differently. For example, were there any gaps in the plan, and was the documentation effective and easy to understand? This conversation should take place between one and two weeks after the security incident occurred – long enough to consider situation in hindsight but soon enough to ensure that it remains fresh in everyone's memory.

The purpose of this phase is not to call out team members for mistakes they made, but to ensure that inefficiencies do not occur in the future. If there were failures in the process, it suggests that either the documentation was not clear, appropriate actions weren't outlined or staff training was not adequate.

4.3.5 Incident Response plan

An incident response plan is a document that details the security processes to be carried out in case of an incident, and those responsible for incident response. An incident response plan typically includes the following details:

i. Incident response methods and strategies
ii. How incident response can support your organization's broader mission
iii. Activities required for each stage of incident response
iv. Roles and responsibilities for completing incident response activities
v. Communication channels between the incident response team and the rest of the organization
vi. Metrics for evaluating the efficiency of incident response
vii. The benefits of an incident response plan do not end when a cybersecurity incident is resolved. The plan continues to provide support for litigation, documentation to submit to auditors, and historical knowledge that enables a better response to similar incidents in the future.

4.3.6 Incident Response Tools and Technology

There are several types of tools that are useful for incident response:
Security Orchestration, Automation, and Response (SOAR)
SOAR refers to platforms that offer tools for collecting security data from various sources. A SOAR solution may combine machine learning and human input to analyze the data to extract insights and prioritize the relevant incident response procedures.

SOAR software typically includes three capabilities:

1. Threat and vulnerability management
2. Incident response
3. Security operations automation

Organizations use SOAR to collect and make sense of threat-related data from diverse sources, enabling automated threat responses.

User and Entity Behavior Analytics (UEBA)

UEBA solutions use large datasets and machine learning to establish baselines for typical behavioral patterns, allowing them to identify a typical behaviour within the network, which may indicate threats. The emphasis on suspicious behavior allows UEBA to detect threats that can evade traditional security and antivirus tools, including non-malware-based attacks. UEBA uses behavioural models to assess threat levels, providing risk scores to guide the response process.

Security Information and Event Management (SIEM)

SIEM is a security management approach that provides a unified system to combine information and event management functions. SIEM solutions deploy multiple data collection agents to hierarchically collect event data from servers, end-user devices, and network infrastructure. A central management console consolidates the data, allowing security analysts to filter the noise and prioritize real security incidents.

Endpoint Detection and Response (EDR)

EDR systems collect and analyze endpoint security data to protect the network from vulnerable user devices and workstations. EDR aims to detect security breaches in real time, enabling rapid response. This approach helps identify emerging and advanced threats that traditional security tools might not. The specific capabilities of each EDR solution may vary significantly.

Extended Detection and Response (XDR)

XDR solutions are SaaS tools for detecting security threats and implementing incident response procedures. XDR tools integrate several security capabilities in a unified security operations solution, making sophisticated incident response capabilities more accessible and affordable.

The advantage of XDR is its consolidation of multiple security products building on EDR capabilities. It can improve the productivity of security operations with enhanced detection and response and centralized visibility and control across enterprise environments. XDR tools ingest and distill multiple telemetry streams and analyze threat vectors and tactics. They help speed up response efforts by handling the detection and investigation processes.

Self-Assessment Exercises

1. What is the purpose of incident response?
2. What Does an Incident Response Team Do?
3. What are Some Common Causes of Incident Response Problems?

4.4 Summary

At the end of this unit, you have been familiarized with the definition, importance, recovery team, lifecycle and plan of an incident response in cybersecurity.

You have learnt from this unit, the importance of incident response and why it should not be neglected.

4.5 References/Further Readings/Web Resources

Alissa Irei (2024). What is incident response? A complete guide. Retrieved from https://www.techtarget.com/searchsecurity/definition/incident-response

BlueVoyant (2024). What is Incident Response? Process, Frameworks, and Tools. Retrieved from https://www.bluevoyant.com/knowledge-center/what-is-incident-response-process-frameworks-and-tools

Cynet (2024). What is Incident Response? Retrieved from https://www.cynet.com/incident-response

4.0 Possible Answers to Self-Assessment Exercises

What is the purpose of incident response?

Answer to SAE 1

Incident response aims to reduce the damage an attack causes and help the organization recover as quickly as possible.

What Does an Incident Response Team Do?

Answer to SAE 2

An incident response team consists of a group of IT professionals who respond to suspected security incidents. The work of the incident response team includes developing an active incident response plan, system vulnerability testing and remediation, and support for all incident management activities performed across the organization. Members of the incident response team can include Level 1, 2, and 3 security analysts, security engineers, and operations specialists.\

What are Some Common Causes of Incident Response Problems?

Answer to SAE 3

Common causes of incident response problems include:

1. Missing event context, which requires time-consuming manual investigation.
2. Lack of effective prioritization, which wastes time for security analysts.
3. Lack of communication tools, enabling analysts to easily report and escalate the incident to others.
4. Lack of opportunities for effective cooperation between security teams and operations, development, or other departments.
5. Lack of visibility of security incidents to other parts of the organization, such as senior leadership, legal teams, PR teams, customers and shareholders.

What are the five steps to achieve incident response?

Answer to SAE 4

Identify - Companies need to identify all types of threats and the assets they could affect. This involves inventorying the environment and conducting a risk assessment.

Protect - All critical assets need to have a protection plan that involves protective technological solutions and employee security awareness training.

Detect - In this step, organizations attempt to detect threats promptly before they have a chance to cause extensive damage to the environment.

Respond - After a threat or incident is detected, a defined response should be put into action to mitigate its damage and prevent its spread to other infrastructure components.

Recover - The recovery step returns the system affected to normal operations. It also evaluates the source of the incident with the goal of identifying improved security measures to prevent its recurrence.

MODULE 3 RISK MANAGEMENT AND DISASTER RECOVERY

Introduction

We all carry out informal risk management numerous times in the course of a day without even realizing it. Every time we cross a street, we stop to weigh the risk of rushing in front of oncoming traffic, waiting for the light to change, using the crosswalk, etc. Our ability to analyze the consequences of each decision is risk assessment. What we decide to do after performing that quick analysis is risk mitigation based on proper early training and our experience of crossing a road. We may decide to wait for the traffic light and use the cross walk which greatly reduces the potential risk, we may follow someone else across the street allowing them to make the decision for us, or we may simply choose not to cross the street. These decisions are as a result of risk assessment of the situation. If you make it across the street, you remember what worked. If anything went wrong such as a honked horn or brakes squealing, you should evaluate if another choice would have been better. Therefore, in this module, you will be introduced to the cybersecurity risk management and disaster recovery to avert future occurrences.

Unit 1 Risk Management
Unit 2 Disaster Recovery
Unit 3 Access Control

In each unit, a particular topic was explored in detail and self-assessment exercises were highlighted at the end of each unit. Finally, resources for further readings are highlighted at the end of each unit.

Unit 1 Risk Management

Unit structure

1.1 Introduction

Risk Management is simply to look at what could go wrong and then decide on ways to prevent or minimize these potential problems. It encompasses three processes – risk assessment, risk mitigation and evaluation.

1.2 Learning Outcomes

By the end of this unit, you will be able to:

- define risk management.
- understand the important of risk management in cyber security
- state the objectives of risk management
- mention some common examples of IT and cyber security risks and threats.

1.3 Risk Management

1.3.1 Definition of Risk Management

Cybersecurity risk management involves a structured approach to recogniseing, evaluating, and addressing potential threats to an organisation's information assets. That is, risk management is a set of techniques, decisions and actions for risks that may affect an organisations or its objectives.

Organisations can effectively safeguard their digital infrastructure, data, and operations from malicious actors by analyzing potential threats and vulnerabilities. This proactive approach enables businesses to anticipate and counteract cyber threats before they manifest into damaging incidents. By implementing robust cybersecurity risk management practices, organisations can minimize the likelihood and impact of cyberattacks, ensuring their sensitive information and systems' confidentiality, integrity, and availability.

Cybersecurity risk management functions as a crucial barrier against the ever-changing array of cyber dangers, enabling organisations to maneuver through the complexities of the digital domain with resilience and confidence.

1.3.2 Importance of Risk Management to Cybersecurity

Risk management plays a pivotal role in cybersecurity by enabling organisations to effectively identify and prioritize potential cyber risks.

In today's digital landscape, where cyber threats constantly evolve and multiply, understanding and managing these risks is vital to maintaining the security and resilience of information assets. By systematically assessing and categorizing risks, organisations can efficiently allocate resources in order to address the most significant threats first, mitigating potential damage and minimizing disruptions to operations.

Furthermore, risk management ensures the confidentiality, integrity, and availability of information assets, safeguarding sensitive data from unauthorized access, tampering, or loss. Ultimately, by integrating robust risk management practices into their cybersecurity strategy, organisations can confidently navigate the complexities of the digital world and fortify their defenses against emerging threats.

3.3 Components of Risk Management

Understanding the components of cyber risks is fundamental to effective cyber risk management. These components include:

i. **Threats**: These can arise from various sources, such as hostile attacks, human errors, and natural disasters, each with the potential to exploit vulnerabilities.
ii. **Vulnerabilities**: These are weaknesses that can be found across information systems, security procedures, and even within supply chains or vendor relationships, making systems susceptible to attacks.
iii. **Consequences**: The adverse outcomes resulting from threats exploiting vulnerabilities, which often lead to the loss or destruction of information.

To quantify cybersecurity risk, businesses often rely on the formula:

Risk = Attack's Impact x Attack's Likelihood

This calculation underscores the importance of both understanding the potential impact of an attack and its likelihood, thereby facilitating a more nuanced approach to cyber risk management.

Cyber risks are not static; they evolve continuously, necessitating an equally dynamic cyber risk management program. This program should

address risks from both external sources, like malware or third-party vendors with inadequate security measures, and internal sources, including employee sabotage or weak security practices. The ultimate goal of cyber risk management is not just to identify existing risks but to understand their potential impact comprehensively and develop strategies to mitigate or manage those risks effectively.

1.3.4 Cybersecurity Risk Management Process

Although specific methodologies vary, a risk management programme typically follows these steps:

1. Identify the risks that might compromise your cyber security. This usually involves identifying cyber security vulnerabilities in your system and the threats that might exploit them.
2. Analyse the severity of each risk by assessing how likely it is to occur and how significant the impact might be if it does.
3. Evaluate how each risk fits within your risk appetite (your predetermined level of acceptable risk).
4. Prioritize the risks.
5. Decide how to respond to each risk. There are generally four options:

i. Treat – modify the risk's likelihood and/or impact typically by implementing security controls.
ii. Tolerate – make an active decision to retain the risk (e.g., it falls within the established risk acceptance criteria).
iii. Terminate – avoid the risk entirely by ending or completely changing the activity causing the risk.
iv. Transfer – share the risk with another party, usually by outsourcing or taking out insurance.

Since cyber risk management is a continual process, monitor your risks to ensure they are still acceptable, review your controls to ensure they are still fit for purpose, and make changes as required. Remember that your risks continually change as the cyber threat landscape evolves, and your systems and activities change.

Cybersecurity Risk Management Process

In cybersecurity, managing risks is a structured process crucial for protecting organisations against potential threats. This process typically involves four key steps: risk identification, risk assessment, mitigation, and monitoring. The following paragraphs will explore each of these steps in detail, highlighting their significance in fortifying an organisation's cybersecurity posture.

Risk Identification

A foundational step in the cybersecurity risk management process, risk identification involves a systematic identification of potential cyber risks that could threaten an organisation's information assets. This process entails identifying various elements, including threats, which are potential events or circumstances that can cause harm to the organisation's assets; vulnerabilities, which are weaknesses or flaws in the organisation's systems that could be exploited by threats; and the potential impact, which refers to the consequences that could result from the exploitation of vulnerabilities by threats.

Through comprehensive risk identification, organisations can gain a clear understanding of the cyber risks they face, allowing them to prioritize and address these risks effectively in subsequent stages of the risk management process.

Risk Assessment

Risk assessment is a critical phase in cybersecurity risk management, focusing on evaluating the likelihood and impact of identified risks to an organisation's information assets. During this process, organisations analyze the probability of each identified risk materializing and the potential severity of its impact if it were to occur. Organisations can systematically gauge the likelihood of threats exploiting vulnerabilities and the possible consequences of such incidents by employing various methodologies, such as qualitative and quantitative risk assessment techniques. This evaluation provides valuable insights into the relative significance of different risks, enabling organisations to prioritize their efforts in mitigating risk according to the level of threat it poses to their operations, data, and systems. Through thorough risk assessment, organisations can make informed decisions about allocating resources and implementing controls to effectively manage and mitigate cyber risks.

Risk Mitigation

Risk mitigation encompasses a range of strategies to reduce the impact or likelihood of identified cyber risks on an organisation's information assets. Among these approaches are strategies such as risk avoidance, where organisations take actions to eradicate or lessen their exposure to specific risks; risk transfer, which entails shifting risk to third parties through insurance or contracts; risk mitigation, where controls and safeguards are established to decrease the probability or severity of recogniseed risks; and risk acceptance, where organisations recognisee certain risks as inevitable or manageable and opt to tolerate them without additional intervention.

By employing these strategies tailored to their specific risk profile and organisational objectives, businesses can effectively improve their resilience to cyber threats and safeguard their critical assets.

Risk Monitoring

Risk monitoring is a vital component of cybersecurity risk management, emphasizing the continuous observation and evaluation of the organisation's digital environment to identify emerging risks and evaluate the efficacy of existing risk mitigation strategies. By maintaining ongoing vigilance, organisations can stay abreast of emerging cyber threats, evolving vulnerabilities, and changes in their operational landscape that may impact their risk profile. Regular monitoring allows timely detection of potential risks, enabling proactive interventions to prevent or mitigate their impact before they escalate into significant incidents. Furthermore, monitoring facilitates the evaluation of the effectiveness of implemented risk mitigation measures, providing valuable feedback for refining strategies and adapting to evolving cyber threats.

Through diligent risk monitoring, organisations can maintain a robust cybersecurity posture and effectively safeguard their information assets in an ever-changing threat landscape.

1.3.5 Risk Management Standards and Frameworks

The government has added many compliance rules for the companies in the past two decades. Cybersecurity risk management standards and frameworks, such as the NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Controls, serve as invaluable guidelines for organisations seeking to implement effective cybersecurity risk management practices. These standards offer comprehensive

frameworks that outline best practices, processes, and controls for identifying, assessing, and mitigating cyber risks. These are the widely recogniseed frameworks for risk management:

1. **COSO ERM Framework**
   This framework was launched in 2004. It highlights the importance of embedding risk considerations into business strategies. It offers precise guidelines for risk management, identifies important Enterprise Risk Management (ERM) ideas and principles and establishes a standard vocabulary for ERM. The main components of this framework, developed by consulting firm are governance and culture; strategy and objective setting; performance; review and revision; information, communication and reporting.
2. **ISO 31000**
   This framework helps organisations apply risk management mechanisms to operations and the processes of identifying, evaluating and mitigating risks. This is a shorter document than other frameworks and provides more strategic guidance on ERM. It highlights how important senior management is to risk programs and how risk management procedures should be integrated across the entire company.
3. **BS 31100**
   This British Standard risk management code of practice provides a process for implementing concepts of identifying, assessing and responding to risks and then reporting on and reviewing risk management activities.
4. **NIST's Risk Management Framework**
   This framework provides a detailed process for integrating security, data privacy and cybersecurity management initiatives into the system development cycle.

Self-Assessment Exercises

1. What does a cyber risk manager do?
2. What are the three types of risk in cyber security?
3. What is the difference between managing risk and managing vulnerability?

1.4 Summary

At the end of this unit, you have learnt the cybersecurity risk management system as well as the various frameworks and standards. In the next unit, you will expose to ways to recover disaster if occur.

You have learnt from this unit, the importance of risk management to cybersecurity and why it needs to be studied.

1.5 References/Further Readings/Web Resources

Andrew Stephen (2023). Cyber Security Risk Management. Retrieved from https://www.udemy.com/course/cyber-security-risk-management

Anne Gomez (2024). What is Risk Management in Cyber Security: An In-Depth Guide. Retrieved from https://www.ollusa.edu/blog/what-is-risk-management-in-cyber-security.html

Jamie Cowper (2024). Cyber Risk Management: A Beginner's Guide

What are the Objectives of Risk Management? Retrieved from https://in.indeed.com/hire/c/info/objectives-risk-management

1.6 Possible Answers to Self-Assessment Exercise(s)

What does a cyber risk manager do?

Answer

A cyber risk manager identifies, assesses, and mitigates cyber risks to protect an organisation's information assets and systems.

What are the three types of risk in cyber security?

Answer

The three types of risk in cybersecurity are strategic risk, operational risk, and reputational risk.

What is the difference between managing risk and managing vulnerability?

Answer

Managing risk involves identifying, assessing, and mitigating potential threats and vulnerabilities while managing vulnerability focuses specifically on addressing weaknesses or flaws in systems or processes.

Unit 2 Disaster Recovery

Unit Structure

2.1 Introduction

Disaster recovery is generally a planning process and it produces a document which ensures businesses to solve critical events that affect their activities. Such events can be a natural disaster (earthquakes, flood, etc.), cyber–attack or hardware failure like servers or routers.

As such having a document in place will reduce the down time of business process from the technology and infrastructure side. This document is generally combined with Business Continuity Plan which makes the analyses of all the processes and prioritizes them according to the importance of the businesses. In case of a massive disruption, it shows which process should be recovered firstly and what should be the downtime. It also minimizes the application service interruption. It helps us to recover data in the organized process and help the staff to have a clear view about what should be done in case of a disaster.

2.2 Learning Outcomes

By the end of this unit, you will be able to:

- define disaster recovery.
- understand disaster recovery plan and how it works.
- state the essential elements of a disaster recovery plan
- understand how to develop and implement a disaster recovery plan

- state the key steps in a disaster recovery plan

2.3 Disaster Recovery

2.3.1 Definition of Disaster Recovery

Disaster recovery is the practice of anticipating, planning, surviving, and recovering from a disaster that may affect a business. Disasters can include:

- Natural events like earthquakes or hurricanes
- Failure of equipment or infrastructure, such as a power outage or hard disk failure
- Man-made calamities such as accidental erasure of data or loss of equipment
- Cyber-attacks by hackers or malicious insiders

2.3.2 Disaster Recovery plan

A disaster recovery plan is an organisation's strategic documentation and process to restore access to compromised systems and infrastructure after a cyber-attack, human error, natural disaster, or other catastrophic events. It is the systematic methodology by which a team allocates its resources to efficiently regain control over critical data and information systems following a disaster.

A disaster recovery plan enables businesses to respond quickly to a disaster and take immediate action to reduce damage, and resume operations as quickly as possible. A disaster recovery plan typically includes:

i. Emergency procedures staff can carry out recovery when a disaster occurs
ii. Critical IT assets and their maximum allowed outage time
iii. Tools or technologies that should be used for recovery
iv. A disaster recovery team**,** their contact information and communication procedures (e.g. who should be notified in case of a disaster)

Why is Disaster Recovery Important?

Drafting a disaster recovery plan, and ensuring you have the right staff in place to carry it out, can have the following benefits:

Minimize interruption: in the event of a disaster, even if it is completely unexpected, your business can continue operating with minimal interruption.

Limit damages: a disaster will inevitably cause damage, but you can control the extent of damage caused. For example, in hurricane-prone areas, businesses plan to move all sensitive equipment off the floor and into a room with no windows.

Training and preparation: having a disaster recovery program in place means your staff are trained to react in case of a disaster. This preparation will lower stress levels and give your team a clear plan of action when an event occurs.

Restoration of services: having a solid disaster recovery plan means you can restore all mission critical services to their normal state in a short period of time. Your Recovery Time Objective (RTO) will determine the longest time you are willing to wait until service is restored.

2.3.3 Essential Elements of Disaster Recovery Plan

A disaster recovery plan should include the following elements:

1. **Risk analysis**
   It identifies potential hazards and risks of disruptive events to an organisation's IT systems. It also evaluates the likelihood and severity of each risk and the possible impact on the business.
2. **Business Impact Analysis**
   A business impact analysis (BIA) is then conducted to determine the potential consequences of a disruption to critical systems, applications, and data. This analysis helps prioritize recovery efforts and allocate resources accordingly.
3. **Recovery Objectives and Strategies**
   Recovery objectives are crucial in guiding the disaster recovery process. The two primary objectives are the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). RTO refers to the maximum amount of time an organisation can afford to be without its critical systems before facing significant consequences. RPO defines the acceptable amount of data loss that can be tolerated in case of a disaster. Based on these objectives, appropriate recovery strategies should be developed to meet the organisational needs.
4. **Disaster Recovery Team and Roles**
   A dedicated disaster recovery team should be established, consisting of members from various departments with clear roles

and responsibilities. This team should include IT personnel, management representatives, and other key stakeholders. Clearly defined roles ensure a coordinated and efficient response during a disaster.

5. **Emergency Response Procedures**
   Emergency response procedures outline the specific steps to be followed during a disaster to minimise downtime and ensure a quick recovery. These procedures should include details about initiating the disaster recovery plan, communication protocols, and escalation processes, as well as steps to restore critical systems and applications. Regular updates and reviews of these procedures are necessary to keep them current and effective.
6. **Recovery Strategies and Technologies**
   Various recovery strategies and technologies are available to help organisations restore their IT systems and data in the event of a disaster. These options should be carefully evaluated based on the organisation's specific needs, recovery objectives, and available resources.
7. **Data Backup and Storage Solutions**
   Regular data backups are crucial for ensuring the availability of essential information during a disaster. Organisations can choose from different backup methods, such as full, incremental, or differential backups, depending on their requirements. Backup data should be stored offsite, ideally in a geographically separate location, to protect against localised disasters. Additionally, implementing encryption and access controls can help secure backup data from unauthorised access.
8. **Failover and Redundancy Systems**
   Failover systems and redundancy help maintain the availability of critical systems during a disaster. By creating duplicate instances of essential applications and hardware, organisations can quickly switch to backup systems if the primary systems fail. This approach can include load balancing, clustering, or mirroring technologies to ensure minimal downtime and data loss.
9. **Cloud-based Disaster Recovery**
   Cloud-based disaster recovery solutions have become increasingly popular due to their flexibility, scalability, and cost-effectiveness. By leveraging the resources of cloud service providers, organisations can quickly restore their IT systems and data in the event of a disaster. Cloud-based solutions also enable the use of virtualized environments, allowing for rapid deployment and easier management of recovery processes. However, it's essential to carefully assess the security and compliance measures of a cloud provider to ensure the protection of sensitive data.

By adopting a combination of these recovery strategies and technologies, organisations can develop a robust disaster recovery plan tailored to their specific needs and risk profile. Regular evaluation and updating of these strategies are necessary to adapt to the evolving technological landscape and emerging threats.

2.3.4 Types of Disaster Recovery

Depending on the industry, criticality, IT infrastructure, and size of the organisations, different types of disaster recovery methods are suitable for them. Businesses can choose from a variety of disaster recovery methods, or combine several:

Back-up: This is the simplest type of disaster recovery which entails storing data off site or on a removable drive. However, just backing up data provides only minimal business continuity help, as the IT infrastructure itself is not backed up, but it does not provide fast recovery or protection against hardware failure or network disruption.

Cold Site: In this type of disaster recovery, an organisation sets up a basic infrastructure in a second, rarely used facility that provides a place for employees to work after a natural disaster or fire. It can help with business continuity because business operations can continue, but it does not provide a way to protect or recover important data, so a cold site must be combined with other methods of disaster recovery.

Hot Site: A hot site maintains up-to-date copies of data at all times. Hot sites are time-consuming to set up and more expensive than cold sites, but they dramatically reduce down time.

Disaster Recovery as a Service (DRaaS): In the event of a disaster or ransomware attack, a DRaaS provider moves an organisation's computer processing to its own cloud infrastructure, allowing a business to continue operations seamlessly from the vendor's location, even if an organisation's servers are down. DRaaS plans are available through either subscription or pay-per-use models. There are pros and cons to choosing a local DRaaS provider: latency will be lower after transferring to DRaaS servers that are closer to an organisation's location, but in the event of a widespread natural disaster, a DRaaS that is nearby may be affected by the same disaster.

Back Up as a Service: Similar to backing up data at a remote location, with Back Up as a Service, a third-party provider backs up an organisation's data, but not its IT infrastructure.

Datacenter disaster recovery: The physical elements of a data center can protect data and contribute to faster disaster recovery in certain types of disasters. For instance, fire suppression tools will help data and computer equipment survive a fire. A backup power source will help businesses sail through power outages without grinding operations to a halt. Of course, none of these physical disaster recovery tools will help in the event of a cyber-attack.

Virtualization: Organisations can back up certain operations and data or even a working replica of an organisation's entire computing environment on off-site virtual machines that are unaffected by physical disasters. Using virtualization as part of a disaster recovery plan also allows businesses to automate some disaster recovery processes, bringing everything back online faster. For virtualization to be an effective disaster recovery tool, frequent transfer of data and workloads is essential, as is good communication within the IT team about how many virtual machines are operating within an organisation.

Point-in-time copies: Point-in-time copies, also known as point-in-time snapshots, make a copy of the entire database at a given time. Data can be restored from this back-up, but only if the copy is stored off site or on a virtual machine that is unaffected by the disaster.

Instant recovery: Instant recovery is similar to point-in-time copies, except that instead of copying a database, instant recovery takes a snapshot of an entire virtual machine.

2.3.5 Benefits of Disaster Recovery Software

No organisation can afford to ignore disaster recovery. The two most important benefits of having a disaster plan in place, including effective Disaster Recovery (DR) software, are:
Cost savings: Planning for potential disruptive events can save businesses hundreds of thousands of dollars and even mean the difference between a company surviving a natural disaster or folding.
Faster recovery: Depending on the disaster recovery strategy and the types of disaster recovery tools used, businesses can get up and running much faster after a disaster, or even continue operations as if nothing had happened.

Self-Assessment Exercises

Why is disaster recovery plan important? Mention some essential elements of a disaster recovery plan.

2.4 Summary

At the end of this unit, you have learnt the importance of disaster recovery in every organisation, its types and recovery process. In the next unit, you will be introduced to access control.
You have learnt from this unit that every organisation requires disaster recovery to be able to restore compromised system if need arise. Hence, it is important for all organisation to have knowledge of disaster recovery and learn the process.

2.5 Reference/Further Readings/Web Resources

CloudShape (2024) what is disaster recovery in cyber security? Retrieved from https://medium.com/@cloudshape95/what-is-disaster-recovery-in-cyber-security

Joe Aucott (2023). What is a Disaster Recovery Plan and How to Create One. Retrieved from https://www.haptic-networks.com/cyber-security/disaster-recovery-plan

Proofpoint (2024). What is Disaster Recovery? Retrieved from https://www.proofpoint.com/us/threat-reference/disaster-recovery

Risk Optics (2021). Steps to Creating a Cybersecurity Disaster Recovery Plan. Retrieved from https://reciprocity.com/blog/steps-to-creating-a-cybersecurity-disaster-recovery-plan

2.6 Possible Answers to Self-Assessment Exercises

Why is disaster recovery plan important?

Answer to SAE 1

Drafting a disaster recovery plan, and ensuring you have the right staff in place to carry it out, can have the following benefits:

i. **Minimize interruption** – in the event of a disaster, even if it is completely unexpected, your business can continue operating with minimal interruption.
ii. **Limit damages** – a disaster will inevitably cause damage, but you can control the extent of damage caused. For example, in hurricane-prone areas, businesses plan to move all sensitive equipment off the floor and into a room with no windows.
iii. **Training and preparation** – having a disaster recovery program in place means your staff are trained to react in case of a disaster. This preparation will lower stress levels and give your team a clear plan of action when an event occurs.
iv. **Restoration of services** – having a solid disaster recovery plan means you can restore all mission critical services to their normal state in a short period of time. Your Recovery Time Objective (RTO) will determine the longest time you are willing to wait until service is restored

Mention some essential elements of a disaster recovery plan

Answer to SAE 2

A disaster recovery plan should include the following elements: **risk analysis**, **business impact analysis,** recovery objectives and strategies, disaster recovery team and roles, emergency response procedures, recovery strategies and technologies, data backup and storage solutions, failover and redundancy systems, cloud-based disaster recovery

Unit 3 Access Control

Unit Structure

3.1 Introduction

Access control is the traditional center of gravity of computer security. It is where security engineering meets computer science. Its function is to control which principals (persons, processes, machines) have access to which resources in the system—which files they can read, which programs they can execute, how they share data with other principals, and so on.

Access control is a security strategy that controls who or what can view or utilize resources in a computer system. It is a fundamental security concept that reduces risk to the company or organisation.

3.2 Learning Outcomes

By the end of this unit, you will be able to:

- define access control.
- understand the components of access control.
- understand how access control work.
- describe types of computer access control
- state the challenges of access control

3.3 Access Control

3.3.1 Definition of Access Control

Access control is a fundamental security principle that limits access to resources to those authorized for their use. Effective access control greatly reduces risk to an organisation. It can help protect personnel or physical devices from damage by hostile attackers, and prevent intrusion from unauthorized or malicious entities. It can also prevent the theft of physical goods or data. Lastly, it often includes a record-keeping or logging component that can leave documentation of access. This can help in security audits, compliance, and investigations.

Access control is one of the ways that security professionals implement the principle of least privilege, the principle of least privilege states that an entity should always have access to the resources needed to perform their organisation function, and no more.

Access control is most often thought of in terms of persons or users. However, it is important to remember that these same principles can be applied to the authorization of computer systems, applications, database queries, automated systems, etc.

Access Control is a method of limiting access to a system or resources. Access control refers to the process of determining who has access to what resources within a network and under what conditions. It is a fundamental concept in security that reduces risk to the business or organisation. Access control systems perform identification, authentication, and authorization of users and entities by evaluating required login credentials that may include passwords, pins, bio-metric scans, or other authentication factors. Multi-factor authentication requires two or more authentication factors, which is often an important part of the layered defense to protect access control systems.

Authentication Factors

- Password or PIN
- Bio-metric measurement (fingerprint & retina scan)
- Card or Key
- For computer security, access control includes the authorization, authentication, and audit of the entity trying to gain access.
- Access control models have a subject and an object.

3.3.2 Components of Access Control

Access control is managed through several components:

1. **Authentication**
   Authentication is the process of verifying the identity of a user. User authentication is the process of verifying the identity of a user when that user logs in to a computer system. 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 organisations' data.
2. **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.
3. **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.
4. **Manage**
   Organisations 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.
5. **Audit**
   Organisations 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.

3.3.3 Categories of Computer Access Controls

Categories of access controls are as stated below;

1. **Attribute-based Access Control (ABAC):** In this model, access is granted or declined by evaluating a set of rules,

policies, and relationships using the attributes of users, systems and environmental conditions.

2. **Discretionary Access Control (DAC):** In DAC, the owner of data determines who can access specific resources.
3. **History-Based Access Control (HBAC):** Access is granted or declined by evaluating the history of activities of the inquiring party that includes behaviour, the time between requests and content of requests.
4. **Identity-Based Access Control (IBAC):** By using this model network administrators can more effectively manage activity and access based on individual requirements.
5. **Mandatory Access Control (MAC):** A control model in which access rights are regulated by a central authority based on multiple levels of security. Security Enhanced Linux is implemented using MAC on the Linux operating system.
6. **Organisation-Based Access control (OrBAC):** This model allows the policy designer to define a security policy independently of the implementation.
7. **Role-Based Access Control (RBAC):** RBAC allows access based on the job title. RBAC eliminates discretion on a large scale when providing access to objects. For example, there should not be permissions for human resources specialist to create network accounts.
8. **Rule-Based Access Control (RAC):** RAC method is largely context based. Example of this would be only allowing students to use the labs during a certain time of day.

Different access control models are used depending on the compliance requirements and the security levels of information technology that is to be protected. Basically, access control is of 2 types:
Physical Access Control: Physical access control restricts entry to campuses, buildings, rooms and physical IT assets.
Logical Access Control: Logical access control limits connections to computer networks, system files and data.

3.3.4 Challenges of Access Control

i. **Distributed IT Systems:** Current IT systems frequently combine internet and on-premise networks. These systems may be distributed geographically and comprise various devices, assets, and virtual machines. Access is allowed to all of these devices, and keeping track of them can be challenging.
ii. **Policy Management:** Policy makers within the organisation create policies, and the IT department converts the planned policies into code for implementation. Coordination between

these two groups is essential for keeping the access control system up to date and functioning properly.

iii. **Monitoring and Reporting:** Organisations must constantly check access control systems to guarantee compliance with corporate policies and regulatory laws. Any violations or changes must be recogniseed and reported immediately.

iv. **Access Control Models:** Access control mechanisms provide varying levels of precision. Choosing the right access control strategy for your organisation allows you to balance acceptable security with employee efficiency.

Types of Authentication Mechanism

i. Two-factor authentication
ii. Multi-factor authentication
iii. one-time password
iv. Three-factor authentication
v. Biometrics
vi. Hard Tokens
vii. Soft Tokens
viii. Contextual Authentication
ix. Device identification

3.3.5 How to Implement Access Control Security

One of the most common methods for implementing access controls is to use Virtual Private Networks (VPNs). This enables users to securely access resources remotely, which is crucial when people work away from the physical office. Companies can use VPNs to provide secure access to their networks when employees are based in various locations around the world. While this is ideal for security reasons, it can result in some performance issues, such as latency. Other access control methods include identity repositories, monitoring and reporting applications, password management tools, provisioning tools, and security policy enforcement services.

Self-Assessment Exercise(s)

State an example of an access control?
What is the role of access control lists (ACLs) in network security?

3.4 Summary

At the end of the unit, you have learnt the definition of access control, its importance, categories and categories encountered while enforcing access control.

You have learnt from this unit, that access control is a fundamental security principle that limits access to resources to those authorized for their use as a means of protecting our data. Therefore, it is important to understand the how of enforcing access control.

3.5 References/Further Readings/Web Resources

Access Control in Computer Network (2024). Retrieved from https://www.fortinet.com/resources/cyberglossary/access-control

https://www.geeksforgeeks.org/access-control-in-computer-network
What Is Access Control? (2023). Retrieved from

3.6 Self-Assessment Exercise(s)

State an example of an access control?

Answer to SAE 1

An example of access control might be an airplane flight check-in. Each customer is expected to present a ticket, and their name is checked against a flight manifest. Any person without a ticket or whose name does not appear on the manifest is denied access to the flight.

What is the role of access control lists (ACLs) in network security?

Answer to SAE 2

Access control list is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

Module 4 Cryptography and Secure Communication

Introduction

There is need to safe guide our data, that is more reason why cryptography is important in cybersecurity. Let look at a story that we help you understand cryptography. A student wanted to buy a new Android phone and went browsing for a discount, he later got one. Moments after he submitted his card details, a huge amount of money was withdrawn from his account.

Where did he go wrong?

The website used was not secure enough to conduct bank transactions... There is http:// and https://

HTTP websites are not secured and the data is visible to everyone trying to look for it while

HTTPS websites are much more secured and the bank transactions are encrypted (not easy to steal).

Unit 1 Basic Cryptography and Methodologies
Unit 2 Steganography

In each unit, related topics are well explored in detail and self-assessment exercise are as well highlighted at the end of each unit. Finally, resources for further reading were captured at the end of each unit.

Unit 1 Basic Cryptography and Methodologies

Unit Structure

1.1 Introduction
1.2 Learning Outcomes
1.3 Basic Cryptography and Methodologies
  1.3.1 Definition of Cryptography
  1.3.2 Plain Text and Cipher-text
  1.3.3 Encryption and Decryption Applications
  1.3.4 Importance of Cryptography
  1.3.5 Applications of Cryptography
  1.3.6 Categories of Cryptography
  1.3.7 Cryptographic Attack
1.4 Summary
1.5 References/Further Readings/Web Resources

1.6 Possible Answers to Self-Assessment Exercises

1.0 Introduction

Cryptography is used to protect digital data. It is a division of computer science that focuses on transforming data into formats that cannot be recognized by unauthorised users. An example of basic cryptography is an encrypted message in which letters are replaced with other characters.

2.0 Learning Outcomes

By the end of this unit, you will be able to:

- define cryptography.
- understand how cryptography work.
- understand word “Plain Text and Cipher-text”
- state the important of cryptography.
- mention the applications area of cryptography.

1.3 Basic Cryptography and Methodologies

1.3.1 Definition of Cryptography

Cryptography is the science of encrypting and decrypting information to prevent unauthorised access. Both the sender and the receiver should know the decryption process.

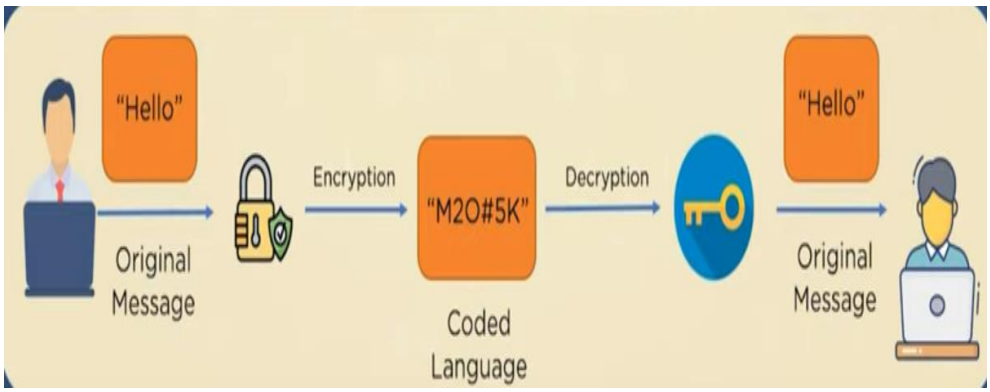


Figure 1.1: Operation of Cryptography

Cryptography uses keys, which are strings of characters that alter data to make it seem random in an encryption algorithm. Similar to its physical counterpart, a key in cryptography locks or encrypts data so that it can only be decrypted by someone who has the proper key. The cryptography process ensures the following:

- **Confidentiality**: Encrypted messages are protected from unauthorised access through cryptography. Even if a cybercriminal intercepts it, without the proper key, the information remains secure.
- **Integrity**: Cryptography maintains the integrity of data by detecting any alterations or tampering. If the data is changed in transit, the decryption process will fail, alerting the recipient of potential foul play.
- **Authentication**: By using digital signatures and certificates, cryptography confirms the identity of the sender or the integrity of a message. This is crucial in the digital world, where trust is built on verifying the source of information. One common method of authentication is the Diffie-Hellman key exchange. This method allows two parties to create a shared secret key over an insecure channel. Public values are generated from private keys using a public prime and a base. Each party calculates an independent secret key based on these public values, which makes it possible to communicate securely.
- **Non-repudiation**: non-repudiation ensures that a sender cannot deny sending a message, and a recipient cannot deny receiving it. Digital signatures play a pivotal role in achieving non-repudiation.

Despite its wide use today, cryptography is not a new practice. In ancient Egypt, Mesopotamia, Greece, and Rome, evidence of cryptography can be found. For example, the Caesar Cipher was a simple encryption technique used by Julius Caesar to share secret messages to his allies. During World War II, the Enigma machine was used to encrypt communications. When the Enigma code was broken, the Allies were able to read German messages and learn about their plans. Modern cryptography blends age-old techniques and innovative approaches to create robust systems for securing data and messages.

1.3.2 Plain Text and Cipher-text

Plain Text and Cipher-text

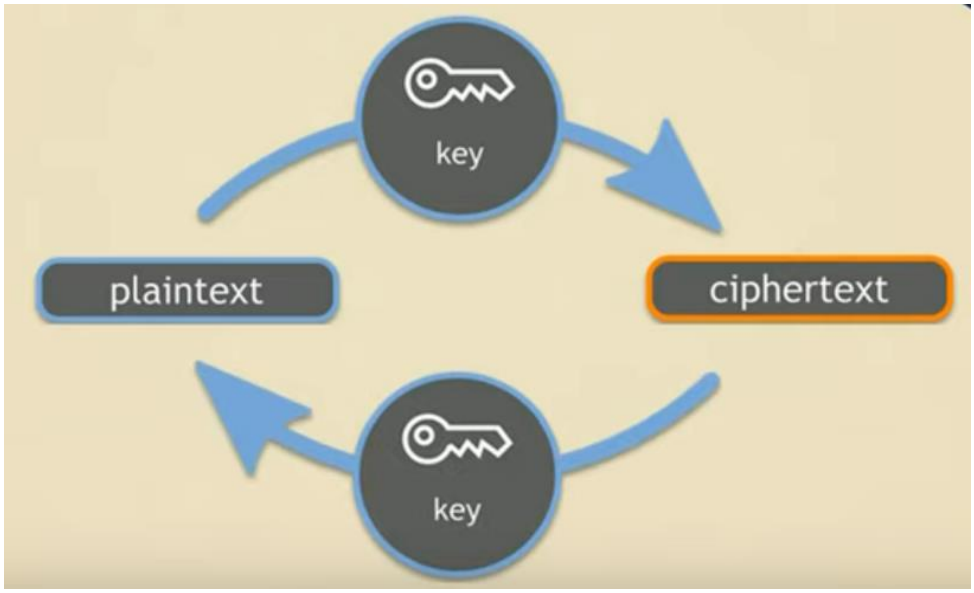


Figure 1.2: Transition of Plaintext and Ciphertext

Plain Text:

Plain text refers to any readable information presented in a format that is accessible and usable without the need for a decryption key or specific decryption tools, encompassing even binary files.

Every communication, document, or file intended to be encrypted or previously encrypted would be categorized as plain text. A cryptographic system takes plain text as input and generates ciphertext as output. Within cryptography, algorithms facilitate the conversion of ciphertext back into plain text and vice versa. The terms “encryption” and “decryption” denote these respective processes. This mechanism ensures that data can only be comprehended by its intended recipient.

Safeguarding plain text stored within computer files is of utmost importance, as unauthorised theft, disclosure, or transmission can expose its contents entirely, potentially leading to actions based on that information. To this end, the storage medium, the device itself, its components, and any associated backups must all be secured if preservation is necessary.

Cipher-text:

Cipher is a frequently used algorithm in cryptology, a subject concerned with the study of cryptographic algorithms. It is a method of encrypting and decrypting data.

When data cannot be understood by individuals or devices lacking the appropriate cypher, it is considered encrypted. To interpret the data, the

cypher is necessary. Algorithms transform plaintext into ciphertext, and vice versa, to convert ciphertext back into plaintext. These processes are known as encryption and decryption.

Cipher-text, represents a cryptographic approach in which an algorithm utilizes substitutions instead of original plaintext elements. Substitution ciphers replace individual letters, letter pairs, letter triplets, or various combinations of these while preserving the initial sequence. Single-letter substitutions are utilized in simple substitution cyphers, while polygraphed cyphers involve larger letter groupings.

In simpler terms, letters are substituted for other letters. In the past, recording corresponding characters to decipher a message was feasible.

Example of Cipher-text
Here is some simple cipher-text encrypted using the Caesar cipher, Julius Caesar's original method which uses letters only:

JV PBZOBQ QBUQ

to encrypt the original message into the ciphertext above, each letter of the text was shifted three letters back in the alphabet.

"A" shifts three letters back and becomes "X"
"B" becomes "Y"
"C" becomes "Z" and so on.

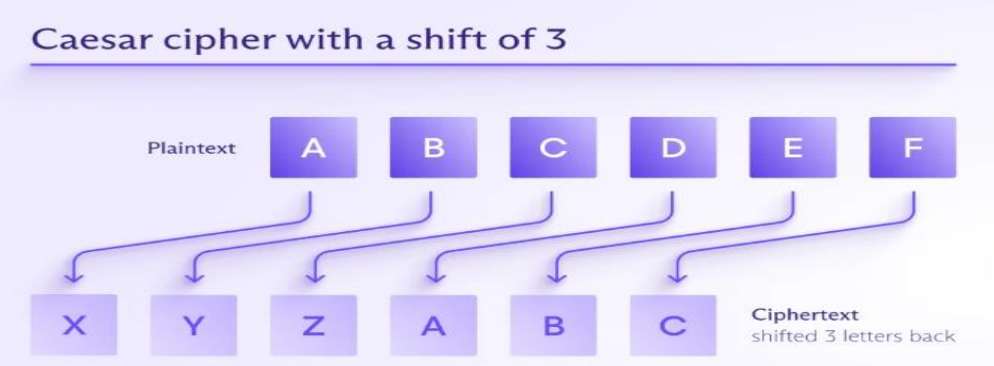


Figure 1.3: Julius Caesar's method of Encryption

So, to decrypt the message into readable plaintext, you must shift each letter three letters forward in the alphabet.

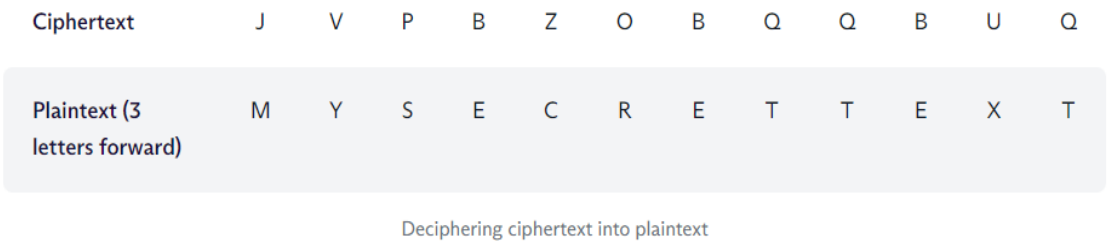


Figure 1.4: Method of Deciphering ciphertext to plaintext

So, JV PBZOBQ QBUQ reads “MY SECRET TEXT”
In this case, the key to the cipher is 3 which is achieved by shifting each letter three places back or forward in the alphabet to encrypt or decrypt it. This is known as a substitution cipher

Table 3.1 Difference Between Plain Text and Cipher Text

Category	Plain Text	Cipher Text
Definition	Original readable data in its natural form.	Encrypted form of data, not easily readable.
Accessibility	It can be understood and used without decryption.	Requires decryption to be understood.
Representation	Represents the actual content of the message.	Represents an encrypted version of the message
Security	Prone to unauthorised access and disclosure.	Offers greater security against breaches.
Conversion	Input to encryption; output from decryption.	Output of encryption; input for decryption.
Purpose	Easily read and understood by humans.	Secure transmission and storage of data.

1.3.3 Encryption and Decryption Applications

Encryption and decryption play pivotal roles in everyday applications, ensuring data confidentiality, integrity, and security in our digital interactions. Here are some examples of how they are used in daily affairs:

Secure Messaging Apps

End-to-end Encryption

Messaging applications like WhatsApp, Signal, and Telegram use end-to-end encryption to secure conversations. When you send a message, it's encrypted and only decrypted on the recipient's device, preventing anyone, including the service provider, from intercepting and reading your messages.

Online Banking

Secure Communication

When you access your bank's website or mobile application, encryption ensures that your login credentials, personal information, and financial transactions are transmitted securely over the Internet. This protects you from eavesdropping and data theft.

Two-Factor Authentication (2FA)

Many online banking services use encryption to secure the delivery of one-time codes for 2FA. This ensures only you can access your account, even if someone has your password.

E-commerce

Payment Security

When making online purchases, encryption (usually SSL/TLS) secures the connection between your browser and the e-commerce website. This safeguards your credit card information and personal details during the transaction.

Digital Wallets

Mobile payment apps like Apple Pay and Google Pay use encryption to protect your payment card data when making in-store or online purchases.
[
Email Encryption

Secure Email Services

Some email services, like Proton Mail, offer end-to-end encryption for email communication. This means that the content of your emails is encrypted and can only be read by the intended recipient.

1.3.4 Importance of Cryptography

As our business processes become increasingly more digitalized and web-based practices like online shopping became more mainstream, much bigger amounts of sensitive information circulate. That is why keeping personal data private has gained significant importance and nowadays, cyber security professionals are putting great emphasis on encryption and cryptography.

Few decades ago, hackers would only target big organizations but as the circulation of private information has become more common and information itself has turned into one of the biggest assets one can have, hackers have been targeting organizations of every size, even individuals. In fact, recent research shows that smaller organizations have been attracting hackers even more since most of them do not allocate much resource and human power to their **cybersecurity operations**. In other words, they are easier to take down.

If you want to keep your business safe, you definitely need proper cryptography and encryption practices in order to keep your personnel information, customer data, business communications and such safe from the **malicious attackers**.

1.3.5 Applications of Cryptography

There are many real-world applications for cryptography, including securing online banking transactions, protecting personal emails, shielding sensitive government communications, and ensuring secure e-commerce transactions. Cryptography also serves a variety of other crucial functions, including:

- **Data Encryption:** Without the decryption key, unauthorised parties cannot comprehend encrypted data, even if they gain access to it.
- **Digital Signatures:** A digital signature verifies the authenticity and integrity of an electronic document or message.
- **Authentication**: In various online interactions, cryptography is used to establish the identity of users or entities.
- **Blockchain Technology:** Unlike other distributed ledger systems, blockchain uses cryptographic principles to protect transactions.

Cryptography has a menagerie of uses depending on the context of the application.

1.3.6 Categories of Cryptography

In today's cybersecurity industry, cryptography can be broadly categorized into three types:

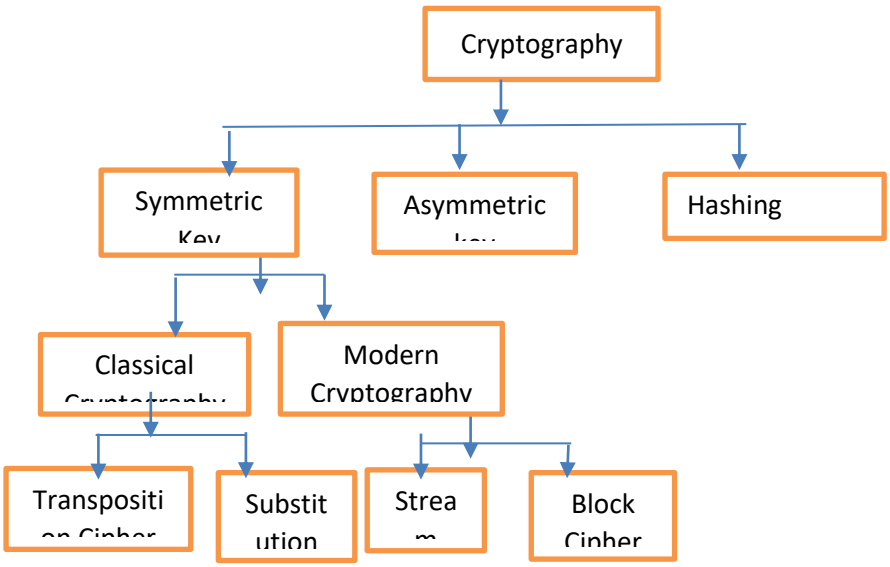


Figure 1.5: Examples of Cryptography

A. Symmetric Encryption

Symmetric encryption or secret-key cryptography uses a single key for both encryption and decryption of data. It is like having a single secret key to lock and unlock a door. Less secure than asymmetric, but relatively faster. Both sender and receiver need to have the secret key. Symmetric encryption is used more for storage and cannot be used for ensuring the integrity and/or authenticity of data. The most popular symmetric key system is the Data Encryption Standard (DES). Others are Advanced Encryption Standard (AES), Triple DES (3DES) and 64-bit Block Cipher (Blowfish).

There are two main forms of symmetric key cryptography: classical and modern cryptography. The classical cryptography is also sub-divided into transposition cipher and substitution cipher while modern cryptography is sub-divided into stream cipher and block cipher.

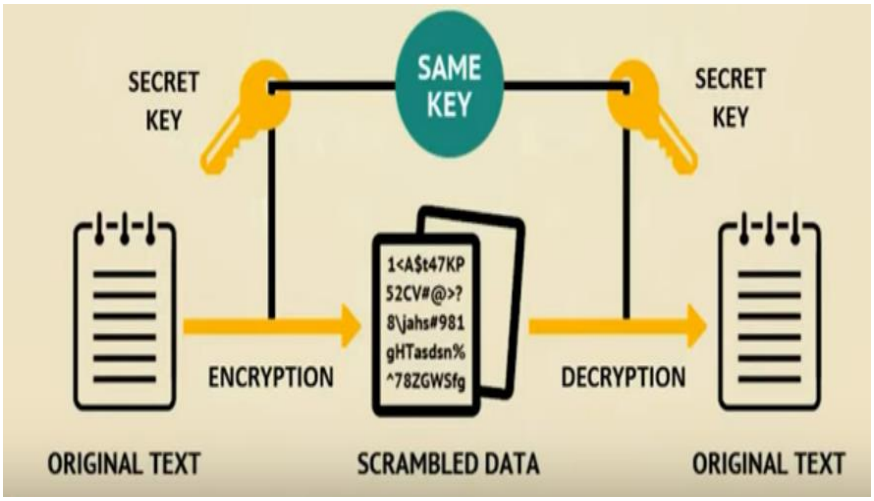


Figure 1.6: Examples of Symmetric Encryption

Transposition Cipher

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext

Plain Tet: MEET ME AFTER PARTY
Key Used: 421635

1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A		T	

Figure 1.7: Examples of Transposition Cipher

Substitution Cipher: A substitution cipher simply means that each letter in the plaintext is substituted with another letter to form the ciphertext. If the same occurs more than once in the plaintext then it appears the same at each occurrence in the ciphertext.

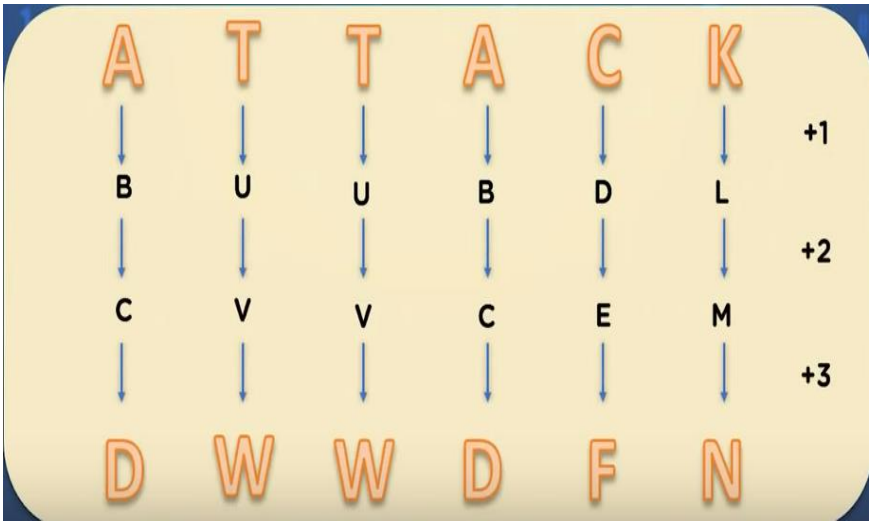


Figure 1.8: Examples of Substitution Cipher

In this case, the key to the cipher is 3. This is achieved when you shift each letter three places back or forward in the alphabet to encrypt or decrypt it.

Stream Cipher

Plaintext is encrypted one bit at a time and encrypted individually. Stream ciphers work on a single bit or byte at any time and constantly change the key using feedback mechanisms. A self-synchronizing stream cipher ensures the decryption process stays in sync with the encryption process by recognizing where it sits in the bit keystream. A synchronous stream cipher generates the keystream independently of the message stream and generates the same keystream function at both the sender and the receiver. One of the most popular stream ciphers is the RC4 (Rivest Cipher 4), which encrypts messages one byte at a time.

Block Cipher

Plaintext is broken into blocks of data and chained together post encryption. Block ciphers encrypt one block of fixed-size data at a time.

It will always encrypt a plaintext data block to the same ciphertext when the same key is used. A good example of block cipher is Advanced Encryption Standard (AES) which is the most commonly used symmetric algorithm. Blocks of 128-bit data are encrypted and decrypted using cryptographic keys of 128, 192, and 256 bits. Another good example of this is the Feistel cipher, which uses elements of key expansion, permutation, and substitution to create vast confusion and diffusion in the cipher.

The stages of encryption and decryption are similar if not identical, which means reversing the key reduces the code size and circuitry required for implementing the cipher in a piece of software or hardware.

B. Asymmetric Encryption

Asymmetric cryptography, also known as public key cryptography, is a process that uses a pair of related keys – one public key and one private key to encrypt and decrypt a message and protect it from unauthorised access or use. In asymmetric encryption public keys are used for encryption and private keys are used for decryption of information.

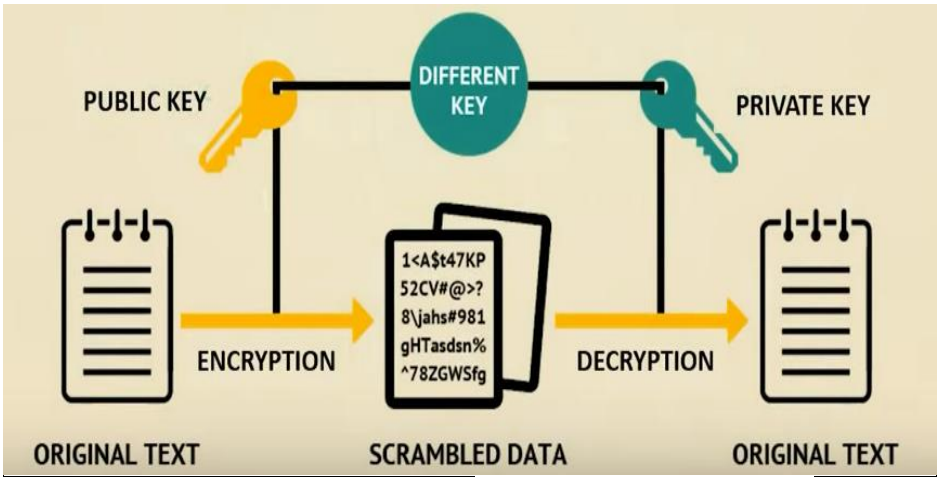


Figure1.9: Examples of Asymmetric Encryption

These algorithms possess an important feature:
It's impossible to figure out the decryption key just by knowing the encryption key and the cryptographic algorithm.
Either of the two keys can be used for encryption, while the other is used for decryption.

Asymmetric-key cryptography uses mathematical functions to transform plaintext and ciphertext represented as numbers for encryption and decryption, while symmetric-key cryptography involves symbol substitution or permutation. In asymmetric-key cryptography, plaintext and ciphertext are treated as integers, requiring encoding and decoding processes for encryption and decryption.
Advantages of Asymmetric Encryption

Asymmetric encryption also known as public key cryptography is a method of cryptography that uses two different keys to encrypt and decrypt data, here are some advantages of asymmetric encryption: –

- **Enhanced Security:** Asymmetric encryption provides a higher level of security compared to symmetric encryption where only

one key is used for both encryption and decryption with asymmetric encryption a different key is used for each process and the private key used for decryption is kept secret by the receiver making, it harder for an attacker to intercept and decrypt the data.

- **Authentication:** Asymmetric encryption can be used for authentication purposes which means that the receiver can verify the sender s identity. This is achieved by the sender encrypting a message with their private key which can only be decrypted with their public key if the receiver can successfully decrypt the message, it proves that it was sent by the sender who has the corresponding private key.
- **Non-repudiation:** Asymmetric encryption also provides non-repudiation which means that the sender cannot deny sending a message or altering its contents this is because the message is encrypted with the sender s private key and only their public key can decrypt it. Therefore, the receiver can be sure that the message was sent by the sender and has not been tampered with.
- **Key distribution:** Asymmetric encryption eliminates the need for a secure key distribution system that is required in symmetric encryption with symmetric encryption, the same key is used for both encryption and decryption and the key needs to be securely shared between the sender and the receiver asymmetric encryption, on the other hand, allows the public key to be shared openly and the private key is kept secret by the receiver.
- **Versatility:** Asymmetric encryption can be used for a wide range of applications including secure email communication online banking transactions and e-commerce it is also used to secure SSL/TSL connections which are commonly used to secure internet traffic.

Key Components

- **Plaintext**: This refers to the original, readable message or data that is inputted into the encryption algorithm.
- **Encryption algorithm**: This algorithm transforms the plaintext in various ways.
- **Public and private keys**: A pair of keys chosen so that if one is used for encryption, the other is used for decryption. The specific transformations performed depend on whether the public or private key is provided as input.
- **Ciphertext**: The encrypted, scrambled message produced as output. It can be find using both the plaintext and the key, but if there are different keys then it will give different ciphertexts for the same message or plaintext.
- **Decryption algorithm**: This algorithm takes the ciphertext and the corresponding key and retrieves the original plaintext.

C. Hashing

This is a third type of cryptography that does not use a key. It uses a fixed length hash value based on the plain text message. This can then be used to ensure that the message has not been altered or compromised. Hash functions add an extra layer of security, as the hashed output can't be reversed to reveal the data that was originally input.

Hashing is the practice of transforming a given key or string of characters into another value for the purpose of security. Although the terms "hashing" and "encryption" may be used interchangeably, hashing is always used for the purposes of one-way encryption, and hashed values are very difficult to decode. Encryption always offers a decryption key, whereas hashed information cannot be decoded easily and is meant to be used as a method for validating the integrity of an object or piece of data. In a nut-shell, hashing scrambling data beyond recognition, the output is called hash value, and has a fixed size. Generally, not reversible.

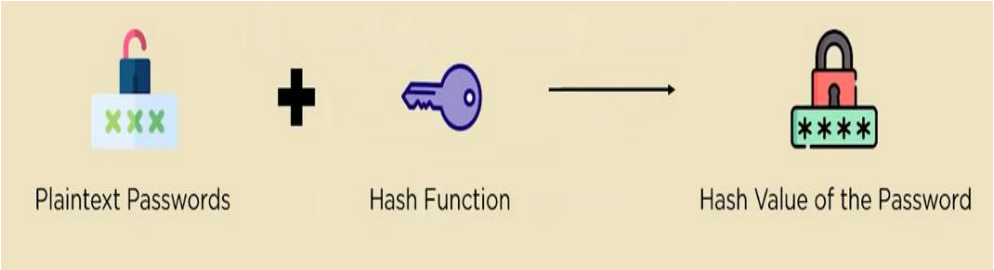


Figure 1.10: Examples of Hashing

From the above, it is clear that the main difference in symmetric and asymmetric encryption in cryptography is that the first only involves one key while the second requires two.

1.3.7 Cryptographic Attack

As cryptography techniques help secure sensitive data and communications, attackers constantly evolve strategies to crack cryptosystems. Understanding common cryptography attacks is key to improving defenses.

1. **Ciphertext-Only Attacks**
   These attacks occur when hackers try to unlock secret messages they've grabbed. They keep guessing different combinations until they crack the code and reveal what's inside. Strong encryption complexity safeguards against this.
2. **Known-Plaintext Attacks**

When attackers have matching plaintext and encrypted ciphertext samples, they analyze patterns to deduce encryption keys or algorithms. Random initialization vectors in ciphers resist such observations.

3. **Chosen-Plaintext Attacks**
   This gives attackers the ability to choose arbitrary plaintexts to be encrypted for examining corresponding ciphertext outputs for clues to brake systems. Padding plaintext variably before encryption counters this.
4. **Chosen-Ciphertext Attacks**
   In these attacks, adversaries pick ciphertexts to be decrypted and have access to the resulting plaintexts. This can potentially uncover hidden relationships between plain and cipher flows. Using robust public key infrastructure prevents this.
5. **Side-Channel Attacks**
   By monitoring cryptosystem secondary outputs like computation time, power consumption, or electromagnetic leaks, attackers can infer secrets enabling ciphertext decoding. Randomizing encryption operations impedes side channels.
6. **Passive Attack**
   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.
7. **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.
8. **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 attack. 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.

Self-Assessment Exercise(s)

1. What is the main problem with public key cryptography?
2. What is the main problem with public key cryptography?
3. Can private key be used for encryption?

1.4 Summary

At the end of this unit, you have learnt the definition of cryptography, its importance in cybersecurity, its components and types. In the next unit, you will be introduced to steganography.

You have learnt from this unit that cryptography as a division of computer science focuses more on methods of transforming data into formats that cannot be recognized by unauthorised users as a means of enforcing security and data protection. Hence, it is important to learn the methods of cryptography to securing our data.

1.5 References/Further Readings/Web Resources

Anshika Modi (2023) What is Asymmetric Encryption? (2023). Retrieved from https://www.geeksforgeeks.org/what-is-asymmetric-encryption

Fullstack Academy Team (2024). What is Cryptography? Retrieved from https://www.fullstackacademy.com/blog/what-is-cryptography

Harry Bone (2023). What is ciphertext? Retrieved from https://proton.me/blog/what-is-ciphertext

4.0 Possible Answers to Self-Assessment Exercises

What is the main problem with public key cryptography?

Answer

The main problem with public key cryptography is that it's slower and takes more computational power and time to encrypt and decrypt data than other types of encryptions.

Can public key be used to decrypt?

Answer

No, the public key cannot be used to decrypt messages encrypted with its corresponding private key. This is a core principle of public key cryptography.

Mathematical asymmetry: The public and private keys are mathematically linked in a way that allows one to encrypt messages the other can decrypt, but not the other way around.

Security by design: Public keys are designed to be easily shared. If they could decrypt messages, anyone with a public key could read any encrypted messages intended for that key, which would defeat the purpose of encryption.

Can private key be used for encryption?

Answer

Yes, but using a private key for encryption is generally not recommended. In asymmetric Key cryptography, the public key is for encryption, and the private key is for decryption. This mathematical asymmetry is what ensures the security of the system. If you use a private key to encrypt data, anyone with access to the public key (which is by definition widely available) could potentially decrypt it.

Unit 2 Steganography

2.1 Introduction

Steganography is a system which lets stoners hide secret information within normal or ordinary lines or dispatches. It offers a way to give enhanced security for data transfer and communication over the network. There are colorful forms of Steganography which includes Image Steganography, Audio Steganography, Text Steganography, etc. Also, there are colorful advantages of using Steganography like it offers better security, it's delicate to discrete.

Steganography is more of a concept than a method of data delivery by secretive methods. This makes the application of Steganography easier in more than one clever way. Steganography is significantly more sophisticated than before. It is often paired with cryptography for double protection.

2.2 Learning Outcomes

By the end of this unit, you will be able to:

- define steganography.
- understand how steganography different from cryptography
- mention some advantages and disadvantages of steganography.
- state tools to perform steganography.

2.3 Steganography

2.3.1 Definition of Steganography

The word **Steganography** is derived from two Greek words- 'stegos' meaning 'to cover' and 'grayfia', meaning 'writing', thus translating to 'covered writing', or 'hidden writing'. Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

Steganography can also be defined as the art and science of embedding secret messages in a cover message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.

2.3.2 Differences between Steganography and Cryptography

Cryptography and steganography are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable, or hides the *meaning* of the data, while steganography hides the *existence* of the data.

In layman's terms, cryptography is similar to writing a letter in a secret language: people can read it, but won't understand what it means. However, the existence of a (probably secret) message would be obvious to anyone who sees the letter, and if someone either knows or figures out your secret language, then your message can easily be read.

If you were to use *steganography* in the same situation, you would hide the letter inside a pair of socks that you would be gifting the intended recipient of the letter. To those who don't know about the message, it would look like there was nothing more to your gift than the socks. But the intended recipient knows what to look for, and finds the message hidden in them.

Similarly, if two users exchanged media files over the internet, it would be more difficult to determine whether these files contain hidden messages than if they were communicating using cryptography.

Cryptography is often used to supplement the security offered by steganography. Cryptography algorithms are used to encrypt secret data before embedding it into cover files.

Steganography	Cryptography
Steganography is defined as a system of concealing data or information underknown-secret data or training.	Cryptography is defined as the system of guarding information and communication with the help of colorful ways.
Its main purpose is to maintain communication security.	Its main ideal is to give data protection.
The structure of data is not modified in the case of Steganography.	The structure of data is modified in the case of Cryptography.
It is less popular.	It is further popular.
The use of key is not obligatory, but if it is used it enhances security.	The use of key is obligatory in the case of Cryptography.
In Steganography, the use of fine metamorphoses is not involved importantly.	But, in Cryptography, there is use of fine metamorphoses to play with the data and increase protection.

2.3.3 Types of Steganography

Depending on the nature of the cover object (actual object in which secret data is embedded), steganography can be divided into five types:

i. Text Steganography
ii. Image Steganography
iii. Video Steganography
iv. Audio Steganography
v. Network Steganography

A. Text Steganography

Text Steganography is hiding information inside the text files. It involves things like changing the format of existing text, changing words within a text, generating random character sequences or using context-free grammars to generate readable texts. Various techniques used to hide the data in the text are:

- Format Based Method
- Random and Statistical Generation
- Linguistic Method

For example, take the following text.
The follow eng tixt contaens a sicrit missagi
Does not really make sense right? But what if we replace the i's with e's and the e's with i's?

The follow ing text contains a secret message
I think that's a little easier on the eyes. This is a pretty easy example, but there are much more complicated ones and even some you could come up with on your own.

B. Image Steganography

Hiding the data by taking the cover object as the image is known as image steganography. In digital steganography, images are widely used cover source because there are a huge number of bits present in the digital representation of an image. It is achieved by making changes in the pixels of the image to render the information. It is generally used for watermarking, covert communication, brand protection, etc. There are a lot of ways to hide information inside an image. Common approaches include:

- Least Significant Bit Insertion
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Coding and Cosine Transformation
- Take a look at the two images below and spot the difference:

Figure 2.1 Text Steganography

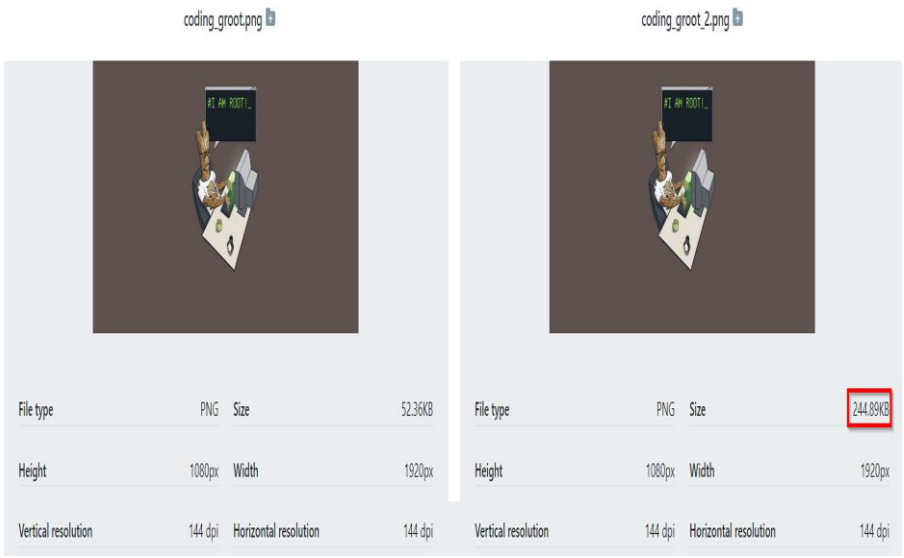


Figure 2.2 Image Steganography

Basically, no human on earth can tell the visual difference. But if you take a closer look at the file details

…

The only difference is the size of the images. That's because the one on the right is hiding 260 words of text in it. How cool is that?

Least Significant Bit (LSB)

Least Significant Bit (LSB) is an example of Spatial methods.

LSB method is a common, simple method to embedding information in a cover file.

In steganography, LSB substitution method is used. i.e since every image has three components (RGB). This pixel information is stored in encoded format in one byte.

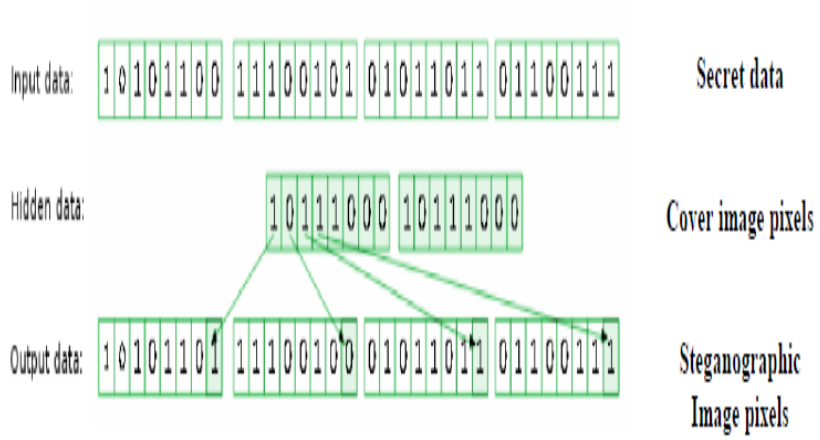


Figure 2.3: Sample Scenario of Pixel information of LSB

Steps used in LSB steganography:

a. Steps for hiding message image:

1. Read the image to be used as cover image. Noise is added to make it easier to disguise changes due to embedding the message image.
2. Read the image to be used as message image.
3. Separate the bit planes of each image.
4. Replace the least 4-bit planes of cover image with the 4 most significant bit planes from message image.
5. Get the resultant Steganographic image by recombining these bit planes.

b. Steps for Retrieving message image:

1. Read the Steganographic image.
2. Extract the required number of bit planes of the image.
3. Recombining the lower four-bit planes would give the retrieved message image.

Masking and filtering

Masking and filtering operations are carried out to mark the carrier image, somewhat like a watermark

Redundant pattern encoding (RPE)

It uses more than one graphic or visual structure, such as color + position, to encode one variable of data

LSB insertion
It replaces the least significant bit of a media file with hidden content

Encrypt and scatter
It hides the message as white noise

Algorithms and transformations
It makes use of algorithms to conceal information in an image

A. Video Steganography

In Video Steganography you can hide any kind of data into digital video format. The advantage of this type is a large amount of data can be hidden inside and the fact that it is a moving stream of images and sounds. You can think of this as the combination of Image Steganography and Audio Steganography. The ideal way to use Video Steganography is to detect secret information in a videotape in such a way that normal people won't notice it. Two main classes of Video Steganography include:

Embedding data in uncompressed raw video and compressing it later
Embedding data directly into the compressed data stream

B. Steganography

Audio Steganography is defined as a type of steganography which involves caching dispatches or secret information within audio lines. The ideal behind using this fashion is to hide information in such a way that people cannot notice it when they hear the audio. It's generally used for digital rights operation in audio lines.

A few audio Steganography methods that are used are:

Spread Spectrum
In this type of Steganography, a signal that is generated with a particular bandwidth is spread in the frequency domain to get a wider bandwidth than the carrier message.

The wider bandwidth, however, maintains the same signal power, and the signal is extremely difficult to distinguish from the noise due to the unclear peak in the spectrum. Hence, it makes for secure communication.

Parity Coding
In this type of Steganography, the carrier audio signal is split into separate samples and the secret message is concealed in the parity bit of each sample area. If the parity bit does not match with the hidden message bit, then the LSB of the sample area is inverted.

Phase Coding
In this type of Steganography, the phase of the carrier file is replaced with a reference phase that represents the concealed data.

LSB Coding
This type of Steganography involves substituting the LSB of each sampling point with a binary message, thus allowing the encoding of a large amount of data. The ideal data transmission rate is 1 Kbps per 1 kHz.

E**cho Hiding**
This type of Steganography allows the embedding of data into the host audio through the introduction of a short echo. The echo is in the form of resonance added to the host signal. After the echo is introduced, the stego signal retains the statistical and perceptual characteristics of the carrier audio.

The data can be hidden by manipulating the three parameters of the echo signal, the initial amplitude, the offset delay, and the decay rate so that the echo is not audible. Thus, data is hidden in this manner without being perceptible.

C. Network Steganography (Protocol Steganography)

It is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP etc. You can use steganography in some covert channels that you can find in the OSI model.

2.3.4 Tools for performing Steganography

There are a lot of software available that offer steganography. Some offer normal steganography, but a few offers encryption before hiding the data. These are the steganography tools which are available for free:

Steg suite is a free steganography tool which is written in Java. With Stegosuite you can easily hide confidential information in image files.
Steghide is an open-source Steganography software that lets you hide a secret file in image or audio file including JPEG, BMP, AU, and WAV

Xiao Steganography is a free software that can be used to hide data in BMP images or in WAV files.

SSuite Picsel is another free portable application to hide text inside an image file but it takes a different approach when compared to other tools.

OpenStego is a professional steganographic tool where you can store files in image, audio, video or flash files.

Self-Assessment Exercises

1. List some examples of Steganography
2. Give an illustration of Steganography?

2.4 Summary

At the end of this unit, you have learnt the definition of steganography, the reason behind steganography, the differences between steganography and cryptography and its various types.

You have learnt from this unit that Cryptography and steganography are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable, or hides the *meaning* of the data, while steganography hides the *existence* of the data. Therefore, it is important to study methodologies of achieving steganography and cryptography for data security and authentication of data.

2.5 References/Further Readings/Web Resources

Daniel Iwugo (2023). What is Steganography? How to Hide Data Inside Data.

Simplilearn (2023). What is Steganography? Types, Techniques, Examples & Applications

2.6 Possible Answers to Self-Assessment Exercises

List some examples of Steganography

Answer to Sae 1

Steganography Examples Include

i. Writing with invisible ink
ii. Embedding text in a picture (like an artist hiding their initials in a painting they've done)
iii. Backward masking a message in an audio file (remember those stories of evil messages recorded backward on rock and roll records?)
iv. Concealing information in either metadata or within a file header
v. Hiding an image in a video, viewable only if the video is played at a particular frame rate
vi. Embedding a secret message in either the green, blue, or red channels of an RRB image

Give an illustration of Steganography?

Answer to SAE 2

An illustration of Steganography includes hiding some information in the title of a participated videotape or image.

MODULE 5 CYBER ATTACKS AND DEFENCE MECHANISMS

Introduction

The world has witnessed a cybersecurity evolution over the past few decades. Gone are the days when the biggest concern was computer viruses. Today, sophisticated cyber- attacks involving phishing malware, machine learning and artificial intelligence put individuals, corporations and governments alike at constant risk.

Unit 1 Definition and Classification of Cyber- attacks
Unit 2 Denial of Service (and other) attack strategies, worms, viruses
Unit 3 Transfer of funds/value across networks

In each unit of this module, I explored each topic in detail and highlight self-assessment exercise at the end of each unit. Finally, I highlight resources for further reading at the end of each unit.

Unit 1 Definition and Classifications of Cyber-attack

Unit Structure

1.1 Introduction

Everyone among us has one time or another has come across some form of attack. It could be physical or emotional or of some other kind. The intent is to cause some sort of harm though sometimes it turns into a blessing in disguise. However, cyber-attacks always aim at causing harm. They can be varied in their nature of approach and type of harm they inflict, depending on the motive, but the purpose is certainly malicious.

1.2 Learning Outcome

By t the end of this unit, you will be able to:

- define cyber-attack
- discuss different types of cyber-attack

1.3 Cyber-attack

1.3.1 Definition of Cyber-attack

Cyber-attack is an attack initiated from a computer against a website, computer system or individual computer system that compromises the confidentiality, integrity or availability of the computer or information stored on it. Cyber-attacks take many forms.

It is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.

Cyber-attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labeled as either a Cyber campaign, cyber warfare or cyber terrorism in different context. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nation.

1.3.2 Types of Cyber-Attack

1. **Backdoors**
   Backdoors type of cyber-attack is a way of bypassing normal authentication, it is a type of cyber threat in which the attacker uses a back door to install a key logging software, thereby allowing an illegal access to your system. This threat can turn out to be potentially serious as it gives room for modification of the files, stealing information, installing unwanted software or even taking control of the entire computer. Default passwords can function as backdoors if they are not changed by the user. Some

debugging features can also act as backdoors if they are not removed in the release version.

Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer (generally a PC on broadband running Microsoft Windows and Microsoft Outlook). Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines. Others, such as the Sony/BMG rootkit distributed silently on millions of music CDs through late 2005, are intended as Digital Rights Management (DRM) measures and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers.

2. Denial-of-Service Attack

A denial-of-service (DoS) attack is attacking the network to bring it down completely with useless traffic by affecting the host device which is connected to the Internet. DoS attack targets websites or services which are hosted on the servers. This type of attack can aim bank servers and credit card payment gateways.

3. Direct-access Attack

A direct-access attack simply means gaining physical access to the computer or its part and performing various functions or installing various types of devices to compromise security. The attacker can install software loaded with worms or download important data, using portable devices.

4. Eavesdropping

As the name suggests, eavesdropping means secretly listening to a conversation between the hosts on a network. There are various programs such as Carnivore and Narus Insight that can be used to eavesdrop.

5. Spoofing

Spoofing is a cyber-attack where a person or a program impersonate another by creating false data in order to gain illegal access to a system. Such threats are commonly found in emails where the sender's address is spoofed.

6. Tampering

Tampering is a web-based attack where certain parameters in the keys of Uniform Resource Locator (URL) looks and appears exactly the same. Tampering is basically done by hackers and criminals to steal the identity and obtain illegal access to information.

7. Repudiation Attack

A repudiation attack occurs when the user denies the fact that he or she has performed a certain action or has initiated a transaction. A user can simply deny having knowledge of the

transaction or communication and later claim that such transaction or communication never took place.

8. Information Disclosure

Information disclosure breach means that the information which is thought to be secured is released to unscrupulous elements who are not trustworthy.

9. Privilege Escalation Attack

A privilege escalation attack is a type of network intrusion which allows the user to have an elevated access to the network which was primarily not allowed. The attacker takes the advantage of the programming errors and permits an elevated access to the network.

10. Exploits

An exploit attack is basically a software designed to take advantage of a flaw in the system. The attacker plans to gain easy access to a computer system and gain control, allows privilege escalation or creates a DOS attack.

11. Social Engineering

An attack by a known or a malicious person is known as social engineering. They have knowledge about the programs used and the firewall security and thus it becomes easier to take advantage of trusted people and deceive them to gain passwords or other necessary information for a large social engineering attack.

12. Indirect Attack

Indirect attack means an attack launched from a third-party computer as it becomes more difficult to track the origin of the attack.

13. Computer Crime

A crime undertaken with the use of a computer and a network is called as a computer crime.

14. Malware

Malware refers to malicious software that are being designed to damage or perform unwanted actions in the system. Malware is of many types like viruses, worms, Trojan horses, etc., which can cause havoc on a hard drive. They can either delete some files or a directory or simply gather computer data without the actual knowledge of the user.

15. Adware

Adware is a software that supports advertisements which renders ads to its author. It has advertisements embedded in the application. So, when the program is running, it shows the advertisement. Basically, adware is similar to malware as it uses ads to inflict computers with deadly viruses.

16. Bots

Bots is a software application that runs automated tasks which are simple and repetitive in nature. Bots may or may not be

malicious, but they are usually found to initiate a DoS attack or a click fraud while using the internet.

17. Ransomware

Ransomware is a type of cyber security threat which will restrict access to your computer system at first and will ask for a ransom in order for the restriction to be removed. This ransom is to be paid through online payment methods only which the user can be granted an access to their system.

18. Rootkits

A rootkit is a malicious software designed in such a way that hides certain process or programs from normal anti-virus scan detection and continues to enjoy a privilege access to your system. It is that software which runs and gets activated each time you boot your system and are difficult to detect and can install various files and processes in the system.

19. Spyware

Spyware, as the name suggests, is a software which typically spies and gathers information from the system through an internet connection without the user's knowledge. A spyware software is majorly a hidden component of a freeware program which can be downloaded from the internet.

20. Scareware

Scareware is a type of threat which acts as a genuine system message but actually are not. The main purpose of the scareware is to create anxiety among the user and use the anxiety to coax them to download irrelevant software.

21. Trojan Horses

Trojan Horses are a form of threat that are malicious or harmful codes hidden behind genuine programs or data which can allow complete access to the system and can cause damage to the system or data corruption or loss/theft of data. It acts as a backdoor and hence it is not easily detectable.

22. Virus

A computer virus is a self-replicating program which, when executed, replicates or even modifies by inserting copies of itself into another computer file and infects the affected areas once the virus succeeds in replicating. This virus can be harmful as it spreads like wildfire and can infect majority of the system in no time.

23. Worm

Just like a virus, worm is a self-replicating program which relies on computer network and performs malicious actions and spreads itself onto other computer networks. Worms primarily rely on security failures to access the infected system.

24. Phishing

Phishing is a cyber threat which makes an attempt to gain sensitive information like passwords, usernames and other details for malicious reasons. It is basically an email fraud where the perpetrator sends a legitimate looking email and attempts to gain personal information.

25. Identity theft

Identity theft is a crime wherein your personal details are stolen and these details are used to commit a fraud. An identity theft is committed when a criminal impersonates individuals and use the information for some financial gain.

26. Intellectual Property Theft

Intellectual Property theft is a theft of copyrighted material where it violates the copyrights and the patents. It is a cybercrime to get hands onto some trade secrets and patented documents and research. It is basically a theft of an idea; plan and the methodology being used.

27. Password Attacks

Password attack is a form of a threat to your system security where attackers usually try ways to gain access to your system password. They either simply guess the password or use an automated program to find the correct password and gain an entry into the system.

28. Bluesnarfing

Bluesnarfing is a threat of information through unauthorized means. The hackers can gain access to the information and data on a Bluetooth enabled phone using the wireless technology of the Bluetooth without alerting the user of the phone.

29. Bluejacking

Bluejacking is simply sending of texts, images or sounds, to another Bluetooth enabled device and is a harmless way of marketing. However, there is a thin line between bluejacking and bluesnarfing and if crossed it results into an act of threat.

30. DDoS

DDoS basically means a Distributed Denial of Service. It is an attempt to make any online service temporarily unavailable by generating overwhelming traffic from multiple sources or suspend services of a host connected to the internet.

31. Keylogger

A keylogger is a spyware that has the capability to spy on the happenings on the computer system. It has the capability to record every stroke on the keyboard, websites visited and every information available on the system. This recorded log is then sent to a specified receiver.

Self-Assessment Exercises

Self-Assessment Exercises 1

i. _____is an attack initiated from a computer against a website, computer system or individual computer.
ii. _____ is a spyware that has the capability to spy on the happenings on the computer system.
iii. _____ is the act or practice of obtaining secrets without the permission of the holder of the information
iv. _____is a threat of information through which the hackers can gain access to the information and data on a Bluetooth enabled phone.
v. _____is a type of cyber security threat which will restrict access
vi. to your computer system at first and will ask for a ransom in order for the restriction to be removed.

Self-Assessment Exercises 2

State True or False:

i. Hostile code like StuxNet is an example of weapons for cyber warfare.
ii. Phishing is basically an email fraud where the perpetrator sends a legitimate looking email and attempts to gain personal information.
iii. The ransom in Ransomware attack is to be paid through online payment methods.
iv. In a privilege escalation attack, URL are changed without the customer's knowledge
v. Hacktivists are responsible for denial-of-service (DoS).

1.4 Summary

At the end of this unit, you have learnt the definition and various types of cyber-attacks. In the next unit, you will be introduced to Denial of Service (and other) attack strategies, worms, viruses

You have learnt from this unit that cyber-attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices towards means of malicious acts and should be guide against at all cost to enforce data integrity

1.5 References/Further Reading/Web Resources

Nilesh K. Modi (2021) Cyber Attacks and Counter measures: Users perspectives, published by Dr. Babasaheb Ambedkar Open University. Babasaheb

The Evolution of Cyber-Threats; Past, Presents and Future (2024), online.yu.edu

1.6 Possible Answers to Self-Assessment Exercises

Self-Assessment Exercises 1

Fill in the blanks:

i. _____is an attack initiated from a computer against a website, computer system or individual computer.
ii. _____ is a spyware that has the capability to spy on the happenings on the computer system.
iii. _____ is the act or practice of obtaining secrets without the permission of the holder of the information
iv. _____is a threat of information through which the hackers can gain access to the information and data on a Bluetooth enabled phone.
v. _____is a type of cyber security threat which will restrict access to your computer system at first and will ask for a ransom in order for the restriction to be removed.

Answers

i. Cyber attack
ii. Keylogger
iii. Cyber spying, or cyber espionage
iv. Bluesnarfing
v. Ransomware

Self-Assessment Exercises 2

State True or False:

i. Hostile code like StuxNet is an example of weapons for cyber warfare.
ii. Phishing is basically an email fraud where the perpetrator sends a legitimate looking email and attempts to gain personal information.
iii. The ransom in Ransomware attack is to be paid through online payment methods.
iv. In a privilege escalation attack, URL are changed without the customer's knowledge
v. Hacktivists are responsible for denial-of-service (DoS).

Answers

i. True
ii. True
iii. True
iv. False
v. True

Unit 2 Denial of Service (and other) attack strategies, worms, viruses

Unit Structure

2.1 Introduction

In the ever-evolving field of cybersecurity, understanding potential threats is the first line of defense. One such threat that has caused significant disruptions over the years is the Denial-of-Service (DoS) attack. This type of cyber-attack seeks to make a computer, network, or service unavailable to its intended users by overwhelming the target's resources. DoS attacks usually happen by generating mass bot traffic. Denial of Service attacks are usually generated for malicious intentions and, sometimes, they can happen unintentionally as well. Several DoS attack tools are available on the internet. It is recommended to install or invest in anti-DoS tools to prevent your site or your organization’s site from being subjected to DoS attacks and ensuring hassle-free user experience for your audience.

2.2 Learning Outcomes

By the end of this unit, you will be able to:

- define Denial-of-Service (DoS) Attack.
- understand types of DoS Attacks
- understand the difference between DoS and DDoS Attacks

- state the meaning of a computer virus
- state types of computer virus
- list examples of computer virus and anti-virus

2.3 Denial-of-Service Attack

2.3.1 Definition of Denial-of-Service Attack

A Denial-of-Service Attacks (DoS) attack is a security threat that occurs when an attacker makes it impossible for legitimate users to access computer systems, devices, services or other IT resources. That is, a DoS attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

Denial of Service Attacks (DoS) attack can also be defined as a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to it customers.

Aim of "DoS Attacks"

- Purpose is to shut down a site, not penetrate it.
- Purpose may be vandalism, extortion or social action (including terrorism, sports betting sites often extorted)
- Modification of internal data, change of programs (includes defacement of web sites)
-

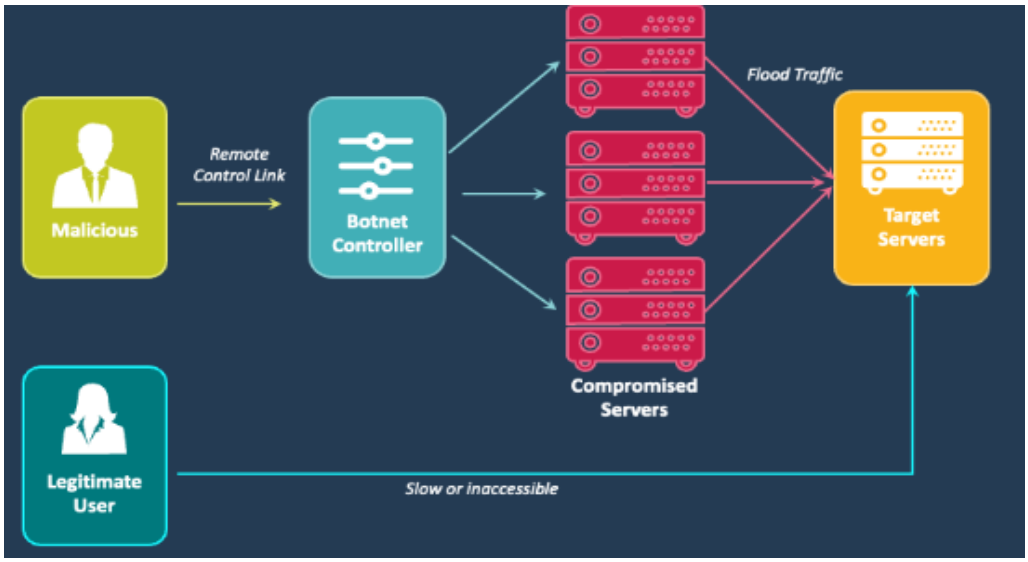


Figure 2.1: Denial of Service Attack

2.3.2 Types of DoS Attacks

DoS attacks can be classified into several types based on the techniques used. Here are four of the most common ones:

1. Volume-Based Attacks: The aim of a volumetric attack is to saturate the bandwidth of the targeted site, and magnitude is measured in bit per second (Bps). Examples include Internet Control Message Protocol (ICMP) floods and User Datagram Protocol (UDP) floods. An example of this would be an attack that exploits the ICMP protocol by sending a large number of ICMP "echo" requests to the victim. As a result, the bandwidth will be overloaded by these requests and the network will only be able to let through a few legitimate requests, if any at all.

2. Protocol Attacks: This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measure in Packet per second. Example includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS

Examples:

SYN Floods:

This is a type of 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. It will therefore be slowed down or even become inaccessible. This attack exploits the TCP protocol.

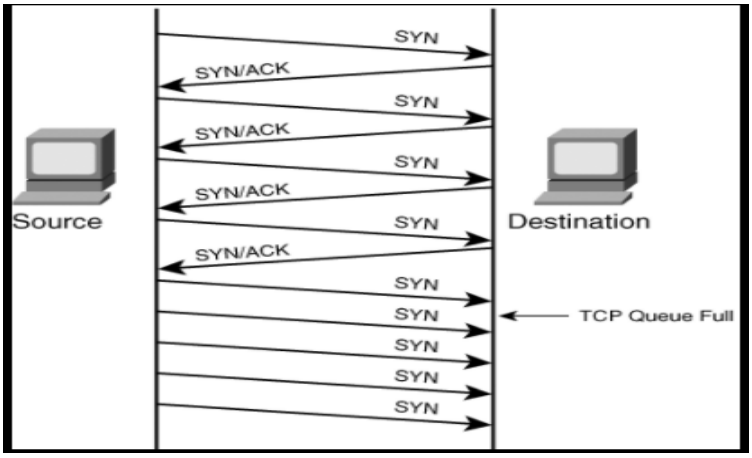


Figure 2.2: Example of Protocol Attack

(Source:https://swordfish.wordpress.com/2006/03/16/denial-of-service-attacks-dos/)

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.

Smurf Attack:
Here, the perpetrator exploits the broadcast address of a weak network by distributing spoofed packets that belong to the aimed device. Once the receivers of these spoofed packets respond, their Internet Protocol (IP) address is then flooded with those responses.

Considering the fact that a particular Internet Broadcast Address can sustain at most 255 hosts, a smurf attack works by intensifying each ping by 255. The outcome is that the network becomes slow to a level where it becomes difficult to use and discarded.

Ping of Death or ICMP Flood:
ICMP flood attack is utilized to take misconfigured or unconfigured network and implement them in distributing spoof packets to ping all the system within that network.

The ping of death attack is often merged together with ICMP flood.

Application layer attacks: These attacks consist of exploiting certain protocols at layer 7 of the OSI model, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second. HTTP floods are a common example. This is the type of attack that we are used to using during web application penetration tests.

Advanced Persistent DoS (APDoS): This is a more advanced form of DoS, where the attacker uses multiple attacking systems and different attack vectors.

Teardrop attacks: In a Teardrop attack, the attacker sends heavy packets fragmented into many pieces to the victim. However, the attacker will have fragmented these packets abnormally, which will destabilize the target system when it tries to reassemble the fragments into packets. This attack therefore exploits the IP protocol.

2.3.3 Difference between DOS and DDoS Attacks

The main difference between a Denial of Service (DoS)and a distributed denial of service (DDoS) attack is that in a DoS attack, the victim is attacked by a single system while in a DDoS attack, on the other hand, the attacker uses a multitude of systems to attack the victim. Because the

attack comes from several sources at once, DDoS is generally faster and harder to block than DoS, and it is difficult to trace its source.
Carrying out DDoS tests as part of a penetration test is of little use, as it will always be possible to bring down a service if you devote the necessary resources to it.

DoS tests, on the other hand, can identify vulnerabilities in configurations or applications. And in these cases, patches can be implemented.

DoS = when a single host attack
DDoS = when multiple hosts attack simultaneously

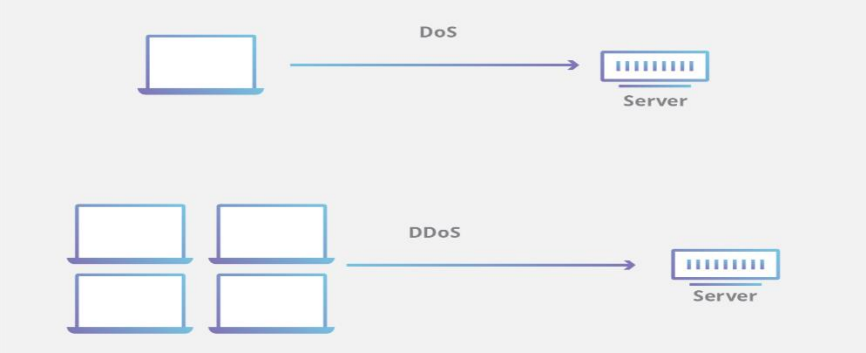


Figure 2.3: DoS and DDoS

DoS utilizes a single connection, while a DDoS attack utilizes many sources of attack traffic, often in the form of a botnet. Generally speaking, many of the attacks are fundamentally similar and can be attempted using one more many sources of malicious traffic.

2.3.4 Counter Measures

More generally, to protect against denial-of-service attacks and limit their impact, here is a non-exhaustive list of solutions that can be put in place:

Implement rate limiting: It is possible to restrict access to the server to one or more IPs if they are considered to be malicious.
Use one or more load balancers: A load balancer can be used to redirect incoming traffic equally to several servers so as not to overload a single server.

Implement a WAF: A WAF or “application firewall” can be used to establish rules that can recognise and block malicious traffic before it reaches the server.

Monitor network traffic: By constantly analysing network traffic, you can quickly detect a denial-of-service attack. The response to such an attack can be rapid and the damage limited.

Keep components up to date: Having up-to-date components prevents attackers from exploiting known vulnerabilities in certain versions of components (use up-to-date anti-virus and IDS tools.), which could lead to a denial-of-service attack.

Perform network analysis to find out the possibility of DOS attack.
Shut down unnecessary services in the target network.
Use strong encryption mechanisms.

2.4 Computer Virus

2.4.1 Definition of Computer Virus

Computer viruses are malicious executable code written by software developers to check piracy on some of their system and application software attached to another executable file that can be harmless or can modify or delete data. When computer program runs attached with a virus it performs some action such as deleting a file from the computer system.

A computer virus is a small software program that interferes with computer operation and spreads from one computer to another.
A virus is a self-replicating program that copies itself and that can infect other programs by modifying them or their environment such that a call to an infected program implies a call to a virus.

2.4.2 Types of computer Virus

Computer virus can be classified into three categories such as boot sector virus, direct action virus (executable virus), and document virus among other.

1. **Boot Sector Virus:** A boot sector is a region of a hard disk, optical disc, or other data storage devices, that contain machine code to be loaded into RAM. The purpose of a boot sector is to allow the boot process of a computer, to load a program, usually an operating system stored on the same storage device. The location and size of the boot sector, are specified by the design of the computing platform. Boot sector virus targets the boot sector of a hard disk and crucially affects the boot process. Boot sector virus became popular because of the use of disks to boot a computer. The widespread usage of the internet and the death of

the floppy has made other means of virus transmission more effective.

It is challenging and a complex task to remove this virus and often requires the system to be formatted. Mostly it spreads through removable media.
Examples of boot sector virus are polybootB, AntiEXE

2. **Direct Action Virus:** When a virus attaches itself directly to a .exe or .com file and enters the device while its execution is called a Direct-Action Virus. If it gets installed in the memory, it keeps itself hidden. It is also known as Non-Resident Virus or Executable virus.
3. **Document virus:** this virus can affect the document by moving from a disk partition table to a different sector and replace it with its own code, therefore, infecting document as they are accessed.
4. **Resident Virus**: A virus which saves itself in the memory of the computer and then infects other files and programs when its originating program is no longer working. This virus can easily infect other files because it is hidden in the memory and is hard to be removed from the system.
5. **Multipartite Virus:** A virus which can attack both, the boot sector and the executable files of an already infected computer is called a multipartite virus. If a multipartite virus attacks your system, you are at risk of cyber threat.
6. **Overwrite Virus:** One of the most harmful viruses, the overwrite virus can completely remove the existing program and replace it with the malicious code by overwriting it. Gradually it can completely replace the host's programming code with the harmful code.
7. **Polymorphic Virus:** Spread through spam and infected websites, the polymorphic virus are file infectors which are complex and are tough to detect. They create a modified or morphed version of the existing program and infect the system and retain the original code.
8. **File Infector Virus:** As the name suggests, it first infects a single file and then later spreads itself to other executable files and programs. The main source of this virus are games and word processors.

9. **Spacefiller Virus**: It is a rare type of virus which fills in the empty spaces of a file with viruses. It is known as cavity virus. It will neither affect the size of the file nor can be detected easily.

10. **Macro Virus:** A virus written in the same macro language as used in the software program and infects the computer if a word

processor file is opened. Mainly the source of such viruses is via emails.

Examples of Computer Viruses

Some of the known viruses are:

a. Trojan horse virus
b. Sleeper
c. Logic bomb Alabama virus
d. Christmas virus
e. Jerusalem virus
f. Resident virus
g. Nonresident virus
h. Code Red
i. I love you
j. Creeper virus
k. Stone
l. November 17

2.4.3 Sources of Computer Virus and Warning signs

These are the means through which viruses could be spread from one system to the other.
i. Infected memory devices
ii. E-mails attachments
iii. Internet downloads
iv. Computer network
v. Illegal duplication of software/cracked software
vi. Unsecured websites

3.5.4 Virus detection and Preventive Measures
Anti-viruses are also written programs by software developers to stop and curb the spread of the virus in a system. Antivirus software is a type of utility software used for scanning and removing viruses from your computer. Once an anti-virus is installed on a system, it will be hard for a virus to enter the system except if the antivirus is outdated. All antivirus can be updated on the internet.
Examples of Antivirus Programs
Computer Antivirus programs include:
i. Norton Anti-virus
ii. McAfee
iii. AVG
iv. Bitdefender
v. Panda Dome
vi. Trend Micro

vii. Malwarebytes
viii. Avira Prime
ix. Intego
x. TotalAV
xi. Bitdefender Total Security
xii. Dr Solomon's Tool Kit
xiii. Penicillin
xiv. Avast
xv. Windows Defender
xvi. Kaspersky

2.4.4 Computer Virus Preventive Measures

Computer virus preventive measures include:
1. Install a good Computer Antivirus.
2. Timely update of the operating system.
3. Timely update of antivirus software
4. Installation of only trusted or licensed software
5. Exercise care when browsing the internet

Self-Assessment Exercise(s)

1.	Why should DDoS attacks worry cybersecurity professionals?
2.	What role do botnets play in DDoS?
3.	Why are DDoS attacks so hard to stop with traditional forms of cybersecurity filtering?
4.	What is the Creeper Virus?

2.5 Summary

At the end of this unit, you will be able to define Denial-of-Service attack, its types and possible countermeasure against it.

You have learnt from this unit the definition of DoS is the kind of attack that has cause disruptions over the years.

2.6 References/Further Readings/Web Resources

Chad Kime (2022). Complete Guide to the Types of DDoS Attacks

Computer Virus and its Types. Retrieved from https://byjus.com/govtexams/computer-virus

COMPUTER VIRUS Retrieved from https://cmpnote.blogspot.com/p/computer-viruses.html

Denial of Service Attacks and its Types. Retrieved from https://www.greycampus.com/opencampus/ethicalhacking/denial-of-service-attacks-and-its-types

Difference between Computer Virus and Computer Worms. Retrieved from https://www.geeksforgeeks.org/difference-between-wormsand-virus/

Lorenzo CARTE (2024). What is a DoS Attack? Types, Exploitations and Security Tips. Retrieve from https://www.vaadata.com/blog/what-is-a-dos-attack-types-exploitations-and-security-tips

Nathan Mahr and Monica Gragg (2023). Computer Virus, Types & Protection

Naveen (2024). Denial-of-Service (DoS) Attack - What is, Types, and Prevention. Retrieved from https://intellipaat.com/blog/what-is-adenial-of-service-attack-dos

Pranav Bhardwaj (2021). Denial-of-Service (DoS) Attack and its Types. Retrieved from https://www.tutorialspoint.com/denial-of-servicedos-attack-and-its-types

What is a DoS Attack? Types, Exploitations and Security. Retrieved from https://www.vaadata.com/blog/what-is-a-dos-attack-typesexploitations-and-security-tips

Possible Answers to Self-Assessment Exercises

Why should DDoS attacks worry cybersecurity professionals?

Answer to SAE 1

DDoS attacks can wreak havoc on the availability of profitable online resources and can also serve as a diversionary tactic to carry out other illicit activities elsewhere on the network.

What role do botnets play in DDoS?

Answer to SAE 2

Botnets are criminally controlled networks of compromised machines. Sometimes referred to as bots or as zombies, these compromised machines can be laptops, desktops, servers, or even IoT devices. Attackers coordinate these machines to create distributed sources of attack traffic to overwhelm an organization infrastructure.

Why are DDoS attacks so hard to stop with traditional forms of cybersecurity filtering?

Answer to SAE 3

The distributed nature of DDoS makes it hard to block the flood of malicious traffic by turning off any one specific spigot.

What is the Creeper Virus?

Answer to SAE 4

Creeper virus was the first-ever computer virus that was released in the year 1971. Its creator was Bob Thomas.

Unit 3 Transfer of Funds/Value Across Networks

Unit Structure

3.1 Introduction

The advent of technology has brought about digital banking, online investment platforms, electronic payment systems, and other internet-based financial services. This digital transformation has made financial services more accessible and convenient. However, the shift to digital platforms has also introduced new challenges, particularly in terms of cybersecurity. Financial institutions handle a huge amount of money and sensitive data, making them an attractive target for cyber criminals.

3.2 Learning outcomes

By the end of this unit, students will be able to:

- explain threats faced by financial institutions during transfer of funds
- identify Common Cybersecurity Threats in Financial Services

3.3 Transfer of Funds/value across networks

3.3.1 Transfer of Funds attack in financial institutions

Funds transfer fraud is a common cyber-attack in which hackers redirect funds from a victim's account before or during a money transfer so that the fraudsters receive the payment instead of the intended recipient. The computer fraud scheme often involves an attacker impersonating an executive, vendor, or bank — and sending fake invoices or payment

instructions. If the sender doesn't verify the information or realize the scam, the criminals usually close their bank accounts within days, making the money difficult to recover. Fraudulent transfers are often immediately transferred to cryptocurrency wallets and quickly dispersed, making recovery efforts impossible. Adding to these costs, the actual vendors who failed to receive payments or were instructed to send fraudulent funds on behalf of the organization will demand to be paid or reimbursed immediately.

Financial services encompass a broad range of businesses that manage money, including credit unions, banks, credit card companies, insurance companies, consumer finance companies, stock brokerages, investment funds, and some government-sponsored enterprises. These institutions play a critical role in the global economy, facilitating transactions, offering credit, and enabling individuals and entities to invest and grow wealth.

3.3.2 Common Cybersecurity Threats in Financial Services

Among several cybersecurity threats in financial institutions are:
Phishing and Social Engineering Attacks

Phishing and social engineering attacks are common cybersecurity threats in the financial services sector. In these attacks, cybercriminals trick individuals into revealing their personal or financial information, often by impersonating a trusted entity. For instance, they might send an email posing as the individual's bank, asking them to update their account details or to confirm a transaction.

Several cybersecurity measures can help protect against these attacks. These include educating customers about the risks of phishing and social engineering attacks, implementing email filtering systems to block phishing emails, and using multi-factor authentication to prevent unauthorized access even if login credentials are compromised.

Malware and Ransomware
Malware, including ransomware, is another common cybersecurity threat in the financial services sector. Malware is malicious software that can disrupt computer operations, gather sensitive information, or gain unauthorized access to computer systems. Ransomware, a type of malware, encrypts files on a system and demands a ransom for their decryption.

These threats can be addressed by robust malware protection. This includes regularly updating and patching systems to fix vulnerabilities, installing and updating antivirus software, monitoring network traffic for

signs of malware, and regularly backing up data to mitigate the impact of ransomware attacks.

Distributed Denial of Service (DDoS) Attacks
In a Distributed Denial of Service (DDoS) attack, cybercriminals overwhelm a network, service, or infrastructure with traffic, causing it to become inaccessible. Financial institutions may be targeted by DDoS attacks to disrupt their services, cause financial losses, or as a distraction while the attackers attempt to breach their systems.

Financial services companies can combat DDoS attacks through various measures. These include implementing DDoS protection systems that can detect and mitigate DDoS traffic, maintaining redundant systems to ensure availability even in case of an attack, and planning for DDoS incidents to ensure a swift and effective response.

Insider Threats
Insider threats refer to cybersecurity threats that originate from within the organization. These could be employees, contractors, or any other individuals who have authorized access to the institution's systems and data. Insider threats can be particularly challenging to address, as these individuals often have legitimate access and may understand the institution's systems and processes.
To protect against insider threats, financial services companies focus on access control, monitoring, and training. It ensures that individuals only have access to the data and systems they need for their work, monitors for unusual or suspicious behavior, and trains staff to recognize and respond to cybersecurity risks.

API Vulnerabilities
Application Programming Interfaces (APIs) are used in the financial sector to enable integration between different systems and services. However, if not properly secured, APIs can be exploited by cyber criminals to gain unauthorized access to systems and data.
API vulnerabilities can be addressed by implementing secure coding practices, conducting regular security testing, and using API security gateways. Another important measure is to monitor API activity, detect and respond to any signs of a breach.

3.3.3 Cybersecurity solutions for Financial Services

Financial institutions use an array of cybersecurity solutions to protect their services and customer data from cyberattacks. Here are some of the most important defensive measures:

1. **Web Application Firewalls**

   A WAF is a protective shield placed between a web application and the Internet. It monitors, filters, and blocks data packets as they travel to and from a website or web application. By implementing a WAF, financial institutions can prevent common web-based attacks such as cross-site scripting (XSS), SQL injection, and brute force attacks.

   A WAF operates through a set of rules called policies. These policies dictate what traffic should be blocked and what should be allowed through. It's important for financial institutions to continually update these policies to stay ahead of emerging threats. Regular security audits can help in identifying areas of vulnerability and updating WAF policies accordingly.

2. **DDoS Protection**

   In a DDoS attack, cybercriminals overwhelm a network, service, or server with a flood of Internet traffic. This can cause services to slow down or crash, leading to significant business disruption.

   DDoS protection solutions can help financial institutions mitigate the risk of DDoS attacks. These solutions monitor network traffic and identify unusual spikes in activity that may indicate a DDoS attack. Once detected, the DDoS protection solution reroutes suspicious traffic away from the network, thus minimizing disruption.

3. **Anti-Fraud and Online Fraud Prevention**

   Online fraud is a pervasive issue in the financial services sector. Fraudsters use various techniques, such as phishing, identity theft, and card fraud, to steal valuable financial information.

   Anti-fraud solutions can help financial institutions detect and prevent fraudulent activity. These solutions use advanced analytics and machine learning algorithms to identify suspicious patterns and behaviors that may indicate fraudulent activity. By detecting fraud in real-time, financial institutions can take immediate action to prevent financial loss.

4. **Identity and Access Management (IAM)**

   and access management (IAM) is a framework for business processes that facilitates the management of electronic identities. It includes the technology needed to support identity management, such as multi-factor authentication (MFA), single sign-on (SSO), and user provisioning.

   IAM ensures that the right individuals have access to the right resources at the right times for the right reasons. It plays an essential role in preventing unauthorized access to sensitive data

and systems. Financial institutions can leverage IAM to implement strict access controls, thereby minimizing the risk of data breaches.

5. **Advanced Threat Protection Solutions**
   ATP solutions use a combination of technologies, such as endpoint protection, network security, email security, and malicious behavior analytics, to detect and prevent sophisticated cyber threats. These solutions provide real-time threat intelligence and automated response capabilities. By detecting and neutralizing threats before they can cause harm, ATP solutions play a crucial role in safeguarding financial institutions from advanced cyber threats.
6. **Vulnerability Assessment and Penetration Testing (VAPT)**
   VAPT involves identifying, quantifying, and prioritizing vulnerabilities in a system. It is a comprehensive assessment designed to detect weaknesses and evaluate the security posture of a system. In the context of financial services, VAPT helps to secure critical data, prevent data breaches, and meet regulatory compliance. It is a proactive approach towards cybersecurity, where potential threats are identified and neutralized before they can cause any damage.
7. **Security Awareness and Training Programs**
   Even the most sophisticated cybersecurity solutions can be rendered useless if the end-users are not aware of the cyber threats and how to counter them. Security awareness and training programs aim to educate the users about the various cyber threats, their modus operandi, and the best practices to counter them. In the context of financial services, these training programs are particularly important. They not only help to protect sensitive financial data but also instill confidence in the users of digital financial solutions.
8. **Data Activity Monitoring**
   In the financial services industry, unauthorized access or manipulation of data can lead to disastrous consequences. Data activity monitoring is a technology that monitors and records all activities on a database in real-time. In the context of financial services, data activity monitoring provides an additional layer of security. It not only helps to protect against external threats but also internal threats, which can often be overlooked. By keeping a close watch on all data activities, it ensures the integrity and confidentiality of the financial data.
9. **Data Risk Analytics**
   Data risk analytics is a proactive approach towards cybersecurity. It involves analysing the data to identify potential risks and threats. This analysis is done using advanced algorithms and

machine learning techniques, which can detect patterns and anomalies that may indicate a cyber threat. In the context of financial services, data risk analytics provides a strategic edge. By predicting potential threats, it allows for proactive risk management. It also helps to maintain regulatory compliance by providing an objective assessment of the data risks.

Self-Assessment Exercises

Mention the importance of cybersecurity in financial institutions

3.4 Summary

At the end of this unit, you will be able to define transfer of funds over networks and the various attacks associated with it.

You have learnt from this unit the various attacks associated with transfer of funds across networks

3.5 References/Further Readings/Web Resources

https://www.coalitioninc.com/topics/what-is-funds-transfer-fraud

https://www.imperva.com/learn/data-security/financial-servicescybersecurity/

3.4 Possible Answers to Self-Assessment Exercise

Mention the importance of cybersecurity in financial institutions
Answer
Here are a few reasons cybersecurity is critical for financial services companies:

1. **Sensitive Data Protection**
   Financial institutions handle a vast amount of personal and financial information, including customers' names, addresses, social security numbers, credit card details, and transaction histories. This data is not just valuable to the customers but also to cybercriminals who use it for fraudulent activities.

   Financial services organizations deploy various cybersecurity tools to protect sensitive financial data. From encryption and secure networks to robust authentication mechanisms, cybersecurity ensures that the data is only accessible to authorized individuals and systems. It also provides mechanisms to detect and respond to any unauthorized access or data breaches, minimizing the potential damage
2. **Prevention of Financial Loss**
   Cyber-attacks can lead to significant financial losses. Not only can cybercriminals steal money directly from bank accounts or use stolen credit card details for fraudulent transactions, but data breaches can result in regulatory fines, legal costs, and reputational damage. The cost of cybercrime in the financial services industry continues to increase.
   Cybersecurity for financial services is instrumental in preventing losses. Through network security, intrusion detection systems, malware protection, and other cybersecurity measures, financial institutions can prevent cyber-attacks and mitigate their impact.
3. **Maintaining Consumer Trust**
   Trust is the cornerstone of the financial services industry. Customers entrust their money and personal data to financial institutions, expecting them to keep it safe. Any breach of this trust, such as a data breach or a successful cyber-attack, can severely damage a financial institution's reputation and customer relationships. By protecting financial transactions and customer data, cybersecurity in financial services helps maintain consumer trust. It reassures customers that their data and money are safe, fostering confidence in the financial institution's services.

4. Regulatory Compliance

Financial institutions operate within a stringent regulatory environment that sets guidelines to ensure the security and integrity of financial systems and protect consumers. These include regulations such as the Bank Secrecy Act (BSA), Dodd-Frank Act, Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS), among others. These regulations mandate a variety of cybersecurity measures. For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires businesses to secure cardholder data, implement robust access control measures, maintain an information security policy, and regularly test and monitor networks.

MODULE 6 OPERATING SYSTEM AND NETWORK SECURITY

Introduction

In module 5, you have learnt about cyber-attack and defence mechanisms against various attacks. In this module, I will take you through operating system protection mechanisms against cyber threats, ways of detecting intrusions of attacks methods of securing networks and distributed systems.

This module is classified into the following two (2) units:

Unit 1 Operating System Protection Mechanisms
Unit 2 Intrusion Detection Systems

In each unit, related topics was explored in detail and self-assessment exercises was treated at the end of each unit. Finally, resources for further readings were captured at the end of each unit.

Unit 1 Operating System Protection Mechanisms

Unit Structure

1.1 Introduction

System protection in an operating system refers to the mechanisms implemented by the operating system to ensure the security and integrity of the system. System protection involves various techniques to prevent unauthorized access, misuse, or modification of the operating system

and its resources such as user authentication, access control, encryption, antivirus software and so on.

1.2 Learning Outcomes

By the end of this unit, you will be able to:

- define protection.
- understand the needs for protection
- understand the role of protection
- mention advantages and disadvantages of System Protection in an operating System
- understand various ways in which an operating system can provide system protection

1.3 Operating System Protection Mechanisms

1.3.1 Definition of System Protection

System Protection refers to a mechanism which controls the access of programs, processes, or users to the resources defined by a computer system. It can also be defined as a technique for protecting data and processes from harmful or intentional infiltration. It contains protection policies either established by itself, set by management or imposed individually by programmers to ensure that their programs are protected to the greatest extent possible. We can take protection as a helper to multi programming operating system, so that many users might safely share a common logical name space such as directory or files.

1.3.2 Role of System Protection in Operating System Mechanisms

The role of system protection is to provide a mechanism that implement policies which defines the uses of resources in the computer system. Some policies are defined at the time of design of the system, some are designed by management of the system and some are defined by the users of the system to protect their own files and programs.

Every application has different policies for use of the resources and they may change over time so protection of the system is not only concern of the designer of the operating system. Application programmer should

also design the protection mechanism to protect their system against misuse.

Policy is different from mechanism. Mechanisms determine how something will be done and policies determine what will be done. Policies are changed over time and place to place. Separation of mechanism and policy is important for the flexibility of the system.

1.3.3 Advantages and Disadvantages of System Protection in Operating

Advantages

i. Ensures the security and integrity of the system
ii. Prevents unauthorized access, misuse, or modification of the operating system and its resources
iii. Protects sensitive data
iv. Provides a secure environment for users and applications
v. Prevents malware and other security threats from infecting the system
vi. Allows for safe sharing of resources and data among users and applications
vii. Helps maintain compliance with security regulations and standards

Disadvantages

i. It can be complex and difficult to implement and manage
ii. It may slow down system performance due to increased security measures
iii. It can cause compatibility issues with some applications or hardware
iv. It can create a false sense of security if users are not properly educated on safe computing practices
v. It can create additional costs for implementing and maintaining security measures.

1.3.4 Ways in which an Operating System can Provide System Protection

There are several ways in which an operating system can provide system protection:

User authentication: The operating system requires users to authenticate themselves before accessing the system. Usernames and passwords are commonly used for this purpose.

Authentication refers to identifying each user of the system and associating the executing programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic. Operating Systems generally identifies/authenticates users using following three ways

Username/Password: User need to enter a registered username and password with Operating system to login into the system.
User card/key − User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.

User attribute/fingerprint/ eye retina pattern/ signature: User need to pass his/her attribute via designated input device used by operating system to login into the system.

Access control: The operating system uses access control lists (ACLs) to determine which users or processes have permission to access specific resources or perform specific actions.

Encryption: The operating system can use encryption to protect sensitive data and prevent unauthorized access.

Firewall: A firewall is a software program that monitors and controls incoming and outgoing network traffic based on predefined security rules.

Antivirus software: Antivirus software is used to protect the system from viruses, malware, and other malicious software.

System updates and patches: The operating system must be kept up-to-date with the latest security patches and updates to prevent known vulnerabilities from being exploited.

By implementing these protection mechanisms, the operating system can prevent unauthorized access to the system, protect sensitive data, and ensure the overall security and integrity of the system.

Self-Assessment Exercise(s)

1. Highlight the need for protection in operating systems

1.4 Summary

At the end of this unit, you will have familiarised yourself with the meaning, roles as well as advantages and disadvantages of system protection in operating system.

In this unit, you have learnt what system protection is all about and its importance as well as ways of protecting our systems against malicious effects.

1.5 References/Further Readings/Web Resources

Peter Reiher (2022). Introduction to Operating System Security. Retrieved from https://pages.cs.wisc.edu/~remzi/OSTEP/security-intro.pdf

Silberschatz, Galvin, Gagne (2009). Operating Systen Concepts. 8th Edition. Retrieved from https://www.mbit.edu.in/wpcontent/uploads/2020/05/Operating_System_Concepts

Trent Jaeger (2023). Operating System Security (Synthesis Lectures on Information Security, Privacy, and Trust) 1st Edition. Retrieved from https://www.amazon.com/Operating-Security-Synthesis-Lectures-Information

1.6 Possible Answers to Self-Assessment Exercise(s)

Highlight the need for protection in operating systems

Answer to SAE

Need for Protection

Various needs of protection in the operating system are as follows:

i. To prevent the access of unauthorized users
ii. To improve reliability by detecting latent errors.
iii. It is important to ensure no access rights' breaches, no viruses, no unauthorized access to the existing data.
iv. To ensure that each active programs or processes in the system uses resources only as the stated policy

Unit 2 Intrusion Detection Systems

Unit Structure

2.1 Introduction

Intrusion Detection System (IDS) is a vital security component that monitors network and host activity to identify potential intrusions or malicious activities. By analysing network traffic, logs, and system events, IDS helps organizations detect and respond to cyber threats in real time. It provides early warning signs of unauthorized access, suspicious behavior, or known attack signatures, enabling prompt action to mitigate risks.

IDS enhances overall network security, reducing the likelihood of successful attacks and minimizing potential damage. As cyber threats continue to evolve, an effective IDS plays a crucial role in protecting sensitive information, maintaining business continuity, and safeguarding digital assets.

2.2 Learning Outcomes

By the end of this unit, you should be able to:

- define an intrusion in cybersecurity.
- explain intrusion detection system.
- describe major components of an intrusion detection system.
- explain how intrusion detection system work.

- understand types of intrusion detection system.

2.3 Intrusion Detection System.

3.1 Definition of Intrusion Detection System

Intrusion is typically scenario of an attacker gaining unauthorized access to a device, network, or system. Cyber criminals use increasingly sophisticated techniques and tactics to infiltrate organizations without being discovered. This includes common techniques like:

Address spoofing: The source of an attack is hidden using spoofed, misconfigured, and poorly secured proxy servers, which makes it difficult for organizations to discover attackers.

Fragmentation: Fragmented packets enable attackers to bypass organizations' detection systems.

Pattern evasion: Hackers adjust their attack architectures to avoid the patterns that IDS solutions use to spot a threat.

Coordinated attack: A network scan threat allocates numerous hosts or ports to different attackers, making it difficult for the IDS to work out what is happening.

An Intrusion Detection System (IDS) is a security system that monitors network traffic for signs of unauthorized access, misuse, or compromise. It is designed to detect suspicious activities and respond to security threats in real-time to provide additional layers of protection beyond traditional firewalls and antivirus software. Based upon this alert the network administrator or IT personnel can take a proactive measure to prevent the attack.

2.3.2 Major Components of Intrusion Detection System

The major components of IDS include the following:

1. **Sensors**: Sensors monitor network traffic, system logs, and other data sources for suspicious activity. They are the first component of an IDS. These sensors, can either be host- or network-based. They provide alerts when potential breaches are detected.
2. **Analysis Engine:** After the sensors generate alerts, the IDS's analysis engine examines them to determine whether they reflect actual threats. To identify potential threats, this component uses

various techniques like signature-based detection, anomaly detection, and behavioral analysis.

3. **Central Console:** The central console is the IDS component is responsible for receiving and managing warnings from sensors and the analysis engine. The security team can view and manage alerts, investigate problems, and respond appropriately.
4. **Response Mechanism:** Finally, an IDS should provide a reaction mechanism for dealing with discovered threats to mitigate the effects of the intrusion. This can include restricting traffic, quarantining affected systems, or triggering automated actions.

2.3.3 How Does an Intrusion Detection System Operate?

The primary goal of an IDS is to detect and alert system administrators or security personnel about suspicious or unauthorized behavior within a network or system.

The general IDS implementation involves the following steps:

An Intrusion Detection System (IDS) is employed to actively observe the flow of traffic within a computer network, with the primary objective of identifying any potentially suspicious actions or events.

By thoroughly scrutinizing the data traversing the network, the IDS employs analytical techniques to discern discernible patterns and detect indications of abnormal behavior.

To achieve this, the IDS employ a collection of predefined rules and patterns, against which the network activity is meticulously compared.

This process aids in the identification of any activity that may potentially signify an ongoing attack or unauthorized intrusion.

Whenever the IDS encounters an activity that aligns with any of the established rules or patterns, it promptly generates an alert and promptly relays it to the designated system administrator.

Upon receipt of the alert, the system administrator assumes responsibility for investigating the reported incident, subsequently initiating appropriate measures to prevent any detrimental consequences or further compromise to the system.

2.3.4 Types of Intrusion Detection System

Among various types of Intrusion Detection System are:

1. **Network intrusion detection system (NIDS):** This IDS is a reliable security solution that effectively monitors network and detects malicious and suspicious traffic coming to and going from all devices connected to the network.
2. **Host-Based IDS**: A Host-Based IDS is a security tool that focuses on monitoring the activity of a single host or endpoint device. By keeping a close eye on the host, this IDS can effectively detect and identify various types of attacks, such as unauthorized file modifications, attempts to gain elevated privileges, and suspicious network connections.
3. **Signature-Based IDS:** A Signature-Based IDS is a security system that identifies known patterns or signatures of malicious activity within network traffic or system logs. A SIDS solution monitors all packets on an organization's network and compares them with attack signatures on a database of known threats. This approach effectively detects well-known attacks but may struggle with detecting new or unknown threats.
4. **Anomaly-Based IDS:** Anomaly-Based IDS is a type of intrusion detection system that identifies abnormal behavior within a network or system. It establishes a baseline of normal activities and then monitors for deviations from this baseline. By analysing patterns and deviations, it can detect unknown or novel attacks that may evade traditional signature-based detection methods. This approach enhances the ability to identify complex and evolving threats.
5. **Hybrid IDS:** Hybrid IDS combines the features of both network-based and host-based IDS. It monitors network traffic for signs of intrusions, such as suspicious patterns or known attack signatures, while also analysing activity on individual hosts. This comprehensive approach allows for a more robust detection and intrusion prevention system for various types of network attacks.
6. **Perimeter Intrusion Detection System (PIDS):** A PIDS solution is placed on a network to detect intrusion attempts taking place on the perimeter of organizations' critical infrastructures.
7. **Virtual Machine-based Intrusion Detection System (VMIDS):** A VMIDS solution detects intrusions by monitoring virtual machines. It enables organizations to monitor traffic across all the devices and systems that their devices are connected to.
8. **Stack-based Intrusion Detection System (SBIDS):** SBIDS is integrated into an organization's Transmission Control Protocol/Internet Protocol (TCP/IP), which is used as a communications protocol on private networks. This approach enables the IDS to watch packets as they move through the

organization's network and pulls malicious packets before applications or the operating system can process them.

2.3.4 Benefits of Intrusion Detection System (IDS)

Intrusion Detection Systems (IDS) offer several benefits for enhancing the security posture of networks and systems. Some of the key benefits of IDS include:

1. **Malicious Activity Detection:** An Intrusion Detection System (IDS) has the capability to identify and detect any potentially harmful activities or behaviors within a system, thereby notifying the system administrator promptly to prevent substantial damage.
2. **Network Performance Enhancement**: By recognizing and pinpointing performance problems within a network, an IDS can facilitate the identification and resolution of such issues, leading to improved overall network performance.
3. **Compliance Fulfillment:** Through continuous monitoring of network activity and generating comprehensive reports, an IDS assists organizations in meeting compliance requirements, ensuring adherence to relevant regulations and standards.
4. **Provision of Valuable Insights:** Utilizing its ability to analyse network traffic, an IDS generates valuable insights that aid in the identification of vulnerabilities or weaknesses, thus facilitating the enhancement of network security.
5. **Threat Intelligence:** Organizations can receive threat intelligence from IDS to enhance their understanding of the types of attacks and threats they encounter. They can utilize this information to fortify security policies and procedures, develop new security controls, and enhance the overall security posture.
6. **Incident Response:** IDS can give useful data for incident response activities. When a security incident happens, IDS can assist security teams in determining the breadth and impact of the incident and provide information on the sorts of attacks deployed. This information can assist organizations in better understanding the situation and taking relevant mitigation measures.
7. **Continuous Monitoring:** IDS provides continuous monitoring of network traffic and system behavior, which is essential for identifying sophisticated and persistent threats. By monitoring unusual activity over time, IDS can detect attacks that may otherwise go unnoticed.

Self-Assessment Exercises 1

State benefits of Intrusion Detection System (IDS)

2.3.6 Intrusion Detection System Using Machine Learning

Machine Learning (ML) can be used to build more effective IDSs, which have the following advantages:

- **Ability to Detect Unknown Attacks:** ML models can detect intrusions based on anomalous patterns in network traffic, not just known signatures. This allows them to detect new and unknown attacks.
- **Higher Detection Accuracy**: ML models can be trained on large amounts of labeled data to improve their ability to detect intrusions with fewer false alarms accurately.
- **Automated Feature Engineering:** ML algorithms can automatically extract relevant features from network traffic to represent as input data. This reduces the manual feature engineering efforts.
- **Adaptability**: Machine Language models can continuously learn from new data to adapt to the changing network environments and attack techniques. They become "smarter" over time.

2.3.7 Intrusion Detection System in Cryptography

Intrusion Detection System can play a role in cryptography by helping to detect attacks on cryptographic systems and alert security teams to potential security breaches. Mentioned below are some ways in which IDS can be used in cryptography:

- **Detection of Cryptographic Attacks:** IDS detects cryptographic system attacks, including brute-force, dictionary, and other types of attacks that attempt to overcome encryption. It also detects assaults on the key management systems utilized to secure cryptographic keys. By identifying these assaults early, IDS actively aids in preventing the loss of sensitive information and safeguarding the integrity of cryptographic systems.
- **Monitoring of Cryptographic Systems:** IDS can detect anomalous behavior in cryptographic systems, such as unauthorized access or changes to cryptographic settings. This can aid in detecting the attempts to bypass or weaken encryption or even change cryptographic parameters to compromise system

2.3.8 Intrusion Detection System in Network Security

IDS actively monitors network traffic to detect signs of unauthorized access, malicious activities, or intrusion attempts and plays a vital role in

network security. By identifying potential threats, it takes appropriate actions to mitigate them. Let's explore how an IDS functions within the context of network security:

i. **Network Traffic Monitoring**: In real time, an IDS actively monitors network traffic to analyse packets, headers, and payloads to gain visibility into the network's activity. It inspects the flowing data and examines it for any signs of suspicious or abnormal behavior.
ii. **Intrusion Detection**: IDS compares the network traffic against a set of predefined rules, known as signatures, to identify known attack patterns. These signatures are based on known vulnerabilities, attack methods, or malicious activities. If a match is found, the IDS triggers an alert to indicate a potential intrusion attempt.
iii. **Anomaly Detection:** In addition to signature-based detection, an IDS can utilize anomaly detection techniques, as well. It establishes a baseline of normal network behavior by monitoring patterns, statistics, and metrics over time. Deviations from this baseline are flagged as potential anomalies that might indicate an ongoing intrusion or a novel attack.
iv. **Alert Generation:** When an IDS detects an intrusion attempt or suspicious activity, it generates alerts or notifications. These alerts typically contain information about the nature of intrusion, the affected systems or hosts, and the severity level. The alerts are sent to security administrators or a Security Operations Center (SOC) for further investigation and response.

Organizations can enhance their ability to detect and respond to potential threats, minimize the risk of unauthorized access, and safeguard critical assets and data by deploying an IDS in their network security infrastructure.

2.4 Summary

In this unit, I explored the definition of intrusion detection system, its benefits, how it works and its role in cryptography, network security and machine learning.

In this unit, you have learnt what intrusion detection system is all about and its importance in cybersecurity.

2.5 References/Further Readings/Web Resources

Karen Scarfone (NIST), Peter Mell (NIST) (2010). Intrusion Detection and Prevention Systems. Retrieved from https://csrc.nist.gov/pubs/book-section/2010/10/intrusion-detection-and-prevention-systems

Luigi V. Mancini, Roberto Piero (20024). Retrieved from https://link.springer.com/book/Intrusion-dectection-system

2.6 Possible Answers to Self-Assessment Exercise

State benefits of Intrusion Detection System (IDS)

Answer

Intrusion Detection Systems (IDS) offer several benefits for enhancing the security posture of networks and systems. Some of the key benefits of IDS include:

i. Malicious Activity Detection
ii. Network Performance Enhancement
iii. Compliance Fulfilment
iv. Provision of Valuable Insights
v. Threat Intelligence
vi. Incident Response
vii. Continuous Monitoring

Module 7 Vulnerabilities and Counter Measures

Introduction

Before identifying specific dangers to modern data systems, it is crucial to understand the distinction between cyber threats and vulnerabilities.

The purpose of this Software Security chapter is to provide a structured overview of known categories of software implementation vulnerabilities, and of techniques that can be used to prevent or detect such vulnerabilities, or to mitigate their exploitation.

Unit 1 Software Application Vulnerabilities
Unit 2 Formal Models of Security
Unit 3 Countermeasures employed by organisations and agencies

In each unit, each topic is explored in details and self-assessment exercises were highlighted at the end of the unit. Resources for further reading are highlighted at the end of each unit as well.

Unit 1 Software Application Vulnerabilities

Unit Structure

1.1 Introduction

From this unit, you will be expose to the definition and general concepts of System Application Vulnerabilities. After studying this unit, you will have the general understanding of how to manage, transmit, stores, or otherwise handles data in order to institute and enforce mechanisms to monitor their cyber environment, identify vulnerabilities, and close up security holes as quickly as possible.

1.2 Learning Outcomes

By the end of this unit, you will be able to:

- define application vulnerabilities
- explain application vulnerabilities
- understand how to protect software applications against cyber threats using Application security.

1.3 Software Application Vulnerabilities

1.3.1 Definition of Application Vulnerability?

Application vulnerabilities are mostly the weaknesses encountered in an application that an attacker can employ to harm the security of an application. There are many ways/ approaches through which vulnerabilities could be introduced to an application among which are: failures in design implementation, configuration of an application etc.

A software vulnerability is a defect in software that could allow an attacker to gain control of a system. Among the defects that cause software vulnerabilities can result from flaws in the way the software is designed, problems with the software's source code, poor management of data or access control settings within the application or any other type of issue that attackers could potentially exploit.

Vulnerabilities are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them.
Vulnerabilities are weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Cyber threats are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.

Examples of common types of security threats include phishing attacks that result in the installation of malware that infects your data, failure of a staff member to follow data protection protocols that cause a data breach, or even a tornado that takes down your company's data headquarters;

- Disrupting access.
- Categories of vulnerabilities

- Corrupted (Loss of integrity)
- Leaky (Loss of confidentiality)
- Unavailable or very slow (Loss of availability)

Threats: Threats represent potential security harm to an asset when vulnerabilities are exploited
Attacks: Attacks are threats that have been carried out
Passive: Make use of information from the system without affecting system resources
Active: Alter system resources or affect operation
Insider: Initiated by an entity inside the organisation
Outsider: Initiated from outside the perimeter

Self-Assessment Exercises 1

1.	What is Application Vulnerability?
2.	What is Cyber threat?

1.3.2 Common Application Vulnerabilities

Application security are the soft spots or the easiest part of software that intruders want to penetrate. The vulnerabilities could be lurking anywhere, including lines of code, the design backbone or the third-party tools in the application. Using these soft spots can lead vulnerabilities such as unauthorised access, modification of application functionalities, theft of data and or application shutdown.

According to Open Web Application Security Project (**OWASP)**, the Ten (10) list of vulnerabilities that can help the development teams to mitigate the risk of application vulnerability as published in 2021 as from 2017 are:

The top 10 application vulnerabilities as from the 2017 list are as follows:

1. **Injection:** Injection vulnerabilities can occur when a query or command is used to insert untrusted data into the interpreter via SQL, OS, NoSQL, or LDAP injection. The hostile data injected through this attack vector tricks the interpreter to make the application do something it was not designed for.
2. **Broken authentication:** When applications incorrectly execute functions related to session management or user authentication, intruders may be able to compromise passwords, security keys, or session tokens and permanently or temporarily assume the identities and permissions of other users.

3. **Sensitive data exposure:** Without essential data protection measures including the encryption of data in transit or at rest, attackers can view, steal, or modify sensitive data or Personally Identifiable Information (PII) such as credentials, credit card or social security numbers, and medical information. Unencrypted data is a prime target for damaging exploits related to identity theft, fraud, and industrial espionage, to name just a few securities vulnerability examples.
4. **XML External Entities (XXE):** For web applications that parse Extended Markup Language **(**XML**)** input, a poorly configured XML parser can be tricked to send sensitive data to an unauthorized external entity, i.e., a storage unit such as a hard drive. XML External Entity (XXE) attacks are used by hackers to observe critical information, disclose internal files and file shares, scan internal ports, execute code remotely, and mount denial of service (DoS) attacks.
5. **Broken access control:** Broken access control can give website visitors access to admin panels, servers, databases, and other business-critical applications. This OWASP Top 10 threat could be used to redirect browsers to other targeted URLs.
6. **Security misconfigurations:** According to Gartner, up to 95% of cloud breaches are the result of human errors. Security setting misconfigurations are one of the biggest drivers behind that stat. Of the OWASP Top 10, this vulnerability is the most common.
7. **Cross-site scripting (XSS):** Cross-site scripting is also a widespread vulnerability that affects more than half of all web applications. It occurs when malicious client-side JavaScript or HTML scripts are injected into a web page and then use the web application as an attack vector to hijack user sessions, deface websites, or redirect the victim to sites under the attacker's control.
8. **Insecure deserialization:** Insecure deserialization offers hackers an attack vector that is most typically used for remote code execution but can also be used to conduct injection attacks, replay attacks, and attacks utilizing privilege escalation.
9. **Using components with known vulnerabilities:** Modern distributed web applications incorporate open-source components, including libraries and frameworks. Any component with a known vulnerability becomes a weak link that can impact the security of the entire application.
10. **Insufficient logging and monitoring:** The time from attack to detection can take up to 200 days, or sometimes longer. This window gives cyber thieves plenty of time to tamper with servers, corrupt databases, steal confidential information, and plant malicious code if sufficient logging and monitoring is not in place.

Self-Assessment Exercises 2

1.	List ten (10) Application vulnerabilities

1.3.3 Application Security

Application security aims to protect software applications against cyber threats, it is therefore advisable to apply application security during all phases of software development.

Ways to promote application security throughout the software development life cycle is to:

i. introduce security standards and tools during design and application development phases which includes vulnerability scanning during early development
ii. implementation of a strong authentication application which contain sensitive data.
iii. use security systems such as firewalls, intrusion prevention systems and web application firewalls
iv. implementation of security procedures and systems to protect applications in production environment.

1.3.4 Application Security Testing

Application Security Testing (AST) is the process of making applications more resilient to security threats by identifying and remediating security vulnerabilities.

Due to the growing modularity of enterprise software, the huge number of open-source components, and the large number of known vulnerabilities and threat vectors, AST must be automated. Most organisations use a combination of several application security tools.

Static Application Security Testing (SAST)

SAST tools use a white box testing approach, in which testers inspect the inner workings of an application. SAST inspects static source code and reports on security weaknesses.

Static testing tools can be applied to non-compiled code to find issues like syntax errors, math errors, input validation issues, invalid or insecure references. They can also run-on compiled code using binary and byte-code analyzers.

Dynamic Application Security Testing (DAST)

DAST tools take a black box testing approach. They execute code and inspect it in runtime, detecting issues that may represent security vulnerabilities. This can include issues with query strings, requests and responses, the use of scripts, memory leakage, cookie and session handling, authentication, execution of third-party components, data injection, and DOM injection. DAST tools can be used to conduct large-scale scans simulating a large number of unexpected or malicious test cases and reporting on the application's response.

Interactive Application Security Testing (IAST)

IAST tools are the evolution of SAST and DAST tools—combining the two approaches to detect a wider range of security weaknesses. Like DAST tools, IAST tools run dynamically and inspect software during runtime. However, they are run from within the application server, allowing them to inspect compiled source code like IAST tools do.

IAST tools can provide valuable information about the root cause of vulnerabilities and the specific lines of code that are affected, making remediation much easier. They can analyze source code, data flow, configuration and third-party libraries, and are suitable for API testing.

Mobile Application Security Testing (MAST)

MAST tools combine static analysis, dynamic analysis and investigation of forensic data generated by mobile applications. They can test for security vulnerabilities like SAST, DAST and IAST, and in addition address mobile-specific issues like jailbreaking, malicious Wi-Fi networks, and data leakage from mobile devices.

Software Composition Analysis (SCA)

SCA tools help organisations conduct an inventory of third-party commercial and open-source components used within their software. Enterprise applications can use thousands of third-party components, which may contain security vulnerabilities. SCA helps understand which components and versions are actually being used, identify the most severe security vulnerabilities affecting those components, and understand the easiest way to remediate them.

Runtime Application Self-Protection (RASP)

RASP tools evolved from SAST, DAST and IAST. They are able to analyze application traffic and user behavior at runtime, to detect and prevent cyber threats.

Like the previous generation of tools, RASP has visibility into application source code and can analyze weaknesses and vulnerabilities.

It goes one step further by identifying that security weaknesses have been exploited, and providing active protection by terminating the session or issuing an alert.

RASP tools integrate with applications and analyze traffic at runtime, and can not only detect and warn about vulnerabilities, but actually prevent attacks. Having this type of in-depth inspection and protection at runtime makes SAST, DAST and IAST much less important, making it possible to detect and prevent security issues without costly development work.

Application Security Testing Best Practices

Shift Security Testing Left

New organisational practices like DevSecOps are emphasizing the need to integrate security into every stage of the software development lifecycle. AST tools can:

- help developers understand security concerns and enforce security best practices at the development stage.
- help testers identify security issues early before software ships to production.
- advanced tools like RASP can identify and block vulnerabilities in source code in production.

Test Internal Interfaces, not just APIs and UIs

It is natural to focus application security testing on external threats, such as user inputs submitted via web forms or public API requests. However, it is even more common to see attackers exploit weak authentication or vulnerabilities on internal systems, once already inside the security perimeter. AST should be leveraged to test those inputs, connections and integrations between internal systems are secure.

Test often

New vulnerabilities are discovered every day, and enterprise applications use thousands of components, any of which could go end of life (EOL) or require a security update. It is essential to test critical systems as often as possible, prioritize issues focusing on business-critical systems and high-impact threats, and allocate resources to remediate them fast.

Third-party code security

Organisations should employ AST practices to any third-party code they use in their applications. Never "trust" that a component from a third party, whether commercial or open source, is secure. Scan third-party code just like you scan your own. If you discover severe issues, apply patches, consult vendors, create your own fix or consider switching components.

1.4 Summary

At the end of this unit, you have learnt the definition of software application vulnerability, cyber-attack, common Application vulnerabilities, Application security and Application security testing. In the next unit, you will be introduced to formal models of security.

You have learnt from this unit that what a software application vulnerability is and the general way by which our applications can be subjected to vulnerability and how to guide against the future occurrence of vulnerabilities in software application development and usage.

1.5 References/Further Readings/Web Resource

Chris Moschavitis (2018) Cybersecurity Program Development for Business. The Essential Guide, Wiley

Frank Piessens and KU Leuven (2019), Software Security Knowledge Area, Issue 1.0, National Cyber security centre

William Stallings and Lawrie Brown (2018), Computer Security principles and Practice, Pearson.

1.6 Possible Answers to Self-Assessment Exercises

1. *Define Application Vulnerability?*
2. *Define Cyber threat?*

Answers SAEs 1

1. Application Vulnerability is the gaps or weaknesses of a software in a system that make threats possible and tempt threat actors to exploit them.
   It is the software that could allow an attacker to gain control of a system.

2. Cyber threats are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.

List ten (10) Application vulnerabilities

Answers SAEs 2

The ten (10) Application vulnerabilities are as follows:

1. Injection
2. Broken authentication
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken access control
6. Security misconfigurations
7. Cross-site scripting (XSS)
8. Insecure deserialization:
9. Using components with known vulnerabilities
10. Insufficient logging and monitoring

Unit 2 Basic Formal Models of Security

Unit Structure

2.1 Introduction

You will learn from this unit basic formal models of security. After studying the unit, you will be equipped with the skills to identify the different types of formal models of security.

2.2 Learning Outcomes

By the end of this unit, you will be able to:

- identify the different types of Formal Models of Security
- recognise the rules that guide each of the model

2.3 Basic Formal Models of Security

23.1 Definition of Formal Models of Security

Formal models of security are models that are used for maintaining goals of security which are confidentiality, Integrity and Availability. It deals with the CIA Triad Maintenance.

There are 3 main types of Formal Models of security:
i. Bell-LaPadula
ii. Biba
iii. Clarke Wilson Security Model

2.3.2 Basic Classification of Models of Security

The formal models of security can be classified into three (3) main types as discussed above.

1. **Bell-LaPadula**

   Bell-LaPadula model was coined from the name of the two scientists named Elliot Bell and Leonard J. LaPadula who invented it. The model is used to maintain the confidentiality of security. The classification of Subjects (Users) and Objects (Files) are organised in a non-discretionary fashion, with respect to different layers of secrecy.

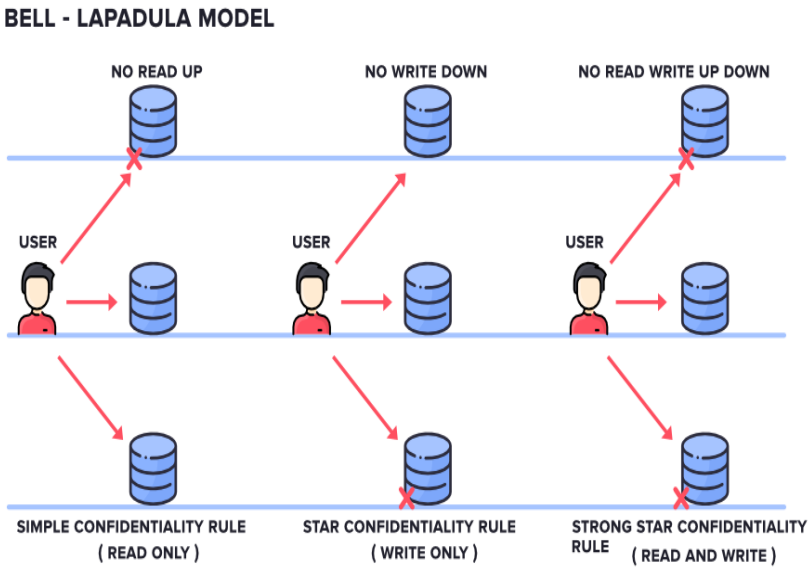


Figure 2.1: Bell-LaPadula Model of Security

Bell-LaPadula has three main rules

- **Simple Confidentiality Rule**: Simple Confidentiality Rule states that the Subject can only Read the files on the Same Layer of Secrecy and the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which this can be called NO READ-UP
- **Star Confidentiality Rule:** Star Confidentiality Rule states that the Subject can only Write the files on the Same Layer of Secrecy and the Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as NO WRITE-DOWN
- **Strong Star Confidentiality Rule:** Strong Star Confidentiality Rule is highly secured and strongest which states that

the Subject can Read and Write the file on the Same Layer of Secrecy only and not the Upper Layer of Secrecy or the Lower Layer of Secrecy, due to which this rule is referred to as NO READ WRITE UP DOWN

2. **Biba Model**

Biba Model was invented by the scientist Kenneth J. Biba and hence the name Biba model. It is used to maintain the Integrity of Security. The classification of Subjects (Users) and Objects (Files) are organised in a non-discretionary fashion, with respect to different layers of secrecy. This works the exact reverse of the Bell-LaPadula Model.

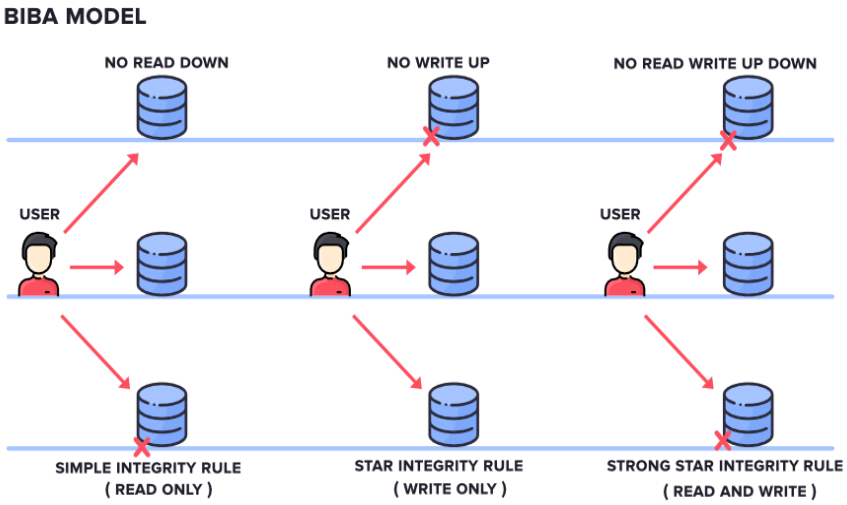


Figure 2.2: Biba model of security

Biba model has three (3) main rules which are:

- **Simple Integrity Rule**: Simple Integrity Rule states that the Subject can only Read the files on the Same Layer of Secrecy and the Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as NO READ DOWN
- **Star Integrity Rule:** Star Integrity Rule states that the Subject can only Write the files on the Same Layer of Secrecy and the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which we call this rule as NO WRITE-UP STRONG STAR INTEGRITY RULE

3. Clarke Wilson Security Model

This Model is a highly secured model. It has the following entities.

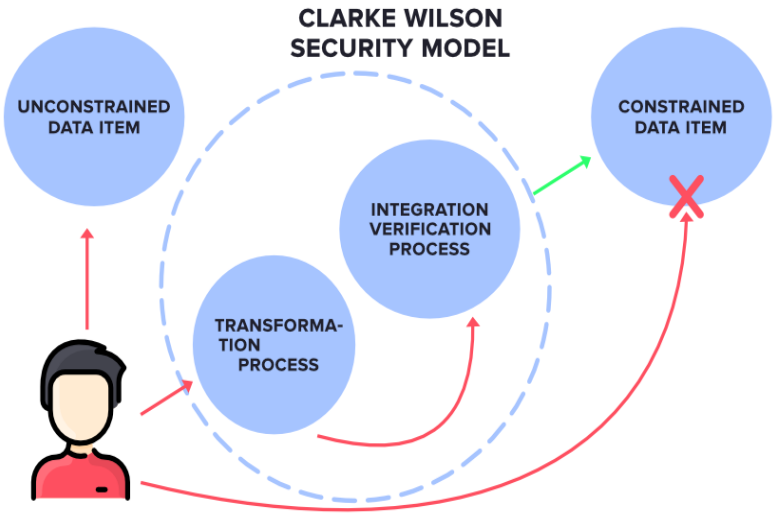


Figure 2.3: Example of Clarke Wilson Security model

- **Subject**: It is any user who is requesting for Data Items.
- **Constrained Data Items:** It cannot be accessed directly by the Subject. These need to be accessed via Clarke Wilson Security Model
- **Uncostrained Data Items:** It can be accessed directly by the Subject.

The Components of Clarke Wilson Security Model

- **Transformation Process**: Here, the Subject's request to access the Constrained Data Items is handled by the Transformation process which then converts it into permissions and then forwards it to Integration Verification Process
- **Integration Verification Process:** The Integration Verification Process will perform Authentication and Authorization. If that is successful, then the Subject is given access to Constrained Data Items.

2.4 Summary

At the end of this unit, you have learnt the types of formal model of security that are important for maintaining security. In the next unit, you will be introduced to Countermeasures employed by organisations and agencies against security breach.
You have learnt from this unit that model of security in software application in important to maintain goals of security.

Self-Assessment Exercises

1. Define formal model of security.
2. List the three major types of security model.

2.5 References/Further Readings/Web Resources

https://www.studocu.com/vn/document/truong-dai-hoc-fpt/operating-system/formal-models-of-security-systems/37750976

https://www.geeksforgeeks.org/introduction-to-classic-security-models/

2.6 Possible Answers to Self-Assessment Exercises

Define formal model of security

Answer SAEs

1. Formal models of security are models that are used for maintaining goals of security which are confidentiality, Integrity and Availability.

List the three major types of security model

2. There are 3 main types of Formal Models of security:

1. Bell-LaPadula
2. Biba
3. Clarke Wilson Security Model

Unit 3 Cyber incidents and Countermeasures

Unit Structure

3.1 Introduction

You will learn from this unit, the definition, types and approach to cyber incident as well as countermeasures by organisations against it. After studying this unit, you will be equipped with understanding of cyber incident ad its various counter-measures.

3.2 Learning Outcomes

By the end of this unit, you will be able to:

- identify cyber incident
- guide against cyber incident

3.3 Cyber incidents and Countermeasures

3.3.1 What is Cyber Incidents?

A cyber incident is defined as "a deliberate attempt to gain unauthorized access to computer systems to disrupt normal operations, steal information, or destroy data." It could involve stealing money, credit card numbers, passwords, or other sensitive information. It may also damage the organisation's reputation or cause a loss of business.

Cyber incidents are becoming more common these days. The term "cybercrime" was coined in 1989, and since then, it has become a

significant concern for both individuals and organisations. Cybercrimes include hacking, phishing, malware, ransomware, spam, identity theft, data breaches, and other malicious activities.

A cyber incident occurs when someone uses information or resources belonging to another person without permission. These incidents can happen at home, school, or work, and they can also involve personal devices such as smartphones, laptops, tablets, and even smart TVs.

3.3.2 Effect of Cyber incident on businesses and organisations

If a cyber incident happens in an organisation or business, it can have severe consequences which are:

1. **Financial Loss**
   Hackers often use cyber incidents to steal money from people's bank accounts. For example, if a hacker gains access to your online banking account, they will be able to transfer funds out of your account. If your employer doesn't reimburse you for the lost income, you'll likely need to pay the amount yourself.
2. **Reputation Damage**
   A cyber incident can make your customers think less highly of your brand, resulting in fewer sales, lower profits, and increased costs.
3. **Legal Liability**
   If an organisation is involved in a cyber incident, the staff in charge could be held liable for damages caused by your employees or contractors. You could be sued for negligence, breach of contract, or failure to provide adequate security.
4. **Business Continuity**
   Your business continuity plan should address all aspects of a cyber incident. In addition to addressing financial losses, it should help prevent further damage to your company's reputation.

Types of Cyber incident

The most common types of cyber incidents are:

5. **Hacking** – An unauthorized attempt to access the computer system by using software tools such as viruses, worms, Trojans, spyware, keyloggers, rootkits, etc.
6. **Phishing** – A fraudulent email message sent to trick users into revealing personal information like usernames, passwords, credit card numbers, bank account details, social security numbers, etc.

7. **Malware** – Malicious code designed to damage computers or steal sensitive information. It can be embedded in various electronic messages (like spam) or downloaded from websites.
8. **Ransomware** – Software used to encrypt files on your computer and demand money for their return. This includes programs like Cryptolocker, Locky, WannaCry, NotPetya, etc.
9. **Denial of Service Attack** – A type of attack where hackers use large amounts of computing power to make a website inaccessible or slow down its performance.
10. **Data Breach** – When confidential information about individuals is stolen. This could include names, addresses, Social Security Numbers, phone numbers, financial records, medical records, etc.
11. **Social Engineering** – Using human psychology against people to gain access to confidential information. For example, someone might call you pretending to be a company representative asking for your password.

Self-Assessment Exercises

1. What are practical examples of cyber incident?

Response to discovery of a cyber incident

Immediately you realize your organisation has been compromised, you need to act fast. Your first step should be to:

1. **Contact your IT support team**: Contact your IT support team so they can investigate what happened. After that, you need to decide how to handle the situation.
2. **Contact law enforcement:** Contact local police departments or the FBI if you believe your organisation was targeted because of national security concerns.
3. **Take immediate action:** Remove any unauthorized devices from your network. Change your passwords and update your antivirus software.
4. **Protect your system:** Install patches for vulnerabilities. Update operating systems and applications.
5. **Report the incident**: File a report with your state's attorney general.

Countermeasures against Cyber Incident in organisations

A countermeasure is an action, device, procedure, or technique that reduces a threat, vulnerability, or attack, eliminating or preventing it by minimizing the harm it can cause. It can also include discovering and reporting vulnerabilities so that corrective action can be taken.

Security countermeasures are the controls used to protect the confidentiality, integrity, and availability of data and information *systems.*
Protect Your Organisation from Cybersecurity Risks today through the following steps:

1. Creating data backups and encrypting sensitive information.
2. Updating all security systems and software.
3. Conducting regular employee cybersecurity training.
4. Using strong and complex passwords.
5. Installing firewalls.
6. Reducing your attack surfaces.

Self-Assessment Exercises

1. What can you do if you discover a cyber incident?
2. Why is countermeasure important to an organisation?

3.4 Summary

At the end of this unit, you have learnt the definition of cyber incidents, its various types, effects on organisations and countermeasures to prevent future occurrence that could affect organisations productivity.

You have learnt about cyber incidents and how to prevent it from this unit. Therefore, it is important to guide against such attack in the nearest future.

2.5 References/Further Readings/Web Resources

https://www.extnoc.com/learn/security/what-is-a-cyber-incident

Babasaheb Ambedkar (2021), Cyber Attacks and Counter Measures: User Perspective

3.6 Possible Answers to Self-Assessment Exercises

What are practical examples of cyber incident?

A cyber incident could take many forms. It might involve a hack into a company website, where sensitive information is stolen, and it could involve a phishing email that tricks users into giving away personal details.
It could involve malware infecting a computer system, which then starts sending out spam emails, or it could include hackers using denial of service (DoS) attacks against a particular website, making it unavailable to its intended audience.

1. *What can you do if you discover a cyber incident?*
2. *Why is countermeasure important to an organisation?*

Answer to SAE 2

1. Immediately you realize your organisation has been compromised, you need to act fast. Your first step should be to:

i. **Contact your IT support team**: Contact your IT support team so they can investigate what happened. After that, you need to decide how to handle the situation.
ii. **Contact law enforcement:** Contact local police departments or the FBI if you believe your organisation was targeted because of national security concerns.
iii. **Take immediate action:** Remove any unauthorized devices from your network. Change your passwords and update your antivirus software.
iv. **Protect your system:** Install patches for vulnerabilities. Update operating systems and applications.
v. **Report the incident**: File a report with your state's attorney general.

Answer to SAE 2

2. Employing countermeasures in computer security often safeguards valuable digital assets and sensitive information from a variety of threats. Countermeasures can be used to detect, prevent or mitigate the impact of an attack on an organisation's computer system, network or device

MODULE 8 CYBERSECURIT POLICIES AND REGULATIONS

Introduction

The purpose of cybersecurity guidelines in an organisation is to provide practical guidance on how an organisation can protect their information technology and operational technology systems, applications and data from cyber threats.

Unit 1 Cybersecurity policy and guidelines
Unit 2 Cyberspace and Cyber operations
Unit 3 Role of standards and frameworks
Unit 4 Trends and Developments in Cybersecurity

In each unit, each topic is explored in details and self-assessment exercises were highlighted at the end of the unit. Resources for further reading are highlighted at the end of each unit as well

Unit 1: Cybersecurity Policies and Guidelines

Unit Structure

1.1 Introduction
1.2 Learning Outcomes
1.3 Cybersecurity Policy and Guideline
  1.3.1 Definition of Cybersecurity policy and Guideline
  1.3.2 Importance of Cybersecurity policy
  1.3.3 Types of Cybersecurity policies
  1.3.4 Steps in developing cybersecurity policy
1.4 Summary
1.5 References/Further Readings/Web Resources
1.6 Possible Answers to Self-Assessment Exercises

1.1 Introduction

You will learn from this unit, the definition, importance, types and steps necessary for the development of Cybersecurity policies and guidelines.

1.2 Learning Outcomes

By the end of this unit, you will be able to:

- recognize the importance of cybersecurity policy
- list and understand the various types of cybersecurity policies
- highlight the steps necessary for developing cybersecurity policy

1.3 Cybersecurity Policy and Guidelines

1.3.1 Definition of Cybersecurity Policy and Guidelines

A cybersecurity policy is a document that outlines clear expectations, rules and approach that an organisation uses to maintain integrity, confidentiality and availability of sensitive information.

A cybersecurity policy provides guidance to an organisation's employees on how to act to protect the company's sensitive information. Companies commonly have several security policies that cover various topics, including IT security, email security, and the use of personal devices for work under a bring your own device (BYOD) policy.

1.3.2 Importance of Cybersecurity Policy

Companies face a range of potential threats to their systems and their data. Many cyberattacks take advantage of an organisation's employees in some way, exploiting negligence or tricking them into taking action via a phishing or social engineering attack. The rise of remote work has also introduced new threats due to the growth of BYOD policies and the potential for compromised devices to be connected to corporate networks.

cybersecurity policies help to protect the organisation against cyber threats and ensure that it remains compliant with applicable regulations. These policies can reduce an organisation's risk by training employees to avoid certain activities and can enable more effective incident response by defining protocols for detecting, preventing, and remediating them.

1.3.3 Types of Cybersecurity Policies

An organisation may implement various cybersecurity policies. Some of the most common ones include the following:

IT Security Policy: An organisation's IT security policy defines the rules and procedures for protecting the organisation against cyber threats. Some of the aspects of an IT security policy include acceptable use of corporate assets, incident response plans, business continuity strategies, and the organisation's plan for achieving and maintaining regulatory compliance.

Email Security Policy: An email security policy defines the acceptable use of corporate email systems to help protect the organisation against spam, phishing, and malware (such as ransomware) and to prevent misuse of corporate email. This type of policy may include general rules for how corporate email can and should be used, as well as specific guidance on how to handle suspicious links and email attachments.

BYOD Policy: A BYOD policy defines rules for personal devices that are used for work. These policies commonly define security requirements for these devices, such as the use of an endpoint security solution, strong passwords, and a virtual private network (VPN) when connecting to corporate networks and IT assets via an untrusted network.

1.3.4 Steps in Developing Cybersecurity Policy

Creating a cybersecurity policy is a multi-stage process with the following key steps:

1. **Determine the Threat Surface:** Different policies are designed to address different threats and risks to the organisation. The first step in writing a policy is to gain a clear understanding of the systems and processes to be regulated, such as the use of personal devices for business.
2. **Identify Applicable Requirements:** Corporate cyber security policies may have both internal and external drivers, such as corporate security goals and regulatory requirements (HIPAA, PCI DSS, etc.). To develop a cyber security policy, the next step is to define the requirements that the policy should fulfill.
3. **Draft the Policy:** After identifying requirements, the next step is to draft the policy. This should be accomplished by a team with stakeholders from IT, legal, HR, and management.
4. **Solicit Feedback:** A cyber security policy is most effective if it is clear and comprehensible to employees. Soliciting feedback from employees outside the policy group can help to avoid misunderstandings and similar issues.
5. **Train Employees:** After the policy has been developed, it needs to be disseminated through the organisation. Also, employees

will need to be trained on these policies to follow their requirements.

6. **Regularly Update the Policy:** Policies can go out of date, and their requirements may change. They should be regularly reviewed and updated to keep them up-to-date.

Self-Assessment Exercise(s)

Cybersecurity policy is necessary in every organisation. True or False Who should be involve in writing cybersecurity policy?

1.4 Summary

In this unit, you have learnt the policies and regulation that guide a cybersecurity firm. In the next unit, you will be exposed to government regulation of an information technology

You have learnt from this unit, the meaning of cybersecurity policy and guideline, its importance in an organisation as well as its various types. Cybersecurity policy is highly necessary to protect sensitive and important data and information of an organisation.

1.5 References/Further Readings/Web Resources

https://www.checkpoint.com/cyber-hub/cyber-security/cyber-security-policy types of cybersecuritypolicies/#:~:text=A%20cyber%20security%20policy%20provides,protect%20the%20company%27s%20sensitive%20information.

https://www.trellix.com/securityawareness/cybersecurity/cybersecurity policies/

1.6 Possible Answers to Self-Assessment exercises

Cybersecurity policy is necessary in every organisation. True or False

Answer to **AES1**
True

Who should be involve in writing cybersecurity policy?

Answer to AES 2

cybersecurity policy has far-reaching impacts across the organisation and can touch multiple departments. For example, IT staff may be responsible for implementing the policy, while the legal or HR teams may have the responsibility for enforcing it.

As a result, IT policies should be developed and maintained by a cross-disciplinary team consisting of personnel from IT, legal, HR, and management. This ensures that the policy is compliant with the company's strategic goals and applicable regulations, and can be effectively enforced either via technical controls or potential disciplinary action.

Unit 2 Cyberspace and Cyber Operations

Unit Structure

2.1 Introduction

You will learn from this unit, the definition of cyberspace and cyber operation, the operational development of cyber operation including cyber space operations and challenges.

2.0 Learning Outcomes

By the end of this unit, you will be able to:

- understand the importance of cyberspace and cyber operations
- assess various stages of the development of cyber operation and its challenges

2.3 Cyber space and Cyber Operation

2.3.1 Definition of Cyber space and Cyber Operation

Cyberspace is a global domain within the information environment (IE) consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. Joint Cyberspace Operations describes cyberspace operations as the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

Cyber operations encompass a range of actions executed within the digital realm to safeguard, secure, or target computer networks, systems, or information. These operations can be broadly categorized as defensive cyber operations (DCO) and offensive cyber operations (OCO). Engaging in cyber operations involves utilizing computer systems, networks, and digital tools to fulfill specific goals, including protecting confidential data, undermining opponent infrastructure, or scrutinizing network activities. These activities are typically conducted by authorised entities like intelligence agencies or military organisations.

Cyberspace operations create effects along lines of operation and lines of effort consistent with combatant command (CCMD) and service priorities. Cyberspace operations can be executed independently, or integrated with operations in other domains, to achieve primary, complementary, or enabling effects. Additionally, cyberspace operations ensure the confidentiality, integrity, and availability of vital command and control (C2) networks and the Department of Defense (DOD) Information Network (DODIN).

2.3.2 The Cyberspace Layer Model

Cyberspace is the global domain within the information environment which consist of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace can be viewed as three layers (Physical, Logical and Social) made up of five components (geographic, physical network, logical network, cyber persona, and persona)

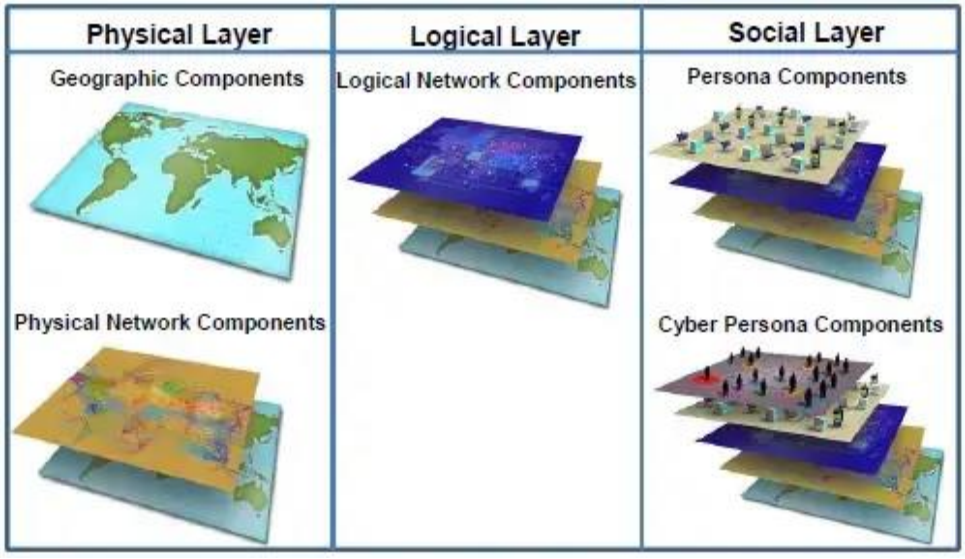


Figure 2.1: Cyberspace Layer Model

Physical: The physical layer includes the geographic component and the physical network component. The geographic component is the physical location of elements of the network. While geopolitical boundaries can easily be crossed in cyberspace at a rate approaching the speed of light, there is still a physical aspect tied to the other domains. The physical network component includes all the hardware and infrastructure (wired, wireless, and optical) that supports the network and the physical connectors (wires, cables, radio frequency, routers, servers, and computers).

Logical: The logical layer contains the logical network component, which is technical and consists of the logical connections that exist between network nodes. Nodes are any devices connected to a computer network. Nodes can be computers, personal digital assistants, cell phones, or various other network appliances. On an Internet protocol (IP) network, a node is any device with an IP address.

Social: The social layer comprises the human and cognitive aspects, including the cyber persona and persona components. The cyber persona component includes a person's identification or persona on the network (e-mail address, computer IP address, cell phone number, and others). The persona component consists of the people actually on the network. An individual can have multiple cyber personas (for example, different e-mail accounts on different computers), and a single cyber persona can have multiple users.

1.3.3 Cyberspace Operations

The cyberspace operations force conducts numerous cyberspace missions to secure and maintain freedom of action in cyberspace. These missions take on many forms, but can be categorized as either OCO, DCO, or DODIN operations based only on the intent or objective of the issuing authority, not based on the cyberspace actions executed, the type of military authority used, the forces assigned to the mission, or the cyberspace capabilities employed.4 To ensure unity of command and effort, missions are consolidated into a daily cyber tasking order (CTO).

These core activities encapsulate a wide spectrum of capabilities and responsibilities to support all other domains and execute operations in cyberspace.

- **OCO**: Missions intended to project power in and through cyberspace.

- **DCO**: Missions to preserve friendly cyberspace capabilities and protect data, networks, devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity.
- **DODIN Operations:** Operations to secure, configure, operate, extend, maintain, and sustain DOD cyberspace to create and preserve the confidentiality, availability, and integrity of the DODIN.

i. **Offensive Cyberspace Operations OCO** are missions intended to project power in and through gray and red cyberspace through actions taken in support of CCDR or national objectives. OCO may exclusively target enemy cyberspace functions or create first-order effects in cyberspace to initiate carefully controlled cascading denial effects into the physical domains to affect weapon systems, C2 processes, logistics nodes, and other high-value targets. All cyberspace operations missions conducted outside of blue cyberspace with intent other than defending blue cyberspace from an ongoing or imminent cyberspace threat are OCO missions

ii. **Defensive Cyberspace Operations DCO Missions** are executed to defend blue cyberspace from imminent or active threats in cyberspace. DCO missions defeat threats that have bypassed, breached, or are threatening to breach security measures, thereby distinguishing DCO from DODIN operations, which endeavor to secure DOD cyberspace from all threats in advance of any threat activity. The Air Force organises defensive cyberspace forces around networks, threats, or mission areas. This organisational practice aligns relevant capabilities with authority to execute operations and ensures defensive cyberspace Airmen are familiar with the cyberspace terrain or mission area they are assigned to defend, or the threat they are assigned to defend against.

iii. **Dod Information Network Operations** Air Force DODIN operations are standing missions that involve day-to-day security and maintenance operations, threat response, and support to DCO forces. Although, many of these activities are regularly scheduled events, they cannot be considered routine, as their aggregate effects establish the framework for most Air Force missions.

2.3.4 Cyberspace Operations Threats

Cyberspace operations face many threats, anywhere from nation-states to individual actors, to accidents and natural hazards. To enable freedom of maneuver in cyberspace, cyberspace operations must reduce or eliminate threats and vulnerabilities and constantly assess, coordinate and deconflict cyberspace operations. In general, cyberspace threats are

divided into two major categories: malicious cyberspace activity and adverse cyberspace activities.

Malicious Cyberspace Activities: Activities, other than those authorised by or in accordance with US law, which seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or the information resident therein. Organised crime or other non-state, illegitimate organisations often make sophisticated malware available for purchase or free, allowing even unsophisticated threat actors to acquire advanced capabilities at little to no cost.

Adverse Cyberspace Activities (ACA): The Air Force term for friendly actions or natural events, disasters, or accidents that inadvertently achieve the same effects as malicious cyberspace activity; providing adversaries the opportunity to capitalize on vulnerabilities and infrastructure degradation. Friendly actions in one segment of the network may result in unintended damage in another. Likewise, natural events can damage and disrupt cyberspace with highly destructive effects requiring both proactive and reactive cyberspace operations to maintain or restore key cyberspace systems. In addition to friendly actions, ACA also includes friendly negligence or deficiencies that create vulnerabilities or open systems to attack such as: failure to implement policy, implementing rushed or inadequate policy, and poor change management practices. There are also numerous examples where individuals (mission or system owners and operators) can, with or without malign intent, become insider threats by executing actions, policies, or changes which adversely affect operations.

Attribution

Perhaps the most challenging aspect of cyberspace-related intelligence is connecting an action to a real-world agent (individual or state) with sufficient confidence and verification to inform decision makers. By design, the internet lends anonymity and complicates attribution. Likewise, government policies and international laws and treaties can make it

very difficult to determine the origin of a cyberspace attack. The ability to hide the source an attack makes it difficult to find and fix an attacker within cyberspace.

Self-Assessment exercises

1.	Differentiate between cyberspace and cyber operation
2.	What are the challenges of cyberspace operations?

2.4 Summary

At the end of this unit, you have learnt the definition of cyber space and cyber operations, the operations of cyber space, the layers of development of cyber space and the various threats faced by cyber operations.

You have learnt cyberspace and cyber operations including cyberspace layer of development, its operation as well as cyberspace threat from this unit. It is important to understand how to guide against cyber operations and space.

2.5 References/Further Readings/Web Resources

Gregory D. Hillebrand and Bill Ault (2023) Strategic Cyberspace Operations Primer

Head Doctrine (2022) Cyber Primer, (3rd Edition), United Kingdom Ministry of defense

https://assets.publishing.service.gov.uk/media/63623df5d3bf7f04e12196d0/Cyber_Primer_Edition_3.pdf

https://nordvpn.com/cybersecurity/glossary/cyber-operations/

https://nordvpn.com/cybersecurity/glossary/cyber-operations/

https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3

The National Strategy to Secure Cyberspace Feb 2003

2.6 Possible Answers to Self-Assessment exercises

Differentiate between cyberspace and cyber operation

Answer to AES 1

Cyberspace is a global domain within the information environment (IE) consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers while cyber operation encompass a range of actions executed within the digital realm to safeguard, secure, or target computer networks, systems, or information.

What are the challenges of cyberspace operations?

Answer to AES 2

Foreign ownership, control, and influence of vendors: Many Commercial Off-the Shelf (COTS) technologies (hardware and software) available for purchase are developed, manufactured, or have components manufactured in foreign countries. Adversaries may exploit this vulnerability by influencing foreign manufacturers, vendors, service providers, or developers to alter products with designed security weaknesses, such as modified chips. This vulnerability is present throughout a product's life cycle, from design and manufacture, to delivery, and through product updates and support.

Unit 3 Role of Standards and Frameworks

Unit Structure

3.1 Introduction

You will learn about cybersecurity standards and frameworks in this unit. After studying this unit, you will be equipped with the skills to identify the various standards and frameworks applicable to cybersecurity.

3.2 Learning Outcomes

By the end of this unit, you will be able to:

- identify different types of frameworks
- differentiate between framework and standards as applicable to cybersecurity

3.3 Role of standards and frameworks

3.3.1 Definition of Framework and Standard

A cybersecurity framework is a structured set of guidelines and best practices designed to help organisations manage and mitigate cybersecurity risks associated with their information and technology systems. Cybersecurity frameworks are generally applicable to all organisations, regardless of their size, industry, or sector.

A cybersecurity standard is a set of guidelines or best practices that organisations can use to improve their cybersecurity posture.

cybersecurity standards represent the crucial means by which an enterprise ensures that their security strategy and policies are implemented in a consistent and measurable manner in day-to-day operations.

Organisations can use cybersecurity standards to help them identify and implement appropriate measures to protect their systems and data from cyber threats. Standards can also provide guidance on how to respond to and recover from cybersecurity incidents.

Purpose of using framework

cybersecurity framework is to offer a holistic strategy for defending against cyber threats. To achieve this, a framework typically consists of several components, including: standards, guidelines, best practices, and processes. These components work together to help organisations identify potential vulnerabilities, protect critical assets, detect anomalies or breaches, respond to threats promptly, and recover effectively after an incident.

3.3.2 Common Cybersecurity Frameworks

Seven common cybersecurity frameworks and standards are:

1. NIST Cybersecurity Frameworks
2. ISO 27001 and ISO 27002
3. SOC2
4. NERC-CIP
5, HIPPA
6. GDPR
7. FISMA

NIST Cybersecurity Framework

The NIST Cybersecurity Framework was established in response to an executive order by former President Obama — Improving Critical Infrastructure Cybersecurity — which called for greater collaboration between the public and private sector for identifying, assessing, and managing cyber risk. While compliance is voluntary, NIST has become the gold standard for assessing cybersecurity maturity, identifying security gaps, and meeting cybersecurity regulations.

Figure 3.1: Layers of NIST Cybersecurity framework

The cybersecurity framework now encompasses six core functions:

1. Identify,
2. Protect,
3. Detect,
4. Respond,
5. Recover, and
6. Govern

The cybersecurity framework providing a holistic approach to managing cybersecurity risk.

NIST has also introduced a suite of resources to facilitate the security framework's adoption. These include quick-start guides tailored for various audiences, success stories from organisations that have implemented the CSF, and a searchable catalog of informative references to align existing practices with the framework's guidance.

- **ISO 27001 and ISO 27002**
  Created by the International Organisation for Standardization (ISO), ISO 27001 and ISO 27002 certifications are considered the international cybersecurity standard for validating a cybersecurity program — internally and across third parties.

  With an ISO certification, companies can demonstrate to the board, customers, partners, and shareholders that they are doing the right things with cyber risk management.

  Likewise, if a vendor is ISO 27001/2 certified, it's a good indicator that they have mature cybersecurity practices and controls in place.

The downside is that the process requires time and resources; organisations should only proceed if there is a true benefit, such as the ability to win new business. The certification is also a point-in-time exercise and could miss evolving risks that continuous monitoring can detect.

- **SOC2**
  Service Organisation Control (SOC) Type 2; is a trust-based cybersecurity framework and auditing standard developed by the American Institute of Certified Public Accountants (AICPA) to help verify that vendors and partners are securely managing client data.

  SOC2 specifies more than 60 compliance requirements and extensive auditing processes for third-party systems and controls. Audits can take a year to complete. At that point, a report is issued which attests to a vendors' cybersecurity posture.

  Because of its comprehensiveness, SOC2 is one of the toughest security frameworks to implement — especially for organisations in the finance or banking sector who face a higher standard for compliance than other sectors.

  Nevertheless, it's an important security framework that should be central to any third-party risk management program.

- **NERC-CIP**
  NERC-CIP was introduced to mitigate the rise in attacks on U.S. critical infrastructure and growing third-party risk, the North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) is a set of cybersecurity standards designed to help those in the utility and power sector reduce cyber risk and ensure the reliability of bulk electric systems. The NERC-CIP security framework requires impacted organisations to identify and mitigate third-party cyber risks in their supply chain.
  NERC-SIP stipulates a range of controls including categorizing systems and critical assets, training personnel, incident response and planning, recovery plans for critical cyber assets, vulnerability assessments, and more. Read more about effective strategies for achieving NERC-CIP compliance.

- **HIPAA**
  The Health Insurance Portability and Accountability Act (HIPAA) is a cybersecurity framework that requires healthcare organisations to implement controls for securing and protecting the privacy of electronic health information. Per HIPAA, in addition to demonstrating compliance against cyber risk best practices — such as training employees — companies in the sector must also conduct risk assessments to manage and identify emerging risk. HIPAA compliance remains a keen challenge for healthcare organisations, as Bitsight research suggests.

- **GDPR**
  The General Data Protection Regulation (GDPR) was adopted in 2016 to strengthen data protection procedures and practices for citizens of the European Union (EU). The GDPR impacts all organisations that are established in the EU or any business that collects and stores the private data of EU citizens — including U.S. businesses.

  The security framework includes 99 articles pertaining to a company's compliance responsibilities including a consumer's data access rights, data protection policies and procedures, data breach notification requirements (companies must notify their national regulator within 72 hours of breach discover), and more.

- **FISMA**
  The Federal Information Security Management Act (FISMA) is a comprehensive cybersecurity framework that protects federal government information and systems against cyber threats. FISMA also extends to third parties and vendors who work on behalf of federal agencies.

The FISMA security framework is aligned closely with NIST cybersecurity standards and requires agencies and third parties to maintain an inventory of their digital assets and identify any integrations between networks and systems.

Sensitive information must be categorized according to risk and security controls must meet minimum security standards as defined by FIPS and NIST 800 guidelines.

Impacted organisations must also conduct cybersecurity risk assessments, annual security reviews, and continuously monitor their IT infrastructure.

3.3.3 Cybersecurity Frameworks Best Practices

Although every framework is different, certain best practices are applicable across the board. Here, we are expanding on NIST's five functions mentioned previously.

i. **Identify**: To manage the security risks to its assets, data, capabilities, and systems, a company must fully understand these environments and identify potential weak spots.
ii. **Protect:** Companies must create and deploy appropriate safeguards to lessen or limit the effects of potential cyber security breaches and events.
iii. **Detect**: Organisations should put in motion the necessary procedures to identify cyber security incidents as soon as possible.
iv. **Respond**: Companies must be capable of developing appropriate response plans to contain the impacts of any cyber security events.
v. **Recover**: Companies must create and implement effective procedures that restore any capabilities and services damaged by cyber security events.

Self-Assessment Exercises

1. What is the purpose of using framework?
2. Why do we need cybersecurity framework?
3. What are the types of cybersecurity framework?

3.4 Summary

At this unit, you have learnt about cybersecurity standards and frameworks and the various categories and classifications as well as the importance.

You have learnt various cybersecurity standards and frameworks from this unit as well as the importance of framework to organisations.

3.6 References/Further Readings/Web Resources

Eric Cisternelli (2024) 7 Cybersecurity Frameworks That Help Reduce Cyber Risk (List & Resources) POLICY & REGULATIONS

https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk

https://www.itgovernanceusa.com/cybersecurity-standards

3.6 Possible Answers to Self-Assessment Exercises

What is the purpose of using framework?

Answer to SAE 1

Cybersecurity framework is to offer a holistic strategy for defending against cyber threats. To achieve this, a framework typically consists of several components, including: standards, guidelines, best practices, and processes. These components work together to help organisations identify potential vulnerabilities, protect critical assets, detect anomalies or breaches, respond to threats promptly, and recover effectively after an incident.

Why do we need cybersecurity framework?

Answer to SAE 2

Cyber security frameworks remove some of the guesswork in securing digital assets. Frameworks give cyber security managers a reliable, standardized, systematic way to mitigate cyber risk, regardless of the environment's complexity. Cyber security frameworks help teams address cyber security challenges, providing a strategic, well-thought plan to protect its data, infrastructure, and information systems. The frameworks offer guidance, helping IT security leaders manage their organisation's cyber risks more intelligently. Companies can adapt and adjust an existing framework to meet their own needs or create one internally.

What are the types of cybersecurity framework?

Answer to SAE 3

1. Control Frameworks

- Develops a basic strategy for the organisation's cyber security department
- Provides a baseline group of security controls
- Assesses the present state of the infrastructure and technology
- Prioritizes implementation of security controls
- Program Frameworks
- Assesses the current state of the organisation's security program
- Constructs a complete cybersecurity program
- Measures the program's security and competitive analysis
- Facilitates and simplifies communications between the cyber security team and the managers/executives

2. Risk Frameworks

- Defines the necessary processes for risk assessment and management
- Structures a security program for risk management
- Identifies, measures, and quantifies the organisation's security risks
- Prioritizes appropriate security measures and activities

Unit 4 Trends and Developments in Cybersecurity

Unit Structure

4.1 Introduction

The top cybersecurity trends of 2024 are redefining the approach to cyber defense and strategy, ushering in an era of innovation and adaptation. By staying abreast of these trends and implementing proactive security measures, organisations can strengthen their resilience against evolving cyber threats and safeguard their digital assets.

4.2 Learning Outcomes

By the end of this unit, you will be able to;

- highlight the trends of cybersecurity
- discuss the effect of Cybersecurity on emerging technologies

4.3.1 Trends and Developments in Cybersecurity

4.3.1 Cybersecurity Trends

One notable trend is the integration of artificial intelligence (AI) and machine learning (ML) into cybersecurity practices. AI and ML algorithms are revolutionizing threat detection and response, enabling organisations to analyze vast amounts of data in real-time and identify anomalies indicative of potential security breaches. By leveraging AI-driven security solutions, businesses can enhance their threat detection capabilities and respond swiftly to emerging cyber threats.

The proliferation of ransomware attacks has catapulted ransomware mitigation strategies to the forefront of cybersecurity priorities. Attackers are increasingly targeting critical infrastructure and high-

profile organisations, demanding exorbitant ransoms for the release of encrypted data. In response, organisations are adopting a multi-layered approach to ransomware defense, employing measures such as robust backup solutions, employee training and proactive threat hunting to mitigate their risks.

Supply chain attacks have emerged as a prominent threat vector, posing significant challenges to organisations across various industries. Malicious actors are exploiting vulnerabilities within third-party vendors and supply chain partners to infiltrate target networks and exfiltrate sensitive data. To address this threat, organisations are placing greater emphasis on supply chain risk management, conducting thorough vendor assessments, and implementing stringent security protocols throughout the supply chain ecosystem.

4.3.2 Emerging Technologies and their Impact on Cybersecurity Artificial Intelligence

Artificial intelligence stands at the forefront of innovation in cybersecurity, revolutionizing the way organisations detect, analyze, and respond to threats in 2024. AI-powered systems possess the capability to autonomously identify anomalous behavior patterns, predict potential security breaches, and even autonomously thwart cyber-attacks in real-time. By harnessing the immense processing power of AI, cybersecurity professionals can augment their security stacks, proactively identifying and mitigating threats before they escalate into full-fledged attacks.

Quantum Computing
Quantum computing represents a paradigm shift in cybersecurity, offering unparalleled computational capabilities that have the potential to both enhance and disrupt existing security protocols. While quantum computing holds promise for accelerating cryptographic breakthroughs and strengthening encryption methods, it also poses a significant threat to traditional cryptographic algorithms. As quantum computers advance, they have the potential to render current encryption standards obsolete, necessitating the development of quantum-resistant encryption techniques to safeguard sensitive data in a new age of computing.

Internet of Things (IoT)
The Internet of Things (IoT) further expands the attack surface of cyberspace, introducing countless interconnected devices that are vulnerable to exploitation by threat actors. From smart homes and connected vehicles to industrial control systems, IoT devices present unique security challenges due to their inherent complexity and diverse ecosystem. As the proliferation of IoT devices continues unabated, cybersecurity professionals must grapple with the task of securing these

interconnected networks, implementing robust authentication mechanisms, and safeguarding against potential IoT-based attacks.

However, the integration of advanced technologies into cybersecurity also presents a double-edged sword, as adversaries seek to exploit the same innovations for malicious purposes. AI-powered malware, quantum-enabled decryption algorithms, and IoT-based botnets are just a few examples of how cybercriminals are leveraging emerging technologies to orchestrate sophisticated cyber-attacks. As defenders race to stay ahead of evolving threats, they must navigate the ethical and security implications of utilizing advanced technologies in their cybersecurity arsenal.

The evolution of cyber threats and attack vectors

The evolution of cyberattacks and threat vectors represents a dynamic and ever-changing landscape, driven by advancements in technology, changes in attacker methodologies, and shifting geopolitical landscapes.

Historically, cyber threats have evolved from relatively simple and opportunistic attacks, such as malware infections and phishing scams, to complex and multifaceted operations orchestrated by well-funded cybercriminal organisations and state-sponsored actors. As cybersecurity defenses have strengthened and detection capabilities have improved, attackers have adapted their tactics, techniques, and procedures (TTPs) to evade detection and maximize the impact of their attacks.

One notable trend in the evolution of cyber threats is the increase in advanced persistent threats (APTs), which are characterized by their stealthy, long-term presence within target networks. APT actors employ sophisticated techniques, such as zero-day exploits, social engineering, and lateral movement, to infiltrate and maintain persistent access to systems and data. These adversaries often possess significant resources and expertise, allowing them to conduct highly targeted campaigns against specific organisations or industries.

Another emerging threat vector is the exploitation of supply chain vulnerabilities, whereby attackers target third-party vendors and service providers to gain unauthorised access to target networks. Supply chain attacks have become increasingly prevalent in recent years, with cybercriminals leveraging trusted relationships and dependencies often within the IT channel to infiltrate target networks and exfiltrate sensitive data. These attacks pose significant challenges to organisations, as they often bypass traditional security measures and require a collaborative approach to mitigation and remediation.

In response to these evolving threats, defense mechanisms must adapt and evolve accordingly. Predictive analytics, threat intelligence sharing,

and proactive threat hunting are just a few strategies that organisations can employ to enhance their cyber resilience and mitigate the risk of emerging threats.

Self-Assessment Exercise(s)

1.	List any two top emerging technologies that has impact on cybersecurity

4.4 Summary

At the end of this unit, students have been exposed to the top trends and development of cybersecurity.

You have learnt the various emerging trends and developments of cybersecurity in this unit.

7.0 References/Further Readings/Web Resources

Allison Ho (2024) 2024 cybersecurity trends: Key steps, strategies and guidance

4.0 Possible Answers to Self-Assessment Exercise

List any two top emerging technologies that has impact on cybersecurity

Answer SAE

Quantum Computing, Internet of Things