COURSE GUIDE

CIT 855
ADVANCED CYBER SECURITY

Course Team Prof. Adekunle A. Eludire - (Developer/Writer)
Prof. Olatunji Okesola- Content Editor
Dr. Francis B. Osang – HOD/Internal Quality Control Expert

NATIONAL OPEN UNIVERSITY OF NIGERIA

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

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

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

First Printed 2022

ISBN: 978-058-557-5

CONTENTS **PAGE**

INTRODUCTION

The Course gives an advanced overview of computer security; cyber security principles, security technologies, security policies, security standards, cyber security challenges, cyber security risk analysis, cyber security threat to e-commerce, data security consideration, digital signature and cyber security tools.

A working knowledge of the cyber security is very important to all would-be IT practitioners, programmers and engineers alike.

COURSE AIM

The aim of this course is to provide you with an understanding of Cyber security. Additionally, it also aims at letting you know the challenges of computer security and the requirements for mitigating them.

This course is made up of modules, units and a course guide. This course guide tells you briefly what the course is all about. It tells you about the course materials you will be using and how you can work with it. In addition, it gives some general guidelines for the amount of time you are likely to spend on each unit of the course in order to complete this course successfully. You have quite a number of tutor-marked assignments meant to test your in-depth understanding of the course.

There will be regular tutorial classes that are related to this course. You are advised to attend tutorial classes. The course will prepare you for the challenges you will meet in the field of cyber security.

COURSE OBJECTIVES

To achieve the aims set out, the course has a set of objectives. Each unit has specific objectives which are presented at the beginning of the unit. You are expected to read these objectives before you study the unit. You may wish to refer to them during your study to check on your progress. You should always look at the unit objectives after completion of each unit. By so doing, you would have followed the instructions in the unit.
Below are the comprehensive objectives of the course as a whole. By meeting these objectives, you should have achieved the aims of the course as a whole. In addition to the aims above, this course sets to achieve some objectives. Thus, after going through the course, you should be able to:

- Recognize the individual components of the big picture of cyber security
- Outline the basic cyber security challenges

- Cite the History of Cyber Security and Cyber Security Goals
- Understand the Fundamentals of Cyber Security - Cyber Security Principles, Security Technologies, Security Policies and Security Standards
- List the Cyber Security Challenges and Risk Analysis
- Compare the Cyber Security Threat to E-Commerce and Security Tools
- Understand the management of Cyber Security
- Understand Data Security Consideration
- Analyse Cyber Attacks and Attackers

WORKING THROUGH THIS COURSE

To complete this course, you are required to read each study unit, read the reading materials specified at the end of each unit in conjunction with the ones which may be provided by the National Open University of Nigeria.

Each unit contains self-assessment exercises and at certain points in the course you would be required to submit assignments for assessment purposes. At the end of the course there will be a final examination. The course should take you about a total of 21 weeks to complete. All the components of the course are listed below so as to assist you in allocating your time to each unit in order to complete the course on time and successfully.

You are required to spend a lot of time in reading and to attend tutorial sessions for you to have opportunity of interacting with other people offering this course.

STUDY UNITS

The study units in this course are as follows:

Module 1 Fundamentals of Cyber Security

Unit 1 Cyber Security Goals
Unit 2 Cyber Security Principles
Unit 3 Security Policies and Standards

Module 2 Cyber Security Challenges and Threats

Unit 1 Cyber Security Challenges
Unit 2 Cyber Security Risk Analysis
Unit 3 Cyber Security Threats
Unit 4 Cyber Security Threat to E-Commerce

Module 3 Managing Cyber Security

Unit 1 Data Security Concerns
Unit 2 Security Technologies
Unit 3 Cyber Security Tools
Unit 4 Cyber Security Operations

Module 4 Cyber Attacks and Attackers

Unit 1 Types of Cyber Attacks and Attackers
Unit 2 Man-in-the-Middle Attacks
Unit 3 Cyber Security Wi-Fi Attacks

The first unit of module 1 explain the goals of cyber security as a course of study. Unit 2 of module 1 describes cyber security principles and explain the fundamentals of cyber security. It explains the merits and demerits of various principles associated with cyber security and discusses how to apply them. Unit 3 explains security policies and standards in relations to cyber security and their applicability.

The first unit of module 2 gives detailed explanation of the security challenges that are identified in the cyber space. It describes the challenges of each of the security models. Unit 2 describes the risk involved in cyber security and a measure of the risk level. Unit 3 describes the available types of cyber security threats while Unit 4 describes the security threats posed by cybercrimes to e-commerce. It highlights the issues associated with the benefits that could accrue to international commercial activities and if the threats can be mitigated properly.

The first unit of module 3 discusses the management of cyber security and provided a general look at data security concerns and considerations. It describes various components of data security and explains how to manage them. Unit 2 explores the available security technologies. Unit 3 covers various tools available for managing cyber security, the characteristics and the ways to carry out data security test with these tools are also included. Finally, Unit 4 addresses the issues of Cyber Security Operations.

Unit 1 of module 4 identifies and explains the types of attacks and attackers available in cyber security while Unit 3 explains in details a special type of attack prevalent in cyber security, the man-in-the-middle attack. It provides the basics of this type of cyber-attack and possible solutions to mitigate it. The issues related to Cyber Security of Wi-Fi enabled networks were examined in Unit 3 of this module.

REFERENCES AND FURTHER READING

Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBok (2019): The Cyber Security Body of Knowledge, National Cyber Security Centre.

Brij Gupta, Gregorio Martinez Perez, Dharma P. Agrawal, Deepak Gupta. (2020) Handbook of Computer Networks and Cyber Security: Principles and Paradigms Springer.

Donald A. Tevault (2020) Mastering Linux Security and Hardening: Protect Your Linux Systems from Intruders, Malware Attacks, And Other Cyber Threats Packtpub.

Ethem Mining Kali. (2019) Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing. Includes Valuable Basic Networking Concepts.

Jack Caravelli, Nigel Jones. (2019) Cyber Security: Threats and Responses for Government and Business 1440861730, 9781440861734 Praeger Security International.

Karnel Erickson. (2019) Cyber Security (Kali Linux for Hackers & Hacker Basic Security).

Kuan-Ching Li, Xiaofeng Chen, Willy Susilo. (2019) Advances in Cyber Security: Principles, Techniques, and Applications Springer Singapore.

Nathan House. (2017) The Complete Cyber Security Course, Volume 1: Hackers Exposed StationX 282.

Venkata P. Krishna, Sasikumar Gurumoorthy, Mohammad S. Obaidat.(2019) Social Network Forensics, Cyber Security, and Machine Learning, SpringerBriefs in Applied Sciences and Technology, Springer Singapore.

Zach Codings. (2019) Computer Programming and Cyber Security for Beginners: This Book Includes: Python Machine Learning, SQL, Linux, Hacking with Kali Linux, Ethical Hacking. Coding and Cybersecurity Fundamentals.

PRESENTATION SCHEDULE

Your course materials have important dates for the early and timely completion and submission of your TMAs and attending tutorials. You should remember that you are required to submit all your assignments by the stipulated time and date. You should guard against falling behind in your work.

ASSESSMENT

There are three aspects to the self-assessment of the course. The first self-assessment is made up of exercises, second consists of the tutor-marked assignments and third is the written examination/end of course examination.

You are advised to do the exercises. In tackling the assignments, you are expected to apply information, knowledge and techniques you gathered during the course.

You are to submit the assignments to your facilitators for formal assessment in accordance with the deadlines stated in the presentation schedule and the assignment file. The work you submit to your tutor for assessment will count for 30% of your total course work. At the end of the course you will need to sit for a final or end of course examination of about three hours' duration. This examination will count for 70% of your total course mark.

TUTOR-MARKED ASSIGNMENT

The TMA is a continuous assessment component of your course. It accounts for 30% of the total score. You will be given four (4) TMAs to answer. Three of these must be answered before you are allowed to sit for the end of course examination.

The TMAs would be given to you by your facilitator and returned after you have done the assignment. Assignment questions are given at the end of each unit in this course. You will be able to complete your assignment from the information and material contained in your reading, references and study units. However, it is desirable in all degree level of education to demonstrate that you have read and researched more into your references, which will give you a wider view point and may provide you with a deeper understanding of the subject.

Make sure that each assignment reaches your facilitator on or before the deadline given in the presentation schedule and assignment file. If for any reason you cannot complete your work on time, contact your

facilitator before the assignment is due to discuss the possibility of an extension. Extension will not be granted after the due date unless there are exceptional circumstances.

FINAL EXAMINATION AND GRADING

The end of course examination for Advanced Cyber Security will be for about 3 hours and it has a value of 70% of the total course work. The examination will consist of questions, which will reflect the type of self-testing, practice exercise and tutor marked assignment problems you have previously encountered. All areas of the course will be assessed.

You should use the time between finishing of the last unit and sitting for the examination to revise the whole course. You might find it useful to review your self-test, TMAs and comments on them before the examination. The end of course examination covers information from all parts of the course.

COURSE MARKING SCHEME

Assignment	**Marks**
Assignment 1 – 4	Four assignments, best three marks of the four count at 10% each – 30% of course marks.
End of course examination	70% of overall course marks
Total	100% of course materials

HOW TO GET THE MOST FROM THE COURSE

Advanced cyber security is a course that intends to provide the concepts of network security and access on the cyber space. The proliferation of Internet amongst the population is getting deep day-by-day. This not only increase the scope of e-governance and e-commerce in the area of healthcare, banking, power distribution, etc. but also expose these sectors to cyber threats like hacking, credential thefts, data tempering, account hijacking, etc. it is interesting to note that the current trend in the cyber space is alarming requiring experts in this subject area.

According to reports, there were around 62,189 cyber security incidents, originating mainly from Countries including US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE, in the period from Jan-May, 2014. Also, around 10,000 Indian government sites were compromised in this period. India has a serious shortage of IT Security professional to deal with such treats in effective manner. According to a report, India needs around one million cyber security professionals to deal with cyber threats effectively.

Going through this course will expose you to the security challenges that abound and the measures in place to mitigate them. In addition, you will be able to answer the following type of questions:

1. Discuss the history of Cyber Security
2. Explain Cyber Security Goals
3. Explain the Fundamentals of Cyber Security
4. Identify and discuss Cyber Security Principles
5. Describe identified Security Technologies
6. Discuss various Security Policies
7. What are the key issues with Security Standards?
8. Differentiate between Cyber Security Challenges and Risk Analysis
9. Identify and discuss various Cyber Security Challenges
10. What are the problems faced with Cyber Security Risk Analysis?
11. Cyber Security Threat to E-Commerce
12. What are the major components in Managing Cyber Security?
13. What are the key issues in Data Security Consideration?
14. Discuss the main characteristics of Digital Signature
15. What are the available Cyber Security Tools?
16. Describe Cyber Attacks and Attackers
17. Identify the Types of Cyber Attacks
18. Explain the Types of Cyber Attackers
19. What are the key issues in Man-in-the-Middle Attacks?

However, the list of questions that you can answer is not limited to the above list. To gain the most from this course you should endeavour to apply the principles you have learnt to your understanding of cyber security.

I wish you success in the course and I hope you will find it both interesting and useful.

FACILITATION

There are 16 hours of tutorials provided in support of this course. You will be notified of the dates, times and location of these tutorials as well as the name and phone number of your facilitator, as soon as you are allocated a tutorial group.

Your facilitator will mark and comment on your assignments, keep a close watch on your progress and any difficulties you might face and provide assistance to you during the course. You are expected to mail your Tutor Marked Assignment to your facilitator before the schedule date (at least two working days are required). They will be marked by

your tutor and returned to you as soon as possible. Do not delay to contact your facilitator by telephone or e-mail if you need assistance.
The following might be circumstances in which you would find assistance necessary, hence you would have to contact your facilitator if:

- You do not understand any part of the study or the assigned readings.
- You have difficulty with the self-tests
- You have a question or problem with an assignment or with the grading of an assignment.

You should endeavour to attend the tutorials. This is the only chance to have face contact with your course facilitator and to ask questions which are answered instantly. You can raise any problem encountered in the course of your study.

To gain much benefit from course tutorials prepare a question list before attending them. You will learn a lot from participating actively in discussions.

ICE BREAKER

Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage, or unauthorized access. The term cybersecurity 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 systems, networks, and technologies.

In other words, 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. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And 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.

Robust cybersecurity implementation is roughly based around three key terms: people, processes, and technology. This three-pronged approach helps organizations defend themselves from both highly organized attacks and common internal threats, such as accidental breaches and human error.

The attacks evolve every day as attackers become more inventive, it is critical to properly define cybersecurity and understand cybersecurity fundamentals.

MAIN COURSE

CONTENTS **PAGE**

MODULE 1 FUNDAMENTALS OF CYBER SECURITY

MODULE INTRODUCTION

This module consists of three units and introduces the learners to the fundamentals of cyber security principles by presenting the cyber security goals, cyber security principles, policies and standards. It highlights the essential cyber security principles such as security technologies, security policies and security standards.

UNIT 1 CYBER SECURITY GOALS

CONTENTS

1.0 INTRODUCTION

This unit covers the details of cyber security goals. The unit has the objective of demonstrating the goals of cyber security enshrined in the need to protect the confidentiality of data, preserve the integrity of data and promote the availability of data for authorised users. These goals are referred to as the CIA triad that describes the major issues in data communication and security.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the CIA triad of cyber security
- Describing the “C” in the CIA triad
- Explaining the “I” in the CIA triad
- Understanding the “A” in the CIA triad

3.0 MAIN CONTENT

Cyber Security Goals

The objective of Cybersecurity is to guard information from being stolen, compromised or attacked. Cybersecurity will be measured by a minimum of one among three goals-

1. Protect the confidentiality of information.
2. Preserve the integrity of knowledge.
3. Promote the provision of knowledge for authorized users.

These goals form the confidentiality, integrity, availability (CIA) triad, the idea of all security programs. The CIA triad could be a security model that's designed to guide policies for information security within the premises of a corporation or company. This model is additionally stated because the AIC (Availability, Integrity, and Confidentiality) triad to avoid the confusion with the American Central intelligence service. the weather of the triad is considered the three most vital components of security.

The CIA criteria are one that the majority of the organizations and corporations use after they have installed a replacement application, creates a database or when guaranteeing access to some data. For data to be completely secure, all of those security goals must get effect. These are security policies where everyone works together, and thus it will be wrong to overlook one policy. The CIA triad is shown in Figure 1.2.

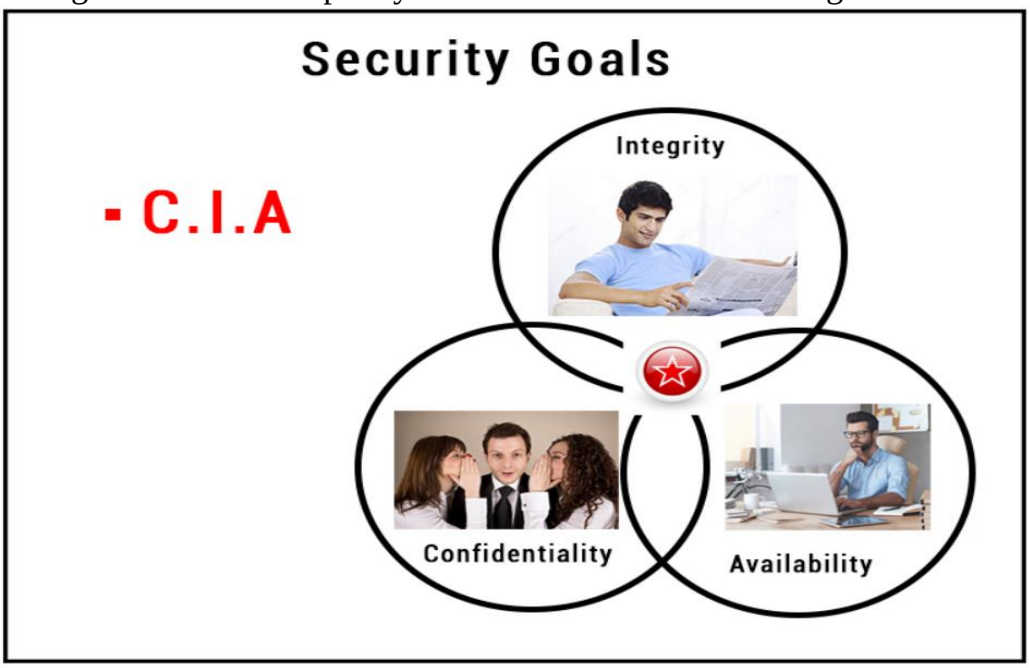

Figure 1.2: The CIA Triad

3.1 Confidentiality

Confidentiality roughly correspond to privacy and avoids the unauthorized disclosure of knowledge. It involves the protection of knowledge, providing access for people who are allowed to access it while disallowing others from learning anything about its content. It prevents essential information from reaching the inapt people while ensuring that the correct people can access it. Encryption may be an ideal example to confirm confidentiality.

Tools for Confidentiality

a. Encryption

Encryption may be a method of reworking information to form it unreadable for unauthorized users by using an algorithm. The transformation of information uses a secret key (an encryption key) so the transformed data can only be read by using another secret key (decryption key). It protects sensitive data like the MasterCard numbers by encoding and remodelling data into incomprehensible cipher text. This encrypted data can only be read by decrypting it. Asymmetric-key and symmetric-key are the 2 primary kinds of encryption.

b. Access control

Access control outlines the rules and policies for limiting access to a system, physical or virtual resources. it's a process by which users are allowed access and given certain privileges to systems, resources or information. In access control systems, users must present their credentials before they will be granted access like the personality's name or a computer's serial number. In physical systems, these credentials may be available in many forms, but credentials that cannot be transferred provide the foremost security.

c. Authentication

An authentication may be a process that certifies and confirms a user's identity or applicable role that somebody has. Authentication is often accomplished in a number of ways, but it's usually reinforced by a mix of something the user –

- has (e.g. a smart card or a radio key for keeping secret keys),
- knows (e.g. a password),
- is (e.g. a human biometric, fingerprint).

Authentication is an inevitable requirement of each establishment because it enables organizations to have their networks secured by permitting only authenticated users to access its secure resources. These resources may include networks, computer systems, websites, databases and other network-based applications or services.

d. Authorization

Authorization could be a security mechanism that grants permission to carry out something or take something. It's wont to determine what someone or a system is allowed access to resources, depending on the access control policy, including computer programs, services, files, information and application features. It's usually preceded by authentication for user biometric identification. System administrators are normally assigned permission levels that covers all system and user resources. During authorisation, users are either granted or refused resource access based on the results of system verified authenticated user's access rules.

e. Physical Security

Physical security describes measures designed to deny the unauthorised access of information technology assets like equipment, facilities, personnel, resources and other properties from damage. It safeguards these assets from physical threats including vandalism, theft, fire and natural disasters.

3.2 Integrity

Integrity refers to the methods for ensuring that data is real, correct and safeguarded from unauthorised user alteration. It’s the property that data has not be altered in an unauthorised way with a guarantee that the source of the obtained information is genuine.

Tools for Integrity

a. Backups

Backup is that process of periodically archiving of information. It's a process of creating copies of information or data files to use within the event when the first data or data files are lost or destroyed. it's also wont to make copies for historical purposes, like for longitudinal studies, statistics or for historical records or to fulfil the wants of an information retention policy. Many applications particularly within the Windows environment, produce backup files with the .BAK file extension.

b. Checksums

A checksum could be a numerical value for verifying the integrity of a file or an information transfer. Alternatively, it's the computation of a function that maps the contents of a file to a numerical value. They're typically applied in comparing two sets of information to confirm that they're identical. A checksum function depends on the whole contents of a file. It's designed in a special way that even a little or low change to the computer file (such as flipping one bit) is likely to leads to different output value.

c. Data Correcting Codes
It is a way of storing data such that little changes can be easily detected and corrected automatically.

3.3 Availability

Availability is that property wherein information is accessible and amendable in a timely manner by authorised users. It's the guarantee of consistent and continual access to sensitive data by authorised users.

Tools for Availability

a. Physical Protections
Physical safeguard means to preserve and make information available even within the event of physical challenges. It guarantees sensitive data and critical information technology resources are housed in secure areas.

b. Computational Redundancies
This is applied as fault tolerant against inadvertent faults. It protects computers and storage devices that function as fallbacks in the event of failures.

In-Text Question(s)
What are the cyber security goals?

Answer:
The goals are to ensure the privacy of information, the correctness of data, and access to authorized users.

SELF-ASSESSMENT EXERCISE(S)

1. Discuss the essential components of cyber security goals.

Answer:
The essential components of cyber security goals are confidentiality, integrity and availability. Additionally, as organisations develop their cyber security strategies, they should consider other critical elements such as accountability, assurance, governance and technology. All these are needed for gaining maximum impact in their operations.

4.0 CONCLUSION

In this unit, we get a brief overview of cyber security goals. The Unit identified that the primary goal of cybersecurity is to ensure privacy of information, correctness of data, and access to authorised users. This goal was examined in the three crucial aspects of security which are confidentiality, integrity, and availability of data collectively known as

the CIA Triad. These three major components of cyber security goals and their evolution were described in details in the unit.

5.0 SUMMARY

In this unit we have learnt about:

- the cyber security goals
- the issues around confidentiality
- the problems of integrity
- the concepts of availability

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Brook S. E. Schoenfield. (2020) Secrets of a Cyber Security Architect, CRC Press

Edward Griffor. (2017) Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems Syngress advanced topics in information security, Syngress

Nicholas J. Daras. (2019) Cyber-Security and Information Warfare, Cybercrime and Cybersecurity Research, Nova Science Publishers

Tony Thomas, Athira P Vijayaraghavan, Sabu Emmanuel. (2020) Machine Learning Approaches in Cyber Security Analytics, Springer

Zheng Xu, Kim-Kwang Raymond Choo, Ali Dehghantanha, Reza Parizi, Mohammad Hammoudeh. (2020) Cyber Security Intelligence and Analytics Advances in Intelligent Systems and Computing 928 Springer International Publishing

UNIT 2 CYBER SECURITY PRINCIPLES

CONTENTS

1.0 INTRODUCTION

This unit covers the Cyber Security Principles showing the steps to cybersecurity for organisations and businesses that are looking to protect themselves from the attacks in cyberspace. Ten steps are discussed in the unit as part of the general guidance originally produced by the National Cyber Security Centre (NCSC). Anyone who is interested in effectively achieving cybersecurity should consider these steps guide as discussed in this unit.

The steps discussed in the unit emanated from the first principle of cybersecurity which is focussing on preventing successful cyber adversary campaigns not just preventing breaches. It also concentrates on reducing the probability that those successful cyber adversary operations could happen, not try to stop them altogether.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the economy of mechanism
- Describing the Fail-safe defaults
- Explaining the least privilege and open design
- Understanding complete mediation

- Explaining the separation of privilege and least common mechanism
- Describing the psychological acceptability and work factor

3.0 MAIN CONTENTS

Cyber Security Principles

Various national Governments and the internet industry recognized the necessity to develop a series of Guiding Principles for improving the online security of the ISPs' customers and limit the rise in cyber-attacks. Cybersecurity for these purposes encompasses the protection of essential information, processes, and systems, connected or stored online, with a broad outlook across the people, technical, and physical domains.

These Principles recognize that the web Service Providers and other service providers, internet users, and Governments all have their part in minimizing and mitigating the cyber threats inherent in online access and usage.

The Guiding Principles are developed to react to this challenge by providing a regular approach to help, inform, educate, and protect Internet Service Provider's customers from online crimes. The Principles are ambitious, developed and delivered as a joint venture between Government and Service Providers. These principles identify that ISPs have different sets of consumers, offer different levels of support and services to protect those customers from cyber threats. Some of the essential cybersecurity principles are described below and shown in Figure 2.1.

Figure 2.1: Security Principles

3.1 Economy of Mechanism

This principle states that security mechanisms should be as simple and minute as possible. The principle of economy of mechanism simplifies the design and implementation of security mechanisms with the result of fewer possibilities existing for errors. The checking and testing process could be lesser complicated as fewer components are required for testing.

Interfaces between security modules are the suspicious area which should be as simple as possible. Because interface modules often make implicit assumptions about input or output parameters or this system state. If the any of these assumptions are wrong, the module's actions may produce unpredicted results. Simple security framework facilitates its understanding by developers and users enabling the efficient development and verification of enforcement methods for it.

3.2 Fail-safe Defaults

The Fail-safe defaults principle posits that the default configuration of a system should have a conservative protection scheme. This principle also restricts how privileges are set when a subject or an object is created. Whenever access, rights/privileges, or some security-related attribute isn't overtly granted, the appropriate access, rights/privileges should not be granted unto the object.
Example: When adding a different user to a Windows group in the Microsoft Windows operating system, the default group of the user should have fewer access rights to files and services.

3.3 Least Privilege

This principle states that a user should only have those privileges that are necessary to complete her task. Its primary function is to manage the assignment of rights granted to the user, not the identity of the user. This implies that whether or not the boss demands root access to a UNIX that you are just administering, he/she mustn't have that right unless a task that needs such level of access is to be processed. If possible, the higher level rights of a user identity should be removed as soon as those rights are no longer needed.

3.4 Open Design

This Open design principle states that the protection of a mechanism mustn't depend upon the secrecy of its design or implementation. It suggests that complexity doesn't add security. This principle is that the other of the approach noted as "security through obscurity." This

principle not only applies to information like passwords or cryptographic systems but also to other computer security related operations.

Example: DVD player and Content Scrambling System (CSS) protection method. The CSS could also be a cryptographic algorithm that protects the DVD movie disks from unauthorised copying.

3.5 Complete Mediation

The principle of complete mediation restricts the caching of knowledge, which often leads to simpler implementations of mechanisms. The concept of this principle is that access to every object must be checked for compliance with a protection scheme to substantiate that they are allowed. As a consequence, there should be wary of performance improvement techniques which save the specifics of previous authorisation checks, since the permissions can change over time.
Whenever someone tries to access an object, the system should authenticate the access rights associated with that subject. The subject's access rights are verified once at the first access, and for subsequent accesses, the system assumes that the identical access rights should be accepted for that subject and object. The software package should mediate all and every access to an object.
Example: an internet banking website should require users to sign-in again after a selected period like we'll say, twenty minutes has elapsed.

3.6 Separation of Privilege

This principle states that a system should grant access permission as result of multiple conditions being satisfied, that is not just one condition. This principle may additionally be restrictive because it limits access to system entities. Thus, before privilege is granted, two or more privileges' verifications should be performed.

Example: For a user to su (change) to root, two conditions must be met-

- knowledge of the root password.
- membership of the correct group.

3.7 Least Common Mechanism

This principle states that in systems with multiple users, the mechanisms allowing resources shared by these users should be minimised to the barest as possible. This principle can even be restrictive because it limits the sharing of resources.

Example: If there is a requirement to access a file or application by many users, then these users should use separate channels to access these resources, which help to forestall from unforeseen consequences which may cause security problems.

3.8 Psychological Acceptability

The psychological acceptability principle states that a security mechanism mustn't make the resource more complicated to access if the protection mechanisms weren't present. This principle recognises the human element in computer security. If security-related software applications or computer systems are too complicated to configure, maintain, or operate, the user won't employ the desired security mechanisms. For example, if a password is matched during a password change process, the password changing application or module should state why it had been denied rather than providing a cryptic error message. Simultaneously, applications mustn't impart unnecessary information which will cause a compromise in security.
Example: once we enter a wrong password, the system should only tell us that the user id or password was incorrect. It shouldn't tell us that only the password was wrong as this provides the attacker information for further actions.

3.9 Work Factor

This principle states that the price of circumventing a security mechanism should be compared with the resources of a possible attacker when designing a security scheme. In some cases, the value of circumventing ("known as work factor") will be easily calculated. In other words, the work factor could be a common cryptographic measure which is employed to work out the strength of a given cryptogram. It doesn't map on to cybersecurity, but the concept does apply.

Example: Suppose the quantity of experiments needed to undertake all possible four character passwords is $(24)^4 = 331776$ combinations. If a potential attacker must try each password at a terminal, one might consider a four-character password combination to be adequate. Alternatively, if the potential attacker could use an astronomical computer capable of trying 1,000,000 passwords per second, a four-letter password would be a minor barrier for the intruder.

3.10 Compromise Recording

This principle states that sometimes it's more desirable to record the main points of intrusion than to adopt a more sophisticated measure to forestall it.

Example: The servers in an office network may keep logs for all accesses to files, all emails sent and received, and every one browsing sessions on the internet. Another example is that web-connected surveillance cameras are typical examples of a compromise sound system which will be placed to safeguard a building.

In-Text Question(s)

1. What is the main principle of cyber security?

Answer:

One of the main cyber security principle is to identify security problems before hackers do. This can be done through simulated attack from outside and inside of the organisation.

2. What are the benefits of cyber security?

Answer:
Benefits of cyber security includes amongst others: Data protection from unauthorised access, loss or deletion; Preventing financial fraud and embezzlement; Protection of intellectual property; Prevention of cyber espionage; Prevention of fraud through financial transactions like wire transfers etc. and improved customer confidence.

SELF-ASSESSMENT EXERCISE(S)

1. Discuss the cyber security principles.

Answer:
The security principles are identifying and managing security risks; implementing controls to reduce security risks; detecting and understanding cyber security events to identify cyber security incidents and responding to and recovering from cyber security incidents. The principles are summarised as Confidentiality, Authentication, Integrity, Non-Repudiation and Access control. All these are needed for gaining maximum impact in their operations.

4.0 CONCLUSION

In this unit, we get a brief on the Cyber Security Principles including the economy of mechanism, the Fail-safe defaults, the least privilege and open design, the complete mediation, the separation of privilege and least common mechanism, the psychological acceptability and work factor.

5.0 SUMMARY

In this unit we have learnt about:

- the Cyber Security Principles
- the economy of mechanism
- the Fail-safe defaults
- the least privilege and open design
- the complete mediation
- the separation of privilege and least common mechanism
- the psychological acceptability and work factor

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Marshall Copeland (auth.). (2017) Cyber Security on Azure: An IT Professional's Guide to Microsoft Azure Security Center, Apress,

Marshall Copeland, Matthew Jacobs. (2021) Cyber Security on Azure: An IT Professional's Guide to Microsoft Azure Security, Apress,

UNIT 3 SECURITY POLICIES AND STANDARDS

CONTENTS

1.0 INTRODUCTION

This unit covers the issues of security policies and security standards. It highlights the need for security policies and presents sample cyber security policies and standards. It will familiarize you with the International Organization for Standardization, the Information Technology Act, the Copyright Act, Patent Law and Intellectual Property Rights.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the security policies
- Explaining the need for security policies
- Describing the sample cyber security policies
- Understanding the security standards
- Describing the International Organization for Standardization
- Explaining the information technology act
- Understanding the copyright act
- Understanding the intellectual property rights
-

3.0 MAIN CONTENT

Security Policies and Standards

Security policies are prescribed set of rules which is issued by a corporation to confirm that the user who are authorised to access the company technology and knowledge assets abide by the rules and guidelines associated with the safety of data. It's a written material within the organisation which is liable for a way to protect the organisations from threats and the way to handle them once they will occur. A security policy is also considered to be a "living document" which suggests that the document isn't finished, but it's continuously updated as requirements of the technology and employee change.

Written norms are essential for making cybersecurity procedures explicit. These standards are called as cybersecurity standards, and that they are generic sets of prescriptions for the simplest execution of specific procedures. Methods, guidelines, reference frames, and other items could also be included within the standards. It ensures security efficiency, improves integration and interoperability, allowing for meaningful measure comparisons, minimises complexity, and provides the framework for brand new advancements.

"A published specification that gives a typical language and contains a technical specification or other precise criteria and is meant to be applied consistently, as a rule, a suggestion, or a definition," paraphrasing Wikipedia definition of cybersecurity standards. The aim of security standards is to form information technology (IT) systems, networks, and significant infrastructures safer. The well-written cybersecurity standards promote consistency among product creators and supply a trustworthy benchmark for security product purchases.

Regardless of the dimensions of the business or the industry or sector within which it operates, security guidelines are generally offered. This section contains details on each standard that's generally considered to be a necessary component of every cybersecurity strategy.

3.1 Need for Security Policies

Need of Security policies-

1. It increases efficiency.
   The best thing about having a policy is the ability to extend the amount of consistency which saves time, money and resources. The policy should inform the staff about their individual duties and what they will do and what they can't do with the organisation’s sensitive information.

2. It upholds discipline and accountability
   When any human mistake will occur, and system security is compromised, then the protection policy of the organisation will keep a copy any disciplinary action and also supporting a case in a special court of law. The organisation policies act as a contract which proves that a corporation has taken steps to shield its material possession, its customers and clients from litigations.
3. It can make or break a transaction
   It is not necessary for companies to supply a replica of their information security policy to other vendors during a dealing that involves the transference of their sensitive information. It's true in an exceedingly case of larger businesses which ensures their own security interests are protected when addressing smaller businesses which have less high-end security systems in situ.
4. It helps to teach employees on security literacy
   A well-written security policy can even be seen as an academic document which informs the readers about their importance of responsibility in protecting the organisation sensitive data. It involves on choosing the proper passwords, to providing guidelines for file transfers and information storage which increases employee's overall awareness of security and the way it may be strengthened.

   We use security policies to manage our network security. Many sorts of security policies are automatically created during the installation process and may be customised to suit our particular environment.

3.2 Sample Cyber Security Policies

Here are some important cybersecurity policies recommendations describe below-

1. **Virus and Spyware Protection policy**

This policy provides the following protection:

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

2. **Firewall Policy**

This policy provides the following protection:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals.

- It removes the unwanted sources of network traffic.

3. **Intrusion Prevention policy**
   This policy automatically detects and blocks the network attacks and browser attacks. It also protects applications from vulnerabilities. It checks the contents of one or more data packages and detects malware which is coming through legal ways.
4. **LiveUpdate policy**
   The LiveUpdate policy may be categorised into two types one is LiveUpdate Content policy, and another is LiveUpdate Setting Policy. This policy contains the setting which determines when and the way client computers download the content updates from LiveUpdate. We will define the machines that the clients contact to test for updates and schedule, when and the way clients' computer often check for updates.
5. **Application and Device Control**
   The device control policy protects a system's resources from malware applications and manages the peripheral devices that may attach to a system. This policy applies to both Windows and Macintosh computers whereas application control policy is applied only to Windows clients.
6. **Exception's policy**
   The exception's policy provides the flexibility to exclude applications and processes from detection by the virus and spyware scans.
7. **Host Integrity policy**
   The host integrity policy provides the flexibility to define, enforce, and restore the safety of client computers to stay enterprise networks and data secure. This policy is applied to make sure that the client's computers who access the network are protected and compliant with company's securities policies. This policy requires that client system must have antivirus software installed.

3.3 International Organisations for Standardisation

The standards devised by the International Organisation for Standardisation (ISO) provide a world-class specification for services, products and computers, to confirm quality, safety and efficiency. These standards are instrumental in facilitating international trade.

ISO standard is officially founded on 23 February 1947 as an independent, non-governmental international organisation. Currently, the total membership consists of 162 national standards bodies and 784 technical committees and subcommittees taking care of standards development. ISO has published well over 22336 International

Standards and its related documents that covers almost every industry, from food safety to information technology, to healthcare and agriculture.

ISO 27000 Series
It is the family of data security standards which is developed by the ISO and also the International Electrotechnical Commission to produce a globally recognized framework for best information security management. It assists organisations in keeping their information assets secure like employee details, intellectual properties, and financial information.

The need for ISO 27000 series arises due to the chance of cyber-attacks that organisations face. The cyber-attacks are growing daily making hackers a relentless threat to any industry that uses technology.

The ISO 27000 series is categorized variously, such as: -

1. ISO 27001- This standard allows us to prove the clients and stakeholders of any organisation to managing the simplest security of their confidential data and data. This standard involves a process-based method for establishing, implementing, operating, monitoring, maintaining, and improving our ISMS.

2. ISO 27000- This standard provides a description of terminologies utilised in ISO 27001.

3. ISO 27002- This standard provides guidelines for organisational information security standards and knowledge security management practices. It takes account of the choice, implementation, operating and management of controls taking into consideration the organisation's information security risk environment(s).

4. ISO 27005- This standard supports the overall concepts laid out in 27001. it's designed to supply the rules for implementation of data security supported a risk management approach. To completely understand the ISO/IEC 27005, the knowledge of the concepts, models, processes, and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is required. This standard is capable for all types of organisations like non-government organisation, government agencies, and commercial enterprises.

5. ISO 27032- The International Standard which focuses explicitly on cybersecurity. This Standard includes guidelines for shielding information beyond the boundaries of a corporation like in

collaborations, partnerships or other information sharing arrangements with suppliers and clients.

3.4 Information Technology Act

The Information Technology Act also referred to as ITA-2000, or the IT Act has the main aim of offering the legal infrastructure worldwide in relation to cybercrime and e-commerce. The IT Act relies on the international organisation Model Law on E-Commerce 1996 recommended by the overall Assembly of UN. This act is additionally applied in checking misuse of cyber network and computer in worldwide. Officially passed in 2000, the Act was amended in 2008. It's been designed to offer enhancement to electronic commerce, e-transactions and related activities related to commerce and trade. It also facilitates electronic governance by using reliable electronic records.

IT Act 2000 has 13 chapters, 94 sections and 4 schedules where the primary 14 sections concern digital signatures and other sections accommodating the certifying authorities who are licenced to issue digital signature certificates. While sections 43 to 47 provide penalties and compensation, section 48 to 64 contains appeal to state supreme court and sections 65 to 79 handle offences, and also the remaining section 80 to 94 cope with miscellaneous of the Act.

3.5 Copyright Act

The Copyright Act, that was enacted in 1957 and amended by the Copyright Amendment Act 2012 and governs the topic of copyright law. Copyright could be a legal term which defines the ownership of control of the rights to the authors of "original works of authorship" that are fixed with a tangible style of expression. A unique work of authorship could be a distribution of certain works of creative expression including books, computer programs, movies, video, and music. The copyright law has been legislated to balance the utilization and reuse of creative works against the will of the creators of art, literature, music and monetise their work by controlling who can make and sell copies of the work.

The act covers the following-

- Rights of copyright owners
- List of protection eligible Works
- Copyright Duration
- Who can claim copyright?

The copyright act doesn't cover the following-

- Methods, processes, procedures, ideas, concepts, systems, principles, or discoveries
- Works that aren't of a tangible form (such as an improvisational speech that has not been written down or a choreographic work that has not been recorded)
- Familiar designs or symbols
- Titles, names, slogans, and short phrases
- Mere variations of typographic ornamentation, lettering, or colouring

3.6 Patent Law

A law that deals with new inventions is referred to as Patent Law. Traditionally, a patent law in principle protect tangible scientific inventions, like circuit boards, heating coils, car engines, or zippers. As time goes on, patent laws are applied in protecting a broader range of inventions like business practices, coding algorithms, or genetically modified organisms. The baseline of this law is the exclusion rights of others people from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.

In general, a patent may be a right that may be granted if an invention is:

- Not a physical object or process
- New
- Useful
- Not obvious.

3.7 Intellectual Property Rights

Intellectual property rights (IPR) are rights which allow creators, or owners of patents, trademarks or copyrighted works to profit from their own plans, ideas, or other intangible assets or investment in a creative work. These IPRs are outlined within the Article 27 of the Universal Declaration of Human Rights. It provides for the possibility to earn profit from the protection of ethical and material interests resulting from authorship of scientific, literary or artistic productions. These property rights allow the holder to exercise a domination on the usage of the item for a specified period.

In-Text Question(s)

1. What are security policies?

Answer:
A security policy is a documented approach that an organisation plans to protect its physical and information technology (IT) assets usually stated and communicated to users in the organisation. policies govern the actions of people,

2. What are security standards?

Answer:
Security standards are set of rules emanating from organisational policies for products or processes that provides consistency, accountability, and efficiency. Standards provide a repeatable way of doing things.

SELF-ASSESSMENT EXERCISE(S)

i. Discuss the security policies presented in this unit.

Answers:
Acceptable use policy; Data breach response policy; Disaster recovery plan; Business continuity plan; Remote access policy; Access control policy.

ii. Discuss the protection standards presented in this unit.

Answer:
ISO 27001. This is one of the common standards that adhere to the organization to implement an Information security management system.
There are other standards such as PCI DSS that stands for Payment Card Industry and Data Security Standard, HIPAA stands for Health Insurance Portability and Accountability Act.

4.0 CONCLUSION

In this unit, we get a brief on security policies. The unit explains the need for Security Policies and describes sample cyber security policies. In this unit, we get a brief on security standards. The unit describes how security standards evolved and it familiarizes you with some of the standards such as the International Organization for Standardization, the Information Technology Act, the Copyright Act, the Patent Law and Intellectual Property Rights.

5.0 SUMMARY

In this unit we have learnt about:
In this unit we have learnt about:

- the available security policies
- the need for security policies
- sample cyber security policies
- the International Organization for Standardization
- the Information Technology Act
- the Copyright Act
- the Patent Law
- the Intellectual Property Rights

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Aaron Franklin Brantly, William Keller, Scott Jones (2016). The Decision to Attack: Military and Intelligence Cyber Decision-Making Studies in Security and International Affairs Studies in Security and Intern.

Carol A. Siegel, Mark Sweeney (2020). Cyber Strategy: Risk-Driven Security and Resiliency Auerbach Publications

Edward J. M. Colbert, Alexander Kott (eds.) (2016). Cyber-security of SCADA and Other Industrial Control Systems Advances in Information Security 66, Springer International Publishing.

Gerard Johansen (2017). Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents, Packt Publishing.

Gupta, Brij, Sheng, Quan Z. (2019) Machine learning for computer and cyber security: principles, algorithms, and practices, CRC Press.

Izzat Alsmadi (2019). The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics, Springer International Publishing.

MODULE 2 CYBER SECURITY CHALLENGES AND RISK ANALYSIS

Unit 1 Cyber Security Challenges
Unit 2 Cyber Security Risk Analysis
Unit 3 Cyber Security Threats
Unit 4 Cyber Security Threat to E-commerce

MODULE INTRODUCTION

This module consists of four units and introduces the learners to Cyber Security Challenges and Risk Analysis. It examined in the details the issues of Cyber Security Challenges, Cyber Security Risk Analysis, Cyber Security Threats and Cyber Security Threats to E-Commerce.

UNIT 1 CYBER SECURITY CHALLENGES

CONTENTS

1.0 INTRODUCTION

This unit covers the cyber security challenges as demonstrated in such areas as Ransomware Evolution, Blockchain Revolution, Internet of Things (IoT) Threats, Artificial Intelligence (AI) Expansion and Serverless Apps Vulnerability.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the Ransomware Evolution
- Describing the Blockchain Revolution
- Explaining the Internet of Things (IoT) Threats
- Understanding Artificial Intelligence (AI) Expansion
- Describing Serverless Apps Vulnerability

3.0 MAIN CONTENT

Cyber Security Challenges
Nowadays, cybersecurity is that the main component of every country's overall national security and economic security strategies. Everywhere on the planet, there are such several number of challenges associated with cybersecurity. With the rise of the cyber-attacks, every organization needs a security analyst who makes sure that their system is secured. These security analysts face many challenges associated with cybersecurity like securing confidential data of state organizations, securing the private organization servers, etc.

The recent important cybersecurity challenges are described below:

3.1 Ransomware Evolution

Ransomware may be a sort of malware within which the information on a victim's computer is locked, and payment is demanded before the ransomed data is unlocked. When payment has been received successful, the victim will have access rights returned to her. Ransomware is the main nuisance of cybersecurity, bane of data professionals, and misery of IT executives.

Ransomware attacks are growing day by day within the areas of cybercrime as depicted in Figure 3.1. IT professionals and business leaders must have a strong recovery strategy against the malware attacks to guard their organization. It involves proper getting to recover corporate and customers' data and application furthermore as reporting any breaches against the Notifiable Data Breaches scheme. Today's Disaster recovery as a service (DRaaS) solutions are the simplest defence against the ransomware attacks. With DRaaS solutions method, we will automatically make a copy our files, easily identify which backup is clean, and launch a fail-over with the press of a button when malicious attacks corrupt our data.

The IBM cyber security intelligence index report 2022 showed that Ransomware was the number one attack type observed by X-Force last year, decreasing to 21% of attacks from 23% in the previous year. The IBM X-Force 's Threat Intelligence Reports https://www.ibm.com/downloads/cas/ADLMYLAZ is shown in Figure 3.2.

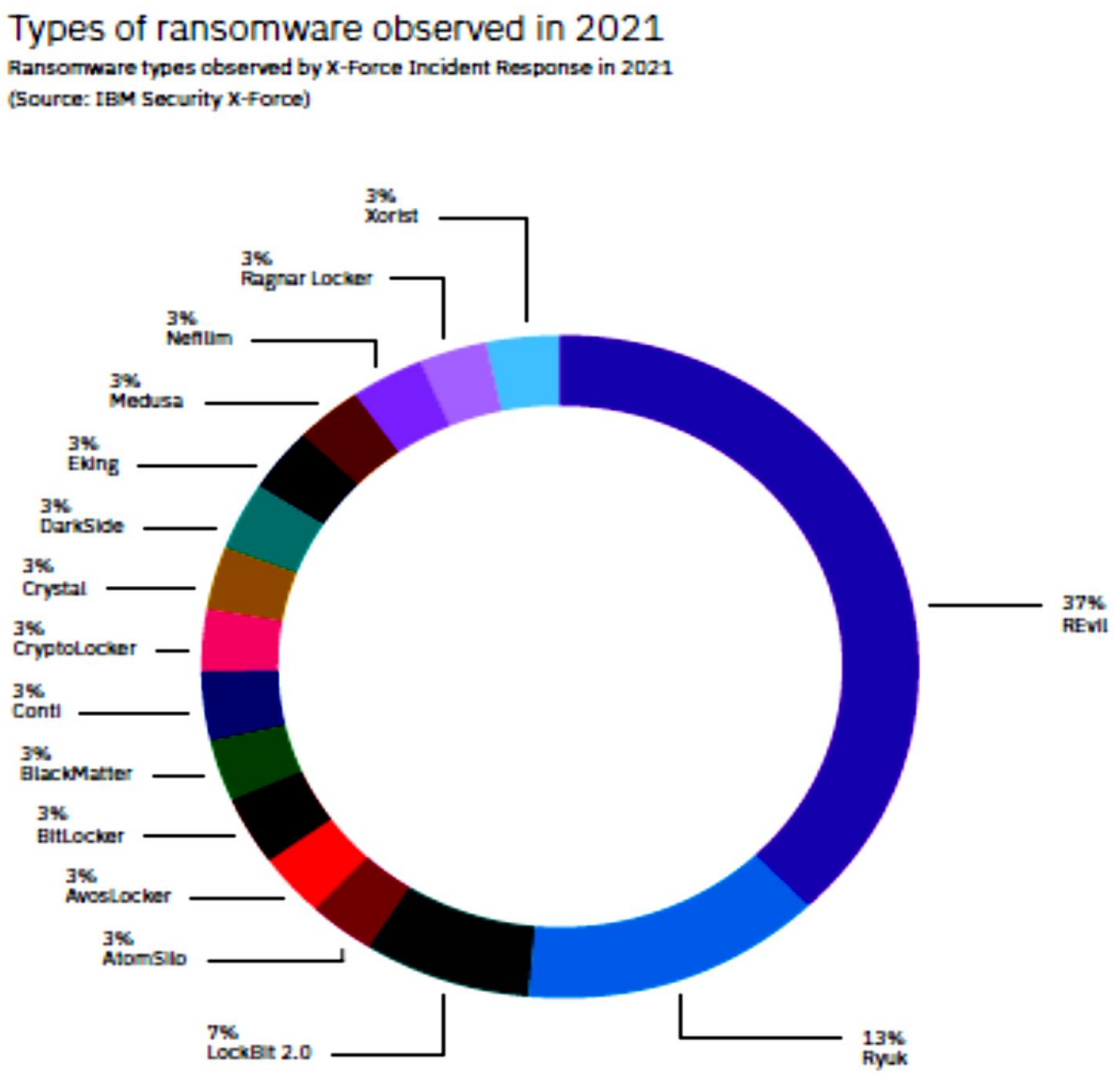

Figure 3.1: Types of Ransomware observed in 2021

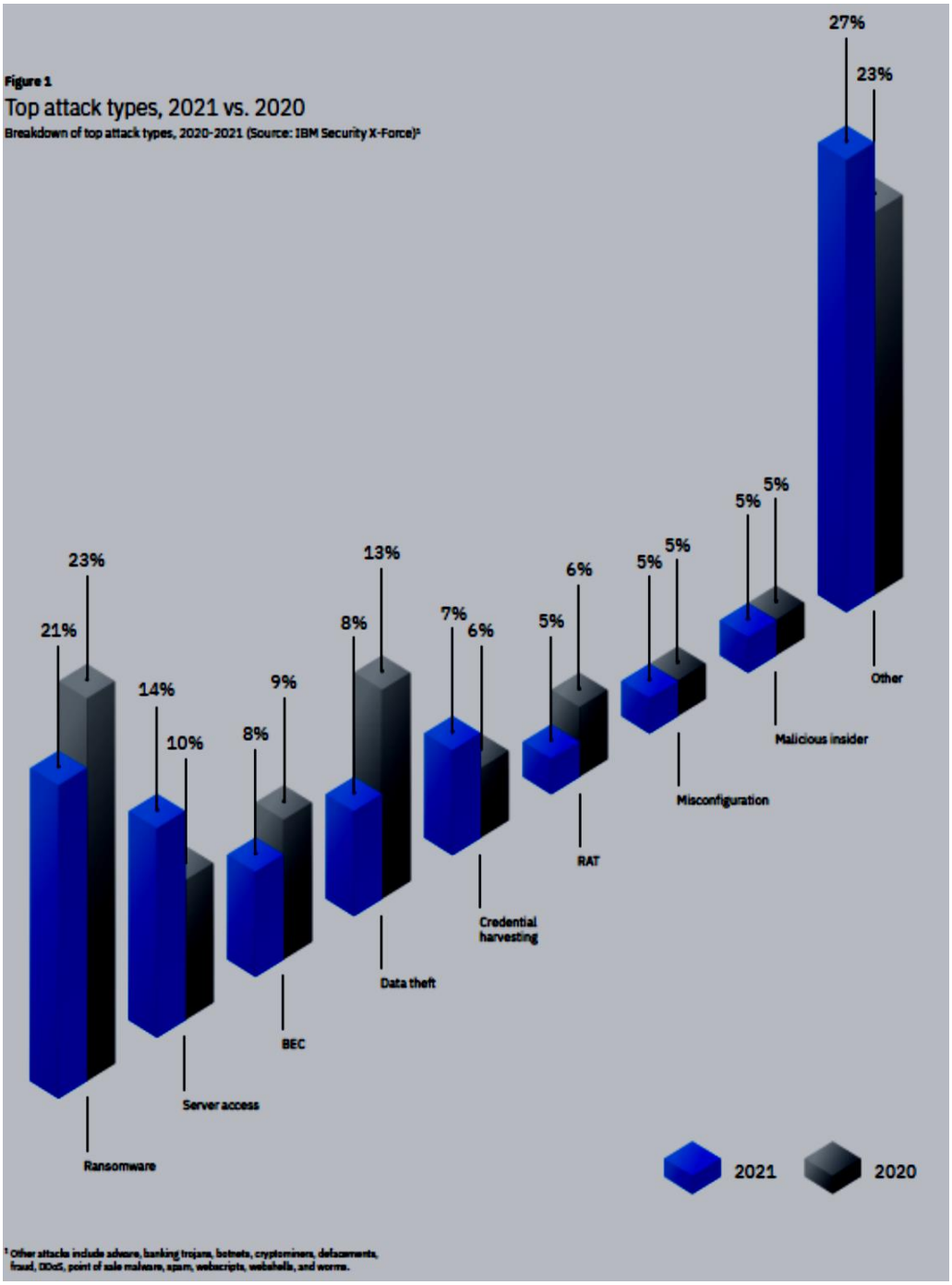

Figure 3.2: Top Attack Types in 2020 and 2021

3.2 Blockchain Revolution

Blockchain technology is the most significant invention in computing era. it's the primary time in human history that we've a genuinely native digital medium for peer-to-peer value exchange. The blockchain may be a technology that allows cryptocurrencies like Bitcoin. The blockchain could be a vast global platform that enables two or more parties to try and do a transaction or do business without having a 3rd party for establishing trust.

It is difficult to predict what blockchain systems will offer with reference to cybersecurity but cybersecurity professionals can make some informed guesses regarding blockchain. With the increased application and utilisation of blockchain within cybersecurity context, there'll be a healthy tension but also complementary integrations with traditional, proven, cybersecurity approaches.

3.3 Internet of Things (IoT) Threats

Internet of Things is a system of interrelated physical devices which might be accessible through the net. The linked physical devices have a unique identifier (UID) and have the flexibility to transfer data over a network with no requirements of the human-to-human or human-to-computer interaction. The firmware and software which is running on IoT devices make consumer and businesses highly vulnerable to cyber-attacks.

When IoT things were designed, it's not envisaged the possible utilisation in cybersecurity and for commercial purposes. So every organisation has to work with cybersecurity professionals to confirm the protection of their password policies, session handling, user verification, multifactor authentication, and security protocols to assist in managing the danger.

3.4 AI Expansion

In line with John McCarthy (https://www.youtube.com/watch?v=Ozipf13jRr4) , father of Artificial Intelligence (AI) defined AI: "The science and engineering of constructing intelligent machines, especially intelligent computer programs."
It is a branch of computer technology associated with the creation of intelligent machines that work and react like humans. a number of the activities associated with AI include speech recognition, Learning, Planning, Problem-solving, etc. The key benefits with AI in cybersecurity strategy is that it could protect and defend an environment when the malicious attack begins, thus mitigating the impact. AI take immediate action against the malicious attacks at a flash when threats impact a business. IT business leaders and cybersecurity strategy teams consider AI as a future protective control that may allow our business to remain prior the cybersecurity technology curve.

3.5 Serverless Apps Vulnerability

Serverless architecture and apps are applications that depend upon third-party cloud infrastructures or back-end services like google cloud function, Amazon web services (AWS) lambda, etc. The serverless apps invite the cyber attackers to spread threats on their system easily because the users access the appliance locally or off-server on their device. Therefore, it's the user responsibility for the safety precautions while using serverless application.

The serverless apps do nothing to stay the attackers removed from your data. The serverless application doesn't help if an attacker gains access to your data through a vulnerability like leaked credentials, a compromised insider or by the other means then serverless.

We can run software with the applying which provides best chance to defeat the cybercriminals. The serverless applications are typically small. It helps developers to launch their applications quickly and simply. they do not must worry about the underlying infrastructure. The web-services and processing tools are samples of the foremost common serverless apps.

In-Text Question(s)

1. What is a blockchain and what functions does it perform?

Answer:
A blockchain is a digital journal of transactions maintained by a network of computers in a way that makes it difficult to hack or alter. It works by giving a secure way for individuals to deal directly with each other.

2. Differentiate between serverless and server based applications
Answer:
Serverless applications the focus is on coding instead of server maintenance. It is more affordable, scalable, and time-efficient. Server based applications ensures unlimited access to data, even with no internet connection with more control.

SELF-ASSESSMENT EXERCISE(S)

i. Discuss the applications available to provide cyber security.

Answer:
Cyber security is the application of technologies, processes and controls to safeguard computer systems and networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and

protect against the unauthorised exploitation of systems, networks and technologies. Such applications include: SecurityAnywherel Avast Mobile Security, SafeDNS, MalwareBytes, Secure Call, LastPass.

4.0 CONCLUSION

In a world where everything is on the internet, Cyber Security is becoming a severe issue for individuals, enterprises, and governments alike. Ensuring that our data remains safe is one of the biggest challenges of Cyber Security. This unit examined some Cyber Security challenges such as ransomware, phishing attacks, malware attacks, and more. The Unit further described cyber security challenges inherent in such areas as Ransomware Evolution, Blockchain Revolution, Internet of Things (IoT) Threats, Artificial Intelligence (AI) Expansion and Serverless Apps Vulnerability.

5.0 SUMMARY

In this unit we have learnt about:
• the cyber security challenges
• the Ransomware Evolution
• the Blockchain Revolution
• the Internet of Things (IoT) Threats
• the Artificial Intelligence (AI) Expansion
• the Serverless Apps Vulnerability

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Agrawal, Dharma Prakash, Gupta, Brij, Wang, Haoxiang.(2019) Computer and cyber security: principles, algorithm, applications, and perspectives, CRC Press.

David Sutton. (2017) Cyber security: A practitioner's guide, Swindon, United Kingdom BCS, the Chartered Institute for IT.

Eugenie de Silva. (2016) National Security and Counterintelligence in the Era of Cyber Espionage Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) IGI Global.

Kuan-Ching Li & Brij B. Gupta & Dharma P. Agrawal. (2021) Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS).

Martti Lehto, Pekka Neittaanmäki. (2015) Cyber Security: Analytics, Technology and Automation Intelligent Systems, Control and Automation: Science and Engineering 78 Springer International Publishing.

Thomas Edgar and David Manz (Auth.). (2017) Research Methods for Cyber Security, Syngress.

https://www.youtube.com/watch?v=Ozipf13jRr4

UNIT 2 CYBER SECURITY RISK ANALYSIS

CONTENTS

1.0 INTRODUCTION

Essentially every organisation has internet connectivity and some form of information technology infrastructure, that means almost all entities are at risk of a cyber-challenge. Understanding the level of the risks and being able to manage it, requires that organisations carry out a cybersecurity risk assessment. This will assist in identifying which assets are most vulnerable to the risks faced by such organisation. This unit covers the cyber security risk analysis. This unit will familiarize you with the benefits of risk analysis and steps to be taken in the risk analysis process. It also highlights the available types of risk analysis.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the cyber security risk analysis
- Describing the types of risk analysis
- Explaining the benefits of risk analysis
- Understanding the steps in the risk analysis process

3.0 MAIN CONTENT

Cyber Security Risk Analysis

Risk analysis refers to the review of risks related to the actual action or event. The concept of risk analysis is applicable to information technology, projects, security issues and the other event where risks could also be analysed using a quantitative and qualitative approach. Risks are a part of every IT project and business organisations. The analysis of risk should occur on an everyday basis and be updated to

spot new potential threats. The strategic risk analysis helps to attenuate the longer term risk probability and damage.
Enterprises and organisations used risk analysis to:

- anticipates and reduce the effect of harmful results that may occur from adverse events.
- plan for technology or equipment disaster or loss from adversarial events both natural and human induced.
- evaluate whether the potential risks of a project are balanced within the decision process when evaluating to maneuver forward with the project
- identify the impact of and prepare for changes in the enterprise environment.

3.1 Benefits of Risk Analysis

Every organization needs to understand about the risks associated with their information systems to protect their IT assets effectively and efficiently. Risk analysis can help an organization to improve their security in many ways. These are:

- Concerning financial and organizational impacts, it identifies, rate and compares the overall impact of risks related to the organization.
- It helps to identify gaps in information security and determine the next steps to eliminate the risks of security.
- It can also enhance the communication and decision-making processes related to information security.
- It improves security policies and procedures as well as develop cost-effective methods for implementing information security policies and procedures.
- It increases employee awareness about risks and security measures during the risk analysis process and understands the financial impacts of potential security risks.

3.2 Steps in the Risk Analysis Process

1. Conduct a risk assessment survey:
   Getting the input from management and department heads is critical to the risk assessment process. The risk assessment survey refers to begin documenting the specific risks or threats within each department.
2. Identify the risks:
   This step is used to evaluate an IT system or other aspects of an organization to identify the risk related to software, hardware, data, and IT employees. It identifies the possible adverse events

that could occur in an organization such as human error, flooding, fire, or earthquakes.

3. Analyse the risks:
   Once the risks are evaluated and identified, the risk analysis process should analyse each risk that will occur, as well as determine the consequences linked with each risk. It also determines how they might affect the objectives of an IT project.
4. Develop a risk management plan:
   After analysis of the Risk that provides an idea about which assets are valuable and which threats will probably affect the IT assets negatively, we would develop a plan for risk management to produce control recommendations that can be used to mitigate, transfer, accept or avoid the risk.
5. Implement the risk management plan:
   The primary goal of this step is to implement the measures to remove or reduce the analyses risks. We can remove or reduce the risk from starting with the highest priority and resolve or at least mitigate each risk so that it is no longer a threat.
6. Monitor the risks:
   This step is responsible for monitoring the security risk on a regular basis for identifying, treating and managing risks that should be an essential part of any risk analysis process.

3.3 Types of Risk Analysis

Qualitative Risk Analysis

- The qualitative risk analysis process is a project management technique that prioritizes risk on the project by assigning the probability and impact number. Probability is something a risk event will occur whereas impact is the significance of the consequences of a risk event.
- The objective of qualitative risk analysis is to assess and evaluate the characteristics of individually identified risk and then prioritize them based on the agreed-upon characteristics.
- The assessing individual risk evaluates the probability that each risk will occur and effect on the project objectives. The categorizing risks will help in filtering them out.
- Qualitative analysis is used to determine the risk exposure of the project by multiplying the probability and impact.

Quantitative Risk Analysis

- The objectives of performing quantitative risk analysis process provide a numerical estimate of the overall effect of risk on the project objectives.

- It is used to evaluate the likelihood of success in achieving the project objectives and to estimate contingency reserve, usually applicable for time and cost.
- Quantitative analysis is not mandatory, especially for smaller projects. Quantitative risk analysis helps in calculating estimates of overall project risk which is the focus.

In-Text Question(s)

1. Enumerate the steps in risk analysis.

Answer:

Step 1: Determine the scope of the risk assessment
Step 2: Identify assets
Step 3 Identify threats
Step 3: Analyse risks and determine potential impact
Step 4: Determine and prioritize risks
Step 5: Document all risks

2. Differentiate between quantitative and qualitative analyses.

Answer:

The basis for risk analyses is main difference between qualitative and quantitative risk analysis. Qualitative risk analysis is based on a person's observation or judgment while quantitative risk analysis is based on tested and specific data.

SELF-ASSESSMENT EXERCISE(S)

i. Discuss the different phases of risk analysis.

Answer:

Risk analysis or assessment is composed of: Risk identification, Risk analysis and Risk evaluation. The steps to be taken to manage risk are referred to as the risk management process. The steps start with identifying risks, then risk analysed, then the risk is prioritised, followed by the implementation of solution, and finally, the risk is monitored.

4.0 CONCLUSION

Alleviating the risks identified during the risk analysis will prevent and reduce costly security incidents and data breaches and avoid regulatory and compliance issues. In this unit, we get a brief on cyber security risk analysis, describing the steps in the risk analysis. We were familiarised with the available types of risk analysis and the benefits of risk analysis. Generally, it was shown that risk assessment process also obliges everyone within an organisation to consider how cybersecurity risks can

impact the organisation's objectives, which helps to create a more risk-aware culture.

5.0 SUMMARY

In this unit we have learnt about:

- the cyber security risk analysis
- the benefits of risk analysis
- the steps in the risk analysis process
- the types of risk analysis

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Agrawal, Dharma Prakash, Gupta, Brij, Wang, Haoxiang. (2019) Computer and cyber security: principles, algorithm, applications, and perspectives, CRC Press.

David Sutton. (2017) Cyber security: A practitioner's guide, Swindon, United Kingdom BCS, the Chartered Institute for IT.

Eugenie de Silva. (2016) National Security and Counterintelligence in the Era of Cyber Espionage Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) IGI Global.

Kuan-Ching Li & Brij B. Gupta & Dharma P. Agrawal. (2021) Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS).

Martti Lehto, Pekka Neittaanmäki. (2015) Cyber Security: Analytics, Technology and Automation Intelligent Systems, Control and Automation: Science and Engineering 78 Springer International Publishing.

Thomas Edgar and David Manz (Auth.). (2017) Research Methods for Cyber Security, Syngress.

UNIT 3 CYBER SECURITY THREATS

CONTENTS

1.0 INTRODUCTION

Cyber threats are a big problem and can cause electrical blackouts, catastrophe of military equipment, and breaches of nation-wide security secrets. They can result in the stealing of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyse systems, making data unavailable. This unit covers the Types of Cyber Security Threats. It presents the details of different types of threats and methods of mitigation. The unit concludes by highlighting the latest cyber threats across the world.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the Malware method
- Describing the Phishing method
- Explaining Man-in-the-Middle Attack
- Understanding how Distributed Denial of Service works
- Describing the Brute Force
- Explaining the SQL Injection
- Understanding the Domain Name System Attack
- Describing the Latest Cyber Threats

3.0 MAIN CONTENT

Types of Cyber Security Threats

A threat in cybersecurity could be a malicious activity by a personal or organization to corrupt or steal data, gain access to a network, or disrupts digital life generally. The cyber community defines the subsequent threats available today:

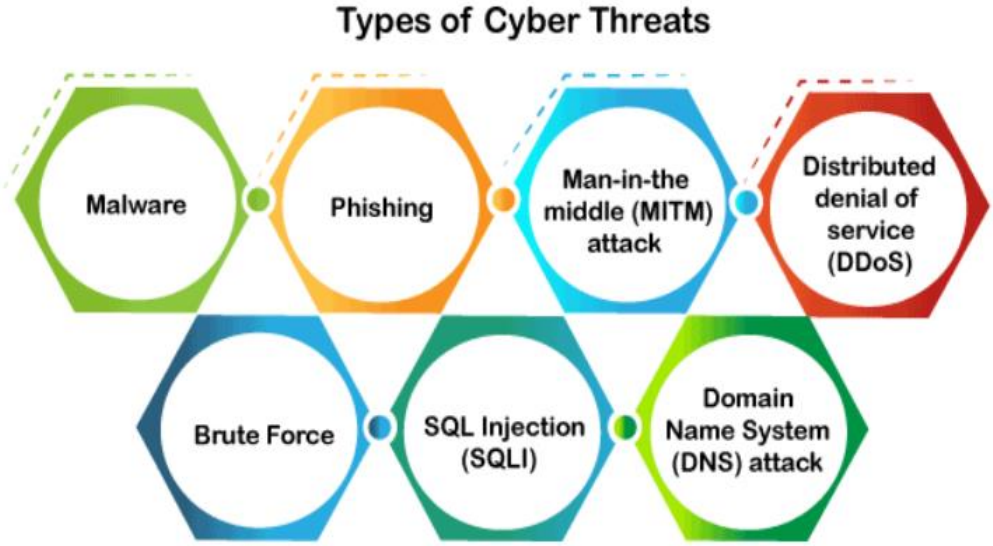

Figure 3.1: Types of Cyber Threats

3.1 Malware

- Malicious software (Malware) could be a most typical cyber attacking tool employed by the cybercriminal or hacker to disrupt or damage a legitimate user's system. The underlisted are the important types:
- Virus: it's a malicious piece of code that spreads amongst different devices i.e. from one device to a different one. It can clean files and spreads throughout a network of computing system, infecting files, stealing information, or damage device.
- Spyware: it's an application software that secretly records information about user activities on their system. as an example, spyware could capture mastercard details which will be utilised by the cybercriminals for unauthorized shopping, money withdrawing, etc.
- Trojans: this is a sort of malware or code that appears as legitimate software or file to fool us into downloading it and running it. Its main purpose is to alter or steal data from our devices or carry out other destructive activities on our network.
- Ransomware: it is a piece of software that encrypts a user's files and data on a machine, rendering them unusable or erasing them. Thereafter, a financial ransom is demanded by the mischievous actors for decryption.

- Worms: it's a type of application software that spreads copies of itself from device to device without human interaction. It doesn't require them to connect themselves to any program to steal or damage the information.
- Adware: it's an advertising software application wont to spread malicious software and displays advertisements on our devices. It's an unwanted program that's installed without the user's permission with the sole objective of getting revenue for its developer by showing the ads on their browsers.
- Botnets: it's a set of internet-connected malware-infected devices that allow cybercriminals to regulate them. It enables cybercriminals to induce credentials leaks, unauthorized access, and information theft without the user's permission.

3.2 Phishing

Phishing could be a style of cybercrime within which a sender seems to return from a real organisation like PayPal, eBay, financial institutions, or friends and colleagues. They contact a target or targets via email, phone, or text message with a link to steer them to click thereon links. This link will redirect them to fraudulent websites to produce sensitive data like personal information, banking and mastercard information, Social Security numbers, usernames, and passwords. Clicking on the link will install malware on the target devices that allow hackers to manage devices remotely.

3.3 Men-in-the-Middle Attack

A man-in-the-middle attack could be a kind of cyber threat (a type of eavesdropping attack) during which a cybercriminal intercepts a conversation or data transfer between two individuals. Once the cybercriminal places themselves within the middle of a two-party communication, they appear like genuine participants and might get sensitive information and return different responses. the key objective of this sort of attack is to obtain access to our business or customer data. as an example, a cybercriminal could intercept data passing between the target devices and also the network on an unprotected Wi-Fi network.

3.4 Distributed Denial of Service (DDoS)

It is a sort of cyber threat or malicious attempt where cybercriminals disrupt targeted servers, services, or network's regular traffic by fulfilling legitimate requests to the target or its surrounding infrastructure with Internet traffic. Here the requests come from several IP addresses which will make the system unusable, overload their

servers, slowing down significantly or temporarily taking them offline, or preventing a user or corporation from effecting its vital functions.

3.5 Brute Force

A brute force attack could be a cryptographic hack that uses a trial-and-error method to guess all possible combinations until the right information is discovered. Cybercriminals usually use this attack to get personal information about targeted passwords, login info, encryption keys, and private/personal identification numbers.

3.6 SQL Injection (SQLI)

SQL injection could be a common attack that happens when cybercriminals use malicious SQL scripts for backend database manipulation to access sensitive information. Once the attack is successful, the malicious actor can view, change, or delete sensitive company data, user lists, or private customer details stored within the SQL database.

3.7 Domain Name System (DNS) Attack

A Domain Name System attack may be a variety of cyberattack during which cyber criminals make the most of the flaws within the name system to redirect site users to malicious websites (DNS hijacking) and steal data from affected computers. It's a severe cybersecurity risk because the DNS system is a necessary element of the net infrastructure.

3.8 Latest Cyber Threats

The following are the most recent cyber threats reported by the U.K., U.S., and Australian governments:

Romance Scams
The U.S. government found this cyber threat in February 2020. This is a threat used by Cybercriminals within dating sites, chat rooms, and apps. They attack people that are seeking a brand new partner and deceiving them into giving for free personal data.

Dridex Malware
It is a sort of economic Trojan malware identifies by the U.S. in December 2019 that affects the general public, government, infrastructure, and business worldwide. It infects computers through phishing emails or existing malware to steal sensitive information like passwords, banking details, and private data for fraudulent transactions. The National Cyber Security Centre of the UK encourages people to

form sure their devices are patched, anti-virus is turned on and up to this point, and files are insured to safeguard sensitive data against this attack.

Emotet Malware
Emotet may be a variety of cyber-attack that steals sensitive data and also installs other malware on the target device. The Australian Cyber Security Centre cautioned users and national organisations about this world-wide cyber threat in 2019. It should be noted every system is susceptible to security breaches and attacks.

In-Text Question(s)
i. List a number of the common cyber threats

Answer:
Common cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS), and injection attacks.

ii. How can fraud be prevented?

Answer:
Fraud can be prevented by putting in place threat mitigating policies and procedures in an organisation

SELF-ASSESSMENT EXERCISE(S)

i. Discuss the non-physical threats in cyber security.

Answer:
A non-physical threat in cyber security is a potential cause of an incident that may result in; Loss or corruption of system data; Disruption of business operations that rely on computer systems and Loss of sensitive information.

4.0 CONCLUSION

In this unit, we get a brief on the malware method

- Describing the phishing method
- Explaining Man-in-the-Middle Attack
- Understanding how distributed denial of service works
- Describing the brute force
- Explaining the SQL Injection
- Understanding the Domain Name System Attack
- Describing the Latest Cyber Threats

5.0 SUMMARY

In this unit we have learnt about:

- the Malware and Phishing attacks
- the Man-in-the-Middle Attack and brute force
- the problems in communications and their solutions
- how Distributed Denial of Service works
- the SQL Injection and the Domain Name System Attack
- the Latest Cyber Threats

6.0 REFERENCES/FURTHER READING

7.0 REFERENCES/FURTHER READING

Clark, Ceri. (2015) A simpler guide to online security for everyone: how to protect yourself and stay safe from fraud, scams and hackers with easy cyber security tips for your Gmail, Docs and other Google services. Simpler Guides Ceri Clark; Lycan Books.

Mamoun Alazab, MingJian Tang. (2019) Deep Learning Applications for Cyber Security Advanced Sciences and Technologies for Security Applications, Springer International Publishing.

Nicholas Kolokotronis & Stavros Shiaeles. (2021) Cyber-Security Threats, Actors, and Dynamic Mitigation, CRC Press.

Robert E. Davis. (2021) Auditing Information and Cyber Security Governance: A Controls-Based Approach Internal Audit and IT Audit 0367568500, 9780367568504 CRC Press.

UNIT 4 CYBER SECURITY THREAT TO E-COMMERCE

CONTENTS

1.0 INTRODUCTION

As was identified in Unit 3 of this module, there are threats and attack generally in the cyber space. This unit covers some of the Cyber Security Threats to Electronic Commerce (e-Commerce). The threat landscape for e-Commerce cybersecurity is evolving rapidly. These attacks mostly compromised payment data, login credentials and personal information of the users. Due to the COVID-19 pandemic, greater reliance on online shopping has also increased the likelihood of attacks on e-Commerce sites. The unit seeks to investigate possible threats with Electronic Payments System and highlights the associated financial risks of Credit / Debit Card Fraud and Tax Evasion.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the security threats to e-commerce
- Describing the electronic payment system
- Explaining the Risk of Fraud and Tax Evasion
- Understanding the associated financial risks of Payment Conflict
- Understanding E-Cash and Credit / Debit Card Fraud
- Using Automated Teller Machine (ATM)

3.0 MAIN CONTENT

Cyber Security Threats to E-Commerce
The action of buying and selling products over the net is e-commerce. It's simply commercial transactions that happen over the web. Mobile commerce, Internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data exchange (EDI), inventory management systems, and automatic data gathering systems are all samples of e-commerce technology.

The use of the web for unfair means with the goal of stealing, fraud, and security breach constitutes an e-commerce threat. E-commerce dangers are available with a spread of shapes and sizes. Some are unintentional, some are deliberate, and a few are the results of human error. Electronic payment systems, e-cash, data abuse, credit/debit card frauds, and other security risks are the foremost widespread.

3.1 Electronic Payments System

With the rapid development of the personal computer, mobile, and network technology, e-commerce has become a routine, a part of human life. In e-commerce, the customer can order products reception and save time for doing other things. There’s no need of visiting a store or a store. The customer can select different stores on the net during a very short time and compare the products with different characteristics like price, colour, and quality.

The electronic payment systems have a really important role in e-commerce. E-commerce organizations use electronic payment systems that visit paperless monetary transactions. It transformed the business processing procedures by reducing paper works, operational costs, and labour cost. E-commerce processing is user-friendly and with reduced time consuming than manual processing. Electronic commerce helps a business organisation expand its market reach expansion. There are certain risks with the electronic payments system and a few of them are:

3.2 Evasion of Tax

The Internal Revenue Service law requires that each business declare their financial transactions and supply paper records in order that tax compliance will be verified. the matter with electronic systems is that they do not key in cleanly into this paradigm. It makes the method of collection very frustrating for the Revenue Service. It's at the business's option to disclose payments received or made via electronic payment systems. The Internal Revenue Service has no system in place to know

whether the business is declaring the reality or not, that creates the avenue to evade taxation easily.

3.3 Payment Conflict

In electronic payment systems, the payments are handled by an automatic electronic system, not by humans. The system is at risk of errors when it handles large amounts of payments on a frequent basis with quite one recipient involved. It's essential to continually check our pay slip after every pay period ends so as to make sure everything is correct. Our failure to try and do this, may lead to conflicts of payment caused by technical glitches and anomalies.

3.4 E-Cash

E-cash may be a paperless cash system which facilitates the transfer of funds anonymously. E-cash is offered without charges to the user while the sellers have paid a fee for this. The e-cash fund may be either stored on a users' card itself or in an account which is related to the card. The foremost common samples of e-cash system are transit card, PayPal, GooglePay, Paytm, etc.

E-cash has four major components-

- Issuers - banks or a non-bank institution.
- Customers - users spending the e-cash.
- Merchants or Traders - vendors who receiving e-cash.
- Regulators - associated authorities or state tax agencies.

In e-cash, we stored financial information on the personal computer/laptops, e-devices or on the net which is liable to hackers. A number of the most important threats associated with e-cash system are -

Backdoors Attacks
It is a kind of attacks which provides an attacker to unauthorized access to a system by bypasses the conventional authentication mechanisms. It works within the background and hides itself from the user that creates it difficult to detect and take away.

Denial of Service Attacks
A denial-of-service attack (DoS attack) could be a security attack during which the attacker takes action that forestalls the legitimate (correct) users from accessing the electronic devices. It makes a network resource unavailable to its intended users by temporarily disrupting services of a device connected to the web.

Direct Access Attacks
Direct access attack is an attack during which an intruder gains physical access to the connected devices or personal computer to perform an unauthorized activity and installing various sorts of software to compromise security. These software are pre-loaded with worms and download a large amount of sensitive data from the target victims.

Eavesdropping
This is an unauthorized way of taking note of private communication over the network. It doesn't interfere with the conventional operations of the targeting system in order that the sender and therefore the recipient of the messages don't seem to be aware that their conversation is being tracked.

3.5 Credit / Debit Card Fraud

A credit master card allows us to borrow money from a recipient bank to carry out purchases. The issuer of the master card has the condition that the cardholder pays back the borrowed money with an extra agreed-upon charge.

A deduction or debit card is a plastic card which is issued by the financial organisation to account holder who operates a savings account which will be used rather than cash to carry out purchases. The deduction card is used only if the amount to spent in the market is within the fund in the account.

Some of the important threats related to the debit/credit card transactions are discussed below.

3.6 Automated Teller Machine

It is the favourite place of the fraudster from there they can steal our card details. Some of the important techniques which the criminals opt for getting hold of our card information is:

Skimming
It is the method of attaching a data-skimming device within the card reader of the ATM. When the customer swipes their card within the ATM card reader, the data is copied from the magnetic strip to the device. By doing this, the criminals get to understand the main particulars of the cards such as number, name, CVV number, expiry date of the cards and other pertinent details.

Unwanted Presence-
As a rule, multiple users should not use the automated teller machine at a time. When we discover that more than one person is lurking around together, the objective behind this is to watch our card details while we were carrying out our transaction.

Vishing/Phishing
Phishing is one activity where an intruder obtained the sensitive data of a user such as password, usernames, and credit card details, often for mischievous reasons, etc.

Vishing is a type of activity in which a prowler obtained the user's sensitive information via sending short message service on mobile phones. These short messages and phone call appears to be from a trustworthy source, but in reality they are fake. The main objective of vishing and phishing is to get the customer's personal identification numbers, account details, and passwords.

Online Transaction
Online transaction service is available to customers for shopping and payment of their bills over the net. Just as the access is easy for the customer, so also it's easy for hacking into our system and stealing our sensitive information by the customer. Some main ways to steal our personal information during an online transaction are-

- downloading software which scans our keystroke and snips our password and card details.
- redirecting a customer to a bogus website which looks like original and steals our sensitive data.
- using public Wi-Fi

Point of Sales Theft
This is usually done at commercial stores at the time of POS transaction. In this case, the salesclerk takes the customer card for handling payment and illegally copies the card details for later use.

In-Text Question(s)

1. Explain the Electronic Payments System and how it functions?

Answer:
Simply put, electronic payment systems allow customers to pay for goods and services electronically without the use of checks or cash. Normally e-payment is done via debit cards, credit cards or direct bank deposits

2. Differentiate between electronic payments system and e-cash

Answer:
Electronic payment is any payment that can be used for payment or making cashless transactions. In e-cash, we stored financial information on the personal computer/laptops, e-devices or on the net which is liable to hackers.

SELF-ASSESSMENT EXERCISE(S)

i. Discuss the cyber security threats in e-commerce.

Answer:
The most common security threats to e-commerce sites are phishing attacks, money thefts, data misuse, hacking, credit card frauds, and unprotected services. These attacks mostly compromised payment data, user login credentials and personal information of the users. The threat landscape for e-Commerce cybersecurity is evolving rapidly. One of the main reasons for e-commerce threats is poor administration by site owners.

Due to the COVID-19 pandemic, greater reliance on online shopping has also increased the likelihood of attacks on eCommerce sites

4.0 CONCLUSION

Electronic payment instrument that can be used to pay a merchant is "e-money", but an electronic payment instrument that can be used to pay another person is "e-cash". In this unit, we examined the possible cyber security threats to e-Commerce in the light of cashless transactions especially over the internet. The unit describes how the e-commerce industry evolved and it familiarises you with the Electronic Payments System and highlights the associated frauds.

5.0 SUMMARY

In this unit we have learnt about:

- the Cyber Security Threats to E-Commerce
- the developments in Electronic Payments System
- the Risk of Fraud and Tax Evasion
- the associated financial risks of Payment Conflict
- the problems of E-Cash and Credit / Debit Card Fraud using Automated Teller Machine

7.0 REFERENCES/FURTHER READING

Clark, Ceri. (2015) A simpler guide to online security for everyone: how to protect yourself and stay safe from fraud, scams and hackers with easy cyber security tips for your Gmail, Docs and other Google services. Simpler Guides Ceri Clark; Lycan Books.

Mamoun Alazab, MingJian Tang. (2019) Deep Learning Applications for Cyber Security Advanced Sciences and Technologies for Security Applications, Springer International Publishing.

Nicholas Kolokotronis & Stavros Shiaeles. (2021) Cyber-Security Threats, Actors, and Dynamic Mitigation, CRC Press.

Robert E. Davis. (2021) Auditing Information and Cyber Security Governance: A Controls-Based Approach Internal Audit and IT Audit 0367568500, 9780367568504 CRC Press.

Robert M. Clark, Simon Hakim (eds.). (2017) Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level, Protecting Critical Infrastructure 3 Springer International Publishing.

MODULE 3 CYBER SECURITY MANAGEMENT

Unit 1 Data Security Concerns
Unit 2 security Technologies
Unit 3 Cyber Security Tools
Unit 4 Cyber Security Operations

MODULE INTRODUCTION

This module consists of four units and introduces the learners to Data Security concerns and considerations, Security technologies, some of the available Cyber Security Tools and Cyber Security Operations.

UNIT 1 DATA SECURITY CONCERNS

CONTENTS

1.0 INTRODUCTION

This unit covers the data security concerns required by system managers to reduce unauthorized access to the systems using or building physical arrangements and software checks. Data security uses various methods to make sure that the data is correct, original, confidential and safe. These methods include backups, archival storage and disposal of data and are discussed in this unit.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the data security considerations
- Describing the backup process
- Explaining the archival storage
- Understanding the disposal of data

3.0 MAIN CONTENT

Data Security Concerns

Data security is that protection of programs and data in computers and communication systems against unauthorized access, modification, destruction, disclosure, or transfer whether accidental or intentional by building physical arrangements and software checks. It refers to the proper of people or organizations to deny or restrict the gathering and use of data about unauthorized access. Data security requires system managers to cut back unauthorized access to the systems by building physical arrangements and software checks.

Data security uses various methods to form sure that the info is correct, original, kept confidentially and is safe. The methods are to confirm the integrity, privacy and stop the loss or destruction of knowledge. Data security methods include encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms.

Data security consideration involves the protection of information against unauthorized access, modification, destruction, loss, disclosure, or transfer whether accidental or intentional. A number of the important data security considerations are described within the following sections.

3.1 Backups

Data backup refers to saving lots of additional copies of our data in separate physical or cloud locations from data files in storage. It's

essential for us to stay secure, store, and backup our data on a daily basis to guide against:

- Unintentional or mischievous damage/modification to data.
- Theft of valuable information.
- Breach of privacy agreements and privacy laws.
- Premature release of knowledge which might avoid intellectual properties claims.
- Release before data are checked for authenticity and accuracy.
- Keeping reliable and regular backups of our data protects against the chance of harm or loss because of breakdown, hardware failure, software or media faults, viruses or hacking, or maybe human errors.

The Backup 3-2-1 Rule is extremely popular and includes:

- Three copies of our data
- Two different formats, i.e., drive + tape backup or DVD (short term) + flash drive
- One off-site backup, i.e., have two physical backups and one within the cloud

Some important backup options are:

a. Hard drives - personal or work computer
b. Departmental or institution server
c. External hard drives
d. Tape backups
e. Discipline-specific repositories
f. University Archives
g. Cloud storage

Some of the highest considerations for implementing secure backup and recovery are-

a. Authentication of the users and backup clients to the backup server.
b. Role-based access control lists for all backup and recovery operations.
c. Encoding options for both transmission and also the storage.
d. Flexibility in choosing encryption and authentication algorithms.
e. Backup of a foreign client to the centralized location behind firewalls.
f. Backup and recovery of a client running Security-Enhanced Linux (SELinux).
g. Using best practices to put in writing secure software.

3.2 Archival Storage

Data archiving is that process of retaining or keeping of information at a secure place for long-term storage. The info could be stored in safe locations so it is often used whenever it's required. The archive data continues to be essential to the organization and should be needed for future reference. Also, data archives are indexed and have search capabilities so the files and parts of files may be easily located and retrieved. the information archival function some way of reducing primary storage consumption of knowledge and its related costs.
Data archival is different from data backup within the sense that data backups created copies of knowledge and used as a knowledge recovery mechanism to revive data within the event when it's corrupted or destroyed. Alternatively, data archives protect the older information that's not needed in day-to-day operations but may need to be accessed occasionally.

Data archives may have many various forms and are often stored as Online, offline, or cloud storage-

- Online data storage places archive data onto disk systems where it's readily accessible.
- Offline data storage places archive data onto the tape or other removable media using data archiving software. Because tape will be removed and consumes less power than disk systems.
- Cloud storage is additionally another possible archive target. as an example, Amazon Glacier is meant for data archiving.

The following list of considerations will help us to boost the long-term usefulness of our archives:

3.2.1 Storage Medium

The first thing is to determine what data-storage medium we intend to use for archives. The archived data are going to be stored for long periods of your time, so we must choose the kind of media that may last as long as our retention policy dictates.

3.2.2 Storage Device

The storage device consideration brings into account the consideration about the memory device we are using for our archives which can be accessible in an exceedingly few years. There's no means to predict which forms of storage devices will stand the most effective. So, it's essential to choose those devices that have the most effective chance of being supported over the future.

3.2.3 Revisiting Old Archives

Because we all know our archiving policies and storage techniques, we are able to predict how they're going to change over time. As a result, a minimum of once a year, we must check our archived data to determine if anything has to be transferred to a unique storage media.

For example, some years back, we utilised Zip drives for archival then we had transferred all of the archives to CD. But nowadays, we keep many of our archives on DVD. Since modern DVD drives may also read CDs, so we have not needed to copy our extremely old archives off CD onto DVD.

3.2.4 Data Usability

In this consideration, we've seen one major problem within the world is archived data which is in an obsolete format.

For example, some years ago, document files that had been archived within the early 1990s were created by an application referred to as PFS Write. The PFS Write file format was supported within the late 80s and early 90s, but today, there don't seem to be any applications which will read that files. To avoid this example, it'd be helpful to archive not only the information but also copies the installation media for the applications that created the information.

3.2.5 Selective Archiving

In this consideration, we've to be sure of what should be archived. which means we are going to archive only a selective a part of data because not all data is equally important.

3.2.6 Space Considerations

If our collections become huge, we must devise plans for the long-term retention of all our data. If we are archiving our data to removable media, capacity planning may be simply making sure that there's free space within the vault to carry all of these tapes, and it makes sure that there's a provision in our IT budget to continue purchasing tapes.

3.2.7 Online vs. Offline Storage

In this consideration, we've to make a decision whether to store our archives online (on a customised archive server) or offline (on removable media). Both methods of archival contain advantages and

downsides. Storing of information online keeps the info easily accessible. But keeping data online could also be susceptible to theft, tampering, corruption, etc. Offline storage enables us to store a vast amount of information, but it's not readily accessible to users.

3.3 Disposal of Data

Data destruction or disposal of knowledge is that method of destroying data which is stored on tapes, hard disks and other electronic media in order that it's completely unreadable, unusable and inaccessible for unauthorized purposes. It also ensures that the organization retains records of knowledge for as long as they're needed. When it's now not required, appropriately destroys them or disposes of that data in another way, as an example, by transfer to an archives service.

The managed process of information disposal has some essential benefits-

- It avoids the unnecessary storage costs incurred by using office or server space in maintaining records which is not any longer needed by the organisation.
- Finding and retrieving information is simpler and quicker because there's less to go looking.

The disposal of information usually takes place as a part of the traditional records management process. There are two essential circumstances within which the destruction of information has to be handled as an addition to the present process-

- The quantity of a legacy record requires attention.
- The functions are being transferred to a different authority and disposal of information records becomes a part of the change process.

The following list of considerations will enable secure disposal of information (it must be ensured that the user account having the eliminating access doesn't have any rights to re-access the disposed data again). This is needed so that the disposed data is not retrieved by the user who disposed of the data.

3.3.1 Destroy the Data

In this consideration, there's not enough reasons that just to get rid of data from storage media are going to be safe. Even nowadays reformatting or repartitioning a drive to "erase" the information that it stores isn't adequate. Today's many tools available which might help us to delete files more securely. To encrypt the info on the drive before

performing any deletion can help us to form data that are harder to recover later.

3.3.2 Destroy the Device

In most cases, storage media have to be physically destroyed to make sure that our sensitive data isn't leaked to whoever gets the drives next. In such cases, we should always not destroy them itself. To do this, there should be experts who can make probably lots better at safely and effectively rendering any data on our drives unrecoverable. If we won't trust this to an outsider agency that makes a speciality of the secure destruction of storage devices, we must always have a specialized team within our organization who has the identical equipment and skills as outside contractors.

3.3.3 Keep Record of Decommissioned Systems

In this case, we've to be sure that the storage media has been fully decommissioned securely and that they don't incorporates something easily misplaced or overlooked. it's best if storage media that haven't been fully decommissioned are kept during a specific location, while decommissioned equipment placed someplace else in order that it'll help us to avoid making mistakes.

3.3.4 Keep Careful Records

In this consideration, it's necessary to preserve the record of whoever is liable for decommissioning a storage media. If over one person is assigned for such responsibility, he should give a documented notice after the completion of the decommissioning process. So that, if something happened wrong, we all know who to speak to seek out what happened and the way bad the error is.

3.3.5 Eliminate Potential Clues

In this consideration, we've got to clear the configuration settings from networking equipment. We need to carry out this because it can provide crucial clues to a security cracker to interrupt into our network and therefore the systems that reside on that.

3.3.6 Keep System Secure Until Data Disposal

In this consideration, we must always need to clarify guidelines for who should have access to the equipment in need of secure disposal. it'll be better to confirm that no-one should have access authentication to that before disposal of information won't get his or her hands thereon.

In-Text Question(s)

1. What is a backup and what functions does it perform?

Answer:
The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure. Backup refers to the copying of physical or virtual files or databases to a secondary location for preservation in case of equipment failure or catastrophe. The process of backing up data is pivotal to a successful disaster recovery plan.

2. Explain the term archival storage

Answer:
Archival storage is storage for data that possibly will not be actively needed but is kept for later use or for record-keeping purposes. Archival storage is often provided using the same system as that used for backup storage.

SELF-ASSESSMENT EXERCISE(S)

i. Discuss the data security considerations.

Answer:
Data security consideration involves the protection or security of data and system resources from unauthorized access, disclosure, or corruption. Information breaches could be intentional or unintentional but ultimately cause huge losses to the organisation hence need to be dealt with seriously.

4.0 CONCLUSION

From cybersecurity's point of view, the consideration of data is important because all categories of data need to be protected from theft and damage. This includes sensitive data, protected health information, personal information, intellectual property, data, and governmental and organisational information systems. In this unit, we looked at a number of approaches to cyber security from the point of data security considerations. The unit describes the concepts of backups and archival storage. It also explains the various methods for the disposal of information.

5.0 SUMMARY

In this unit we have learnt about:
• the data security considerations

• the developments in backups
• the archival storage
• the disposal of data

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. (2019) CyBok: The Cyber Security Body of Knowledge, National Cyber Security Centre

Brij Gupta, Gregorio Martinez Perez, Dharma P. Agrawal, Deepak Gupta. (2020) Handbook of Computer Networks and Cyber Security: Principles and Paradigms Springer.

Ethem Mining Kali. (2019) Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing. Includes Valuable Basic Networking Concepts. Independently published.

Karnel Erickson, (2019) Cyber Security (Kali Linux for Hackers & Hacker Basic Security),

Nathan House. (2017) The Complete Cyber Security Course, Volume 1: Hackers Exposed, StationX.

Zach Codings. (2019) Computer Programming and Cyber Security for Beginners: This Book Includes: Python Machine Learning, SQL, Linux, Hacking with Kali Linux, Ethical Hacking. Coding and Cybersecurity Fundamentals.

UNIT 2 SECURITY TECHNOLOGIES

CONTENTS

1.0 INTRODUCTION

Security technology are policies, concepts and components intended to minimise risk, identify vulnerabilities, and inform how and when to respond to impending incidents.

Technology is critical to enhancing security. Without components such as cameras, detectors and alarms, businesses would be unable to identify threats and respond appropriately. Information technology plays a significant role and will continue to strengthen the national security against future upcoming threats and cyber-attacks. This unit present a number of the Security Technologies that are applicable in cyber security, e.g. Firewall, Virtual Private Network (VPN), Intrusion Detection System and Access Control.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the Security Technologies
- Describe the Firewall
- Explain the Processing Mode
- Identify and describe the Development Era of Firewall
- Understand the Intended Development Structure
- Explain the Architectural Implementation
- Describe the Virtual Private Network (VPN)
- Understand the Intrusion Detection System
- Explain the Access Control

3.0 MAIN CONTENT

Security Technologies

With the rapid development within the Internet, cybersecurity has become a significant fear to organisations throughout the planet. the actual fact that information, tools and technologies needed to breach the protection of corporate organisation networks are widely available has increased the safety concern.

Nowadays, the basic problem is that considerable a part of the protection technologies aims to hold the attacker out, and when that fails, the defences have failed. Every organization who uses internet needed security technologies to hide the three primary control types - preventive, detective, and corrective further as provide auditing and reporting. Most security relies on one in all these kinds of things: thing we possess (e.g. a key or an ID card), thing we all know (e.g. a PIN or a password), or thing we are (e.g. a fingerprint).

Some of the most prominent security technologies applied in the cybersecurity are described below:

3.1 Firewall

Firewall could be an electronic network security system designed to forestall unauthorized access to or from a non-public network. It is implemented as hardware, software, or a mix of both. Firewalls are accustomed to prevent unauthorized Internet users from accessing private networks connected to the net. All messages are entering or leaving the intranet submit to the firewall. The firewall examines each message and blocks those who don't meet the required security criteria.
Firewall can however be categorised into: Processing Mode, Development Era of Firewall, Intended Development Structure and Architectural Implementation.

3.2 Processing Mode

The five processing modes of firewalls are:

1. Packet Filtering
   Packet filtering firewalls scan header information of a knowledge packets going in a network. This firewall is installed on Transmission Control Protocol/Internet Protocol network and determine whether to transmit it to the following network connection or drop the packet supported the instructions programmed within the firewall. It scans network data packets

searching for a violation of the foundations of the firewalls database. Most firewall often supported a mix of:

- IP source and destination address.
- Direction (outbound or inbound).
- TCP or User Datagram Protocol (UDP) source and destination port requests.

Packet filtering firewalls will be characterised into three types-

- Static filtering: The supervisor established a filtering rule or guideline for the firewall. These rules governing how the firewall selects which packets are allowed and which are denied are established and installed.
- Dynamic filtering: It allows the firewall to line some rules for itself, like dropping packets from an address that's sending many bad packets.
- Stateful inspection: A stateful firewalls maintain the track of every network connection between inside and out of doors systems employing a state table.

2. Application Gateways

It is a firewall proxy which is often installed on a specially dedicated machine to provide network security. This proxy firewall acts as an intermediary between the requester and therefore the protected device by filtering incoming node traffic to certain specifications. Examples of these network applications include Telnet, FTP, Real Time Streaming Protocol.

3. Circuit Gateways

A circuit-level gateway operates at the transport layer and provides UDP and TCP connection security meaning that it can reassemble, examine or block all the packets in a User Datagram Protocol connection or TCP. This works between an application layer and a transport layers like the session layer. Unlike application gateways, it screens TCP data packet handshaking and session fulfilment of firewall rules and policies. It should also act as VPN over the web by doing encryption from firewall to firewall.

4. MAC Layer Firewalls

The Media Access Control (MAC) layer firewall is meant to function at the media access control layer of the OSI network model. It’s able to assess a selected host computer's identity within the filtering decisions. MAC addresses of particular host machines are linked to the access control list entries. This entry identifies unique forms of packets that may be forwarded to every host and every one other traffic is blocked. it'll also cross-check the address of a requester to determine whether the pc or device being employed are capable to create the connection is permitted to access the data or not.

5. Hybrid Firewalls

It is a kind of firewalls which combine features of other four styles of . These are elements of packet filtering and proxy services, or of packet filtering logic gate gateways.

3.3 Development Era of Firewall

Firewall is classified according to the generation types as follows:

1. First Generation:
   The first-generation types of firewall come with static packet filtering. A static packet filter is a simple and least expensive varieties of firewall protection. Within this generation, each packet entering and leaving the network is checked and can be either passed or rejected depends on the user-defined rules. we will compare this security with the bouncer of the club who only allows people over 21 to enter and below 21 are going to be disallowed.
2. Second Generation:
   The second generation types of firewall are released with Application level or proxy servers. This generation of firewall increases the protection level between trusted and untrusted networks. An application level firewall uses software to intercept connections for every IP and to perform security inspection. It involves proxy services which act as an interface between the user on the interior trusted network and therefore the Internet. Each computer communicates with one another by passing network traffic through the proxy program. This program evaluates data sent from the client and decides which to transmit on and which to drop.
3. Third Generation:
   The third generation types of firewall are embedded with the stateful inspection firewalls. This generation of the firewall has evolved to satisfy the key requirements demanded by corporate networks of increased security while minimizing the impact on network performance. The requirements of the third-generation firewalls are even more demanding because of the growing support for VPNs, wireless communication, and enhanced virus protection. The foremost challenging element of this evolution is maintaining the firewall's simplicity (and hence its maintainability and security) without compromising flexibility.
4. Fourth Generation:
   The fourth generation types of firewall are released with dynamic packet filtering system. This firewall monitors the state of active connections, and on the premise of this information, it determines which network packets are allowed to have the firewall. By recording session information like IP addresses and port numbers,

a dynamic packet filter can implement a far tighter security posture than a static packet filter.

5. Fifth Generation:
   The fifth-generation types of firewall comes with kernel proxy and operates at the OSI application layer. In this, when a packet arrives, a brand new virtual stack table is formed which contains only the protocol proxies needed to look at the particular packet. These packets are investigated at each layer of the stack, which involves evaluating the information link header together with the network header, transport header, session layer information, and application layer data. This firewall works faster than all the application-level firewalls because all evaluation takes place at the kernel layer and not at the upper layers of the OS.

3.4 Intended Deployment Structure

Firewall may also be classified according to the following structures:

1. **Commercial Appliances**
   The firewall here runs on customised operating system and consists of firewall application software that runs on a general-purpose computer. It's designed to supply protection for a medium-to-large business network. Most of the commercial firewalls are quite complex and infrequently require specialized training and certification to have full advantage of their features.
2. **Small Office Home Office**
   The SOHO firewall is meant for little office or business office networks who need protection from Internet security threats. A firewall for a SOHO (Small Office Home Office) is that first line of defence and plays a vital role in an overall security strategy. SOHO firewall has limited resources in order that the firewall product they implement must be relatively easy to use and maintain and be cost-effective. This firewall connects a user's local area network or a particular ADP system to the Internetworking device.
3. **Residential Software**
   In the case of Residential-grade firewall, the required software is installed directly on a user's system. A number of these applications combine firewall services with other protections like antivirus or intrusion detection but there's a limit to the extent of configurability and protection that software firewalls can provide.

3.5 Architectural Implementation

The firewall configuration that works best for a specific organization depends on three factors: the objectives of the network, the

organization's ability to develop and implement the architectures, and therefore the budget available for the function.

There are four common architectural implementations of firewalls:

1. Packet-filtering routers
   Packet filtering firewall is employed to manage the network access by monitoring the outgoing and incoming packets. It allows them to pass, or halt supported the source and destination IP addresses, protocols and ports. During exchange of data, a node transmits a packet which is filtered and checked with the predefined rules and policies. Once it's matched, a packet is taken into account secure and verified and are ready to be accepted otherwise blocked them.
2. Screened host firewalls
   The screened host firewalls architecture combines packet-filtering router with separate and dedicated firewall. The needed gateway functionality here is allowing the router to pre-screen packets to reduce the network traffic and channel capacity on the interior proxy. The packet-filtering router filters dangerous protocols from reaching the utilisation gateway and site systems.
3. Dual-homed host firewalls
   The specification for the dual-homed host firewall is easy. Its architecture is made round the dual-homed host computer, a computer that has a minimum of two NICs. One NIC is to be connected with the external network, and other is connected to the inner network which provides a further layer of protection. With these NICs, all traffic must undergo the firewall so as to pass between the inner and external networks.
   In Implementing his architecture network address translation (NAT) is often made use of. NAT is a technique for mapping assigned IP addresses to special ranges of no routable internal IP addresses, thereby creating another barrier to intrusion from external attackers.
4. Screened Subnet Firewalls
   This architecture adds an additional layer (perimeter network) of security to the screened host architecture by adding a fringe network that further isolates the inner network from the net. Within this architecture, there are two screening routers and both connected to the perimeter net. One router sits between the perimeter net and therefore the internal network, and also the other router sits between the perimeter net and therefore the external network. To intrude into the interior network, an attacker must get past both routers and there's no single vulnerable point which will compromise the inner network.

3.6 Virtual Private Network (VPN)

A VPN stands for virtual private network and it's a technology which creates a secure and an encrypted connection on the net from a host to a network. This kind of connection helps to make sure our sensitive data is transmitted safely. It prevents our connection from eavesdropping on the network traffic and allows the user to access a personal network securely. This technology is widely utilized in the company environments.

A VPN works same as firewall like firewall protects data local to a host whereas VPNs protects data online. to make sure safe communication on the web, data travel through secure tunnels, and VPNs user used an authentication method to realize access over the VPNs server. VPNs are utilized by remote users who must access corporate resources, consumers who want to download files and business travellers want to access a site that's geographically restricted.

3.7 Intrusion Detection System

An intrusion detection system (IDS) may be a security system which monitors the host systems and network traffic. IDS analyses the traffic for possible aggressive attacks coining from the outsider and also for system misuse or attacks emanating from the insiders. A firewall performs the filtering of the incoming traffic from the net, the IDS in a very similar way compliments the firewall security. Like, the firewall protects a corporation sensitive data from malicious attacks over the net, the Intrusion detection system alerts the supervisor in cases when someone tries to intrude within the firewall security and tries to possess access on any network within the trusted side.

Intrusion Detection System have differing kinds of approaches to detect the suspicious activities-

1. Network Intrusion Detection System (NIDS)
   It is a NIDS that monitors the inbound and outbound traffic to and from all the devices over the network.
2. Host Intrusion Detection System (HIDS)
   It is a HIDS that runs on all devices within the network with direct access to both internet and enterprise internal network. It can detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS didn't catch. HIDS may additionally identify malicious traffic that arises from the host itself.

3. Signature-based Intrusion Detection System
   It is a detection system which refers to the detection of an attack by trying to find the particular patterns, like byte sequences in network traffic, or known malicious instruction sequences employed by malware. This IDS originates from anti-virus software which might easily detect known attacks. Within this terminology, it's impossible to detect new attacks, that do not match existing pattern.
4. Anomaly-based Intrusion Detection System
   This detection system was primarily introduced to detect unknown attacks because of the rapid development of malware. It alerts administrators against the doubtless malicious activity. It monitors the network traffic and compares it against a longtime baseline. It determines what's considered to be normal for the network in relations to bandwidth, protocols, ports and other devices.

3.8 Access Control

Access control could be a process of choosing restrictive access to a system. it's an idea in security to reduce the danger of unauthorized access to the business or organization. Using access control, users are allowed access permission and defined privileges to a system and resources in form of credentials which the users must provide to be granted access to a system. These credentials are available in many forms like password, keycard, the biometric reading, etc. Access control ensures security technology and access control policies to safeguard private data like customer data.

The access control may be categorised into two types- Physical and Logical Control.

Physical Access Control restricts access to physical IT assets, rooms, buildings, and campuses. Whereas, Logical access control limits connection to computer networks, system files, and data.

The safer method for access control involves two - factor authentication. the primary factor is that a user who desires access to a system must show credential and also the second factor may well be an access code, password, and a biometric reading.

The access control comprises of two main components: authentication and authorization. Authentication may be a process which verifies that somebody claims to be granted access whereas an authorization provides that whether a user should be allowed to have access to a system or denied it.

In-Text Question(s)

1. What is a network intrusion detection system?

Answer:
A network intrusion detection system (IDS) is a security system which monitors the host device and network traffic. IDS analyses the traffic for possible aggressive attacks coining from the outsider and also for system misuse or attacks emanating from the insiders.

2. Differentiate between authorisation and authentication

Answer:
An authorization provides that whether a user should be allowed to have access to a system or denied it whereas Authentication is a method which verifies that somebody claims to be granted access.

SELF-ASSESSMENT EXERCISE(S)

i. Discuss the various cyber security detection and prevention mechanisms.

Answer:
Threat detection is the act of analysing the totality of a security ecosystem to identify any malicious activity that could compromise the network. The prevention mechanisms consist of policy, awareness, vulnerability mitigation, and threat mitigation, which can be described as a perfect defence option for computer networks and systems. If threats are detected, then mitigation efforts must be endorsed to properly neutralize the threat before it can abuse any present vulnerabilities.

4.0 CONCLUSION

One of the goals of IT and cyber security is to protect information assets, devices and services from being disrupted, stolen or exploited by unauthorized users, usually known as threat actors. These threats can be external or internal and malicious or accidental in both origin and nature.

Security technologies involves the use of physical barriers and applied sciences to provide or enhance the security of people, property and information. The benefit of data security technology is that it prevents people from tampering with and modifying software. Additional application security measures, such as rigorous testing and real-time logging, are important to ensure cyber, cloud, web and mobile-based applications are protected against the latest vulnerabilities. This unit has

provided some insights to the available security technologies and how to apply them.

5.0 SUMMARY

In this unit we have learnt about:

- the available Security Technologies
- the developments in Firewall
- the problems in Processing Mode
- the Development Era of Firewall
- the Intended Development Structure
- the Architectural Implementation
- Virtual Private Network
- Intrusion Detection System and Access Control

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Gautam Kumar (editor), Dinesh Kumar Saini (editor), Nguyen Ha Huy Cuong (editor) (2021) Cyber Defense Mechanisms: Security, Privacy, and Challenges (Artificial Intelligence (AI): Elementary to Advanced Practices) Artificial Intelligence (AI): Elementary to Advanced Practices, CRC Press,

Marshall Copeland (auth.). (2017) Cyber Security on Azure: An IT Professional's Guide to Microsoft Azure Security Center, Apress,

Marshall Copeland, Matthew Jacobs. (2021) Cyber Security on Azure: An IT Professional's Guide to Microsoft Azure Security, Apress,

Padmavathi Ganapathi (editor), D. Shanmugapriya (editor). (2020) Handbook of Research on Machine and Deep Learning Applications for Cyber Security (Advances in Information Security, Privacy, and Ethics), Information Science Reference.

UNIT 3 CYBER SECURITY TOOLS

CONTENTS

1.0 INTRODUCTION

This unit covers the various cyber security tools available. These tools include Firewalls, Antivirus Software, PKI Services, Managed Detection and Response Service, Penetration Testing and Staff Training. The unit will familiarize you with much of the vocabulary you hear with regards to security tools and also explain some of these concepts in more details.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the cyber security tools
- Describing the Firewalls
- Explaining the Antivirus Software
- Understanding how PKI Services work
- Describing Managed Detection and Response Service
- Explaining Penetration Testing and Staff Training

3.0 MAIN CONTENTS

Cyber Security Tools

Protecting IT environment is incredibly critical. Every organization must take cybersecurity very seriously. There are substantial numbers of hacking outbreaks affecting businesses of different dimensions and sizes. Hackers, malware, viruses are a number of the important security threats within the virtual world. It's essential that each company is responsive to the damaging security attacks, and it's necessary to preserve themselves secured. There are many various aspects of the

cyber defence that might have to be considered. Here are six essential tools and services that each organization must consider in ensuring their cybersecurity is as strong as possible. They're described within the following sections.

3.1 Firewalls

As we know, the firewall is that core of security tools which has becomes the foremost important security tools. Its job is to stop unauthorized access to or from a non-public network. It is often implemented as hardware, software, or a mixture of both. The firewalls are adapted to prevent unauthorized internet users from accessing private networks connected to the web. All messages that are entering or leaving the intranet are routed through the firewall. The firewall examines each message and blocks those messages that don't meet the required security criteria.

The Firewall is extremely useful, but with some limitations also. A talented hacker knew a way to create data and programs that are believing like trusted firewalls. It implies that we will pass the program through the firewall with no problems. Despite these limitations, firewalls are still very useful within the protection of less sophisticated malicious attacks on our system.

3.2 Antivirus Software

Antivirus software could be a program which is meant to stop, detect, and take away viruses and other malware attacks on the individual computer, networks, and IT systems. It also protects computer systems and networks from the variability of threats and viruses like Trojan horses, worms, keyloggers, browser hijackers, rootkits, spyware, botnets, adware, and ransomware. Most antivirus program comes with an auto-update feature and enabling the system to test for brand spanking new viruses and threats regularly. It provides some additional services like scanning emails to make sure that they're free from malicious attachments and web links.

3.3 Public Key Infrastructure (PKI) Services

- Public Key Infrastructure is a tool that maintain the circulation and identification of public encryption keys. It enables users and computer systems to securely exchange data over the net and verify the identity of the opposite party. We are able to also exchange sensitive information without PKI, but in this case, there would be no assurance of the authentication of the opposite party.

- People associate PKI with Secure Sockets Layer (SSL) or Transport Layer Security (TLS). SSL is the technology which encrypts the server communication and is responsible for HTTPS and padlock that we will see in our browser address bar. PKI solve many numbers of cybersecurity problems and deserves an area within the organization security suite.
- PKI may also be used to:
- Enable Multi-Factor Authentication and access control
- Create compliant, Trusted Digital Signatures.
- Encrypt email communications and authenticate the sender's identity.
- Digitally sign and protect the code.
- Build identity and trust into IoT ecosystems.

3.4 Managed Detection and Response Service

- Today's cybercriminals and hackers used more advanced techniques and software to breach organization security So, there's a necessity for each business to use more powerful types of defences of cybersecurity. MDR is a complicated cutting-edge security service that has capacity for threat hunting, threat intelligence, security monitoring, incident analysis, and incident response. It's a service that arises from the necessity for organizations lacking needed resources to be more responsive to risks and improve their ability to detect and answer threats. MDR also uses AI and machine learning to analyse, auto detect threats, and orchestrate response for faster result.
- The managed detection and response has the subsequent characteristics:
- Managed detection and response is concentrated on threat detection, instead of compliance.
- MDR relies heavily on security event management and advanced analytics.
- While some automation is employed, MDR also involves humans to watch our network.
- MDR service providers also perform incident validation and remote response.

3.5 Penetration Testing

Penetration testing, or pen-test, is a crucial and essential method to evaluate our business's security systems and security of an IT infrastructure by safely trying to take advantage of vulnerabilities. These vulnerabilities exist in operating systems, services and application, improper configurations or risky end-user behaviour. In Penetration testing, cybersecurity professionals will use the identical techniques and

processes utilized by criminal hackers to test for potential threats and areas of weakness.

A pen test attempts the type of attack a business might face from criminal hackers like password cracking, code injection, and phishing. The pen test involves a computer-generated real-world attack on an application or networked devices. This tests are often performed by using manual or automated technologies to systematically evaluate servers, web applications, network devices, endpoints, wireless networks, mobile devices and other potential points of vulnerabilities. Once the pen test has successfully taken place, the testers will present their findings on threats and may help by recommending potential changes to the system.

Vulnerability assessment is the process of identifying threats and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the IT ecosystem. A vulnerability assessment therefore is a systematic evaluation of security weaknesses in an information system. The assessment evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

3.6 Staff Training

Staff training isn't a 'cybersecurity tool' but ultimately, having knowledgeable employees who understand the cybersecurity which is one amongst the strongest types of defence against cyber-attacks. Today's many training tools available which will educate company's staff about the most effective cybersecurity practices. Every business can organize these training tools to coach their employee who can understand their role in cybersecurity.

It is known that cyber-criminals still expand their techniques and level of sophistication to breach businesses security, it's made it essential for organizations to speculate in these training tools and services. Failing to try and do this, they will leave the organization during a position where hackers would be easily targeted their security system. So, the expense of the investment on these training tools might put a souvenir for the business concern with long-term security and protection.

In-Text Question(s)

1. What's penetration testing and the way is it performed?

Answer:
Penetration testing, or pen-test, is a crucial and essential method to evaluate our business's security systems and security of an IT infrastructure by safely trying to take advantage of vulnerabilities.
In Penetration testing, cybersecurity professionals will use the identical techniques and processes utilized by criminal hackers to test for potential threats and areas of weakness.

2. Differentiate between vulnerability assessment and penetration testing

Answer:
Vulnerability assessment is the process of identifying threats and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the IT ecosystem. In Penetration testing, cybersecurity professionals will use the identical techniques and processes utilized by criminal hackers to test for potential threats and areas of weakness

SELF-ASSESSMENT EXERCISE(S)

i. Discuss the importance of penetration testing in an enterprise.

Answer:
The key purpose of the penetration test is to improve network security and provide protection for the whole network and connected devices against future attacks. While penetration testing not only helps to identify vulnerabilities within a network, it also offers insight into which channels in the organisation or application are most at risk. This process could help uncover several major system weaknesses previously undiscovered and this will assist in knowing the types of new security tools or protocols that should be invested in.

4.0 CONCLUSION

Security Tools are all the measures and information used to verify the security level of implementing transactions, including but not limited to user name, password, registered telephone number, OTP code, and other types of information as prescribed for each organisation. These tools enable the safe operation of applications implemented on the organisation's IT systems and protect the data technology the organisation collects and uses.

From the unit we can deduce some of the benefits of these tools which includes: Educated Employees, Reduced Risk of Destructive Human Error, meeting Compliance Requirements, keeping customers' Trust and Staying ahead of increasing threats.

5.0 SUMMARY

In this unit we have learnt about:

- the cyber security tools
- the Firewalls developments
- the Antivirus Software
- how PKI Services work
- Describing Managed Detection and Response Service
- Explaining Penetration Testing and Staff Training

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Centre for Cyber Security Belgium, (2015) Cyber Security Incident Management Guide, Centre for Cyber Security Belgium.

Donald A. Tevault. (2020) Mastering Linux Security and Hardening: Protect Your Linux Systems from Intruders, Malware Attacks, And Other Cyber Threats, Packtpub.

Dunkerley Mark, Tumbarello Matt (2020) Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats, Packt Publishing Ltd.

Jack Caravelli, Nigel Jones. (2019) Cyber Security: Threats and Responses for Government and Business, Praeger Security International.

Kuan-Ching Li, Xiaofeng Chen, Willy Susilo. (2019) Advances in Cyber Security: Principles, Techniques, and Applications, Springer Singapore.

Ramjee Prasad, Vandana Rohokale. (2020) Cyber Security: The Lifeline of Information and Communication Technology Springer Series in Wireless Technology, Springer.

Venkata P. Krishna, Sasikumar Gurumoorthy, Mohammad S. Obaidat. (2019) Social Network Forensics, Cyber Security, and Machine Learning, SpringerBriefs in Applied Sciences and Technology, Springer Singapore.

UNIT 4 CYBER SECURITY OPERATIONS

CONTENTS

1.0 INTRODUCTION

This unit covers the Cyber Security Operations. The unit explains how the Security Information Event are effectively managed. It details the staffing requirement for managing security information events with the appropriate escalation chains. Finally, it explores the classification of incidents and highlights the events to monitor in security orchestration and response.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the security information management
- Describing the SOC staffing
- Explaining the escalation chains for security events
- Understanding how to classify security incidents
- Explaining the concept of security orchestration, automation and response

3.0 MAIN CONTENT

Cyber Security Operations

Security Operations is usually contained within a Security Operations Centre (SOC), though the terminologies are used interchangeably. Typically, the SOC's responsibility is to detect threats within the environment and stop them from developing into expensive problems.

3.1 SIEM ("Security Information Event Management")

Security information events are produced as logs from most systems often contain vital security information. An event is just an observation that can be determined from logs and knowledge from the network, for example:

- Users logging in
- Attacks observed within the network
- Transactions within applications

An incident are a few negative things we believe will impact our organisation, that is the occurrence of a definitive threat or the potential of such a threat happening. The SOC should do their best to see which events may be concluded to actual incidents, which should be knowledgeable.

The SIEM processes alerts supported logs from different sensors and monitors within the network, each which could produce alerts that are important for the SOC to reply to. The SIEM also can try and correlate multiple events to see an alerts.
SIEM's typically allow events from the network, host and application areas to be analysed:

- Network
  Events from the network happens to be the commonest, but least valuable as they do not hold the complete context of what is going on. The network usually discloses who is communicating where, when and over which protocols but not the intricate details of what happened, to whom and why.

- Host
  Host events give more information with regard to what actually happened and to whom. Challenges like encryption isn't any longer blurred and more visibility is gained into what's happening. Many SIEM's are enriched with great details about what happens on the hosts themselves, rather than only from the network.

- Applications
  Events from application is where the SOC typically can best understand what's occurring. These events give information about the Triple A, AAA ("Authentication, Authorization and Account"), including detailed information about how the appliance is performing and what the users do.
  For a SIEM to grasp events from applications it typically requires work from the SOC Team to create the SIEM understanding of

these events, as support is commonly not included "out-of-the-box". Many applications are proprietary to a company and therefore the SIEM doesn't have already got an understanding of the information the applications forward.

3.2 SOC Staffing

How a SOC is staffed greatly varies arising from the necessities and structure of a corporation. During this session we take a firm look at typical roles involved in operating a SOC. an outline of potential roles:
SOC Organisation.

As in most organized teams, a task is appointed to steer the department. The SOC Chief decides the policy and strategies involved to counter threats against the organisation.

The SOC Architect is liable for ensuring the systems, platforms and overall architecture is capable of delivering what the team members require to perform their duties. A SOC Architect will help build correlation rules across multiple points of knowledge and ensures incoming data conforms to the platform requirements.

Analyst Lead is responsible that processes, or playbooks, are developed and maintained to confirm analysts are capable to seek out the data necessary to conclude alerts and potential incidents.

Level 1 Analysts function as the primary responders to alerts. Their duty is, within their capabilities, to conclude alerts and forward any troubles to the next level analyst.

Level 2 Analysts are eminent staff presumably having more technical knowledge and experience. They ought to also ensure any troubles in resolving alerts are forwarded to the Analyst for the continued improvement of the SOC. Analyst level 2 along with the Analyst Lead are to escalate incidents to the Incident Response Team.

The Incident Response Team (IRT) may be a natural extension to the SOC Team. The IRT team is deployed to remediate and solve the problems impacting the organization. Penetration Testers ideally also support the defence with the intricate knowledge they have of how attackers operate and may help in root cause analysis and understanding how break-ins occur. Merging attack and defence teams is usually brought up as Purple Teaming and is taken into account a best-practice operation.

3.3 Escalation Chains

Some alerts require immediate actions therefore it's important for the SOC to posses defined a process of whom to contact when different incidents occur. Incidents can occur across many various business units, the SOC should know who to contact, when and on which communication mediums.

Example of an escalation chain for incidents impacting one a part of an organization:

Create an occasion within the appointed Incident Tracking System, assigning it to correct department or person(s)

If no dissent happens from department/person(s): send SMS and Email to primary contact

If still no direct action: telephony primary contact
If still no direct action: call secondary contact

3.4 Classification of Incidents

Incidents should be classified consistent with their:

- Category
- Criticality
- Sensitivity

Depending on the incidents classification and the way it's attributed, the SOC might take different measures to resolve the problem at hand.
The category of incident will determine the way to respond. There exist many varieties of incident and it's important for the SOC to know what each incident type means for the organization. Example incidents are listed below:

- ✓ Inside Hacking
- ✓ Malware on Client workstation
- ✓ Worm spreading across the network
- ✓ Distributed Denial of Service Attack
- ✓ Leaked Credentials

The criticality of an occasion is decided supported what percentage systems is impacted, the potential impact of not stopping the incident, the systems involved and plenty of other things. it's important for the SOC to be ready to accurately determine the criticality that the incident may be closed accordingly. Criticality is what determines how briskly an event should be more established. Should the incident be tried and true immediately or can the team wait until tomorrow?

3.5 Security Orchestration, Automation and Response (SOAR)

To counter the advancements of threat actors, automation is key for a modern SOC to respond fast enough. To facilitate fast response to incidents, the SOC should have tools available to automatically orchestrate solutions to respond to threats in the environment.

The SOAR strategy means ensuring the SOC can use actionable data to help mitigate and stop threats which are developing more real-time than before. In traditional environments it takes attackers very short time from the time of compromise until they have spread to neighbouring systems. Contrary to this it takes organizations typically a very long time to detect threats that have entered their environment. SOAR tries to help solve this.

SOAR includes concepts such as IAC "Infrastructure as Code" to help rebuild and remediate threats. SDN ("Software Defined Networking") to control accesses more fluently and easily, and much more.

3.5.1 What to monitor?

Events can be collected across many different devices, but how do we determine what to collect and monitor? We want the logs to have the highest quality. High fidelity logs that are relevant and identifying to quickly stop the threat actors in our networks. We also want to make it hard for attackers to circumvent the alerts we configure.

If we look at different ways to catch attackers, it becomes evident where we should focus. Here is a list of possible indicators we can use to detect attackers, and how hard it is considered for attackers to change shown in

Table 3.1: Relative level of difficult for attackers making changes

Indicator	Difficulty to change
File checksums and hashes	Very Easy
IP Addresses	Easy
Domain Names	Simple
Network and Host Artifacts	Annoying
Tools	Challenging
Tactics, Techniques and Procedures	Hard

File checksums and hashes can be used to identify known pieces of malware or tools used by attackers. Changing these signatures are considered to be trivial for attackers as their code can be encoded and changed in multiple different ways, making the checksums and hashes change.

IP Addresses are also easy to change. Attackers can use IP addresses from other compromised hosts or simply use IP addresses within the jungle of different cloud and Virtual Private Server (VPS) providers.

Domain Names can also be reconfigured quite easily by attackers. An attacker can configure a compromised system to use a DGA ("Domain Generation Algorithm") to continuously use a new DNS name as time passes. One week the compromised system uses one name, but the next week the name has changed automatically.

Network and Host Artifacts are more annoying to change, as this involves more changes for the attackers. Their utilities will have signatures, like a user-agent or the lack of thereof, that can be picked up by the SOC.

Tools become increasingly harder to change for attackers. Not the hashes of the tools, but how the tools behave and operate when attacking. Tools will be leaving traces in logs, loading libraries and other things which we can monitor to detect these anomalies.

If the defenders are capable of identifying Tactics, Techniques and Procedures threat actors use, it becomes even harder for attackers to get to their objectives. For example, if we know the threat actor likes to use Spear-Phishing and then Pivoting peer-to-peer via to other victim systems, defenders can use this to their advantage. Defenders can focus training to staff at risk for spear-phishing and start implementing barriers to deny peer-to-peer networking.

In-Text Question(s)

1. What are major areas for SIEM analyses?

Answer:
Typically, the major areas for analyses are the network, host and application areas where events are logged.

2. Enumerate four examples of incidents

Answer:
Inside Hacking; Malware on Client workstation; Worm spreading across the network; Distributed Denial of Service Attack and Leaked Credentials

SELF-ASSESSMENT EXERCISE(S)

i. Discuss the best practices in dealing with incident reports

Answer:
Dealing with incident reports can be considered as part of the incident management practices. These are some of the incident Management Practices: Creating Teams with the Right Skills; Clearly Defining the incident Management guidelines; Establishing Communication Channels; Cultivating a security conscious Culture.

4.0 CONCLUSION

In this unit, we have seen the overarching advantage of SIEM which is the ability to perform quick, accurate detection and identification of security events. SIEM can be combined with Security Orchestration Automation and Response (SOAR) for additional benefits. Having Cyber security operation centre is a desirable feature for all organisation and the appropriate level of staffing should be guaranteed.

5.0 SUMMARY

In this unit we have learnt about:
• the Security Information Event Management
• how Security Operation Centre Staffing works
• the types of Escalation Chains
• how to do the Classification of Incidents
• how to monitor Security Orchestration, Automation and Response

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Nicholas J. Daras. (2019) Cyber-Security and Information Warfare, Cybercrime and Cybersecurity Research, Nova Science Publishers

Zheng Xu, Kim-Kwang Raymond Choo, Ali Dehghantanha, Reza Parizi, Mohammad Hammoudeh. (2020) Cyber Security Intelligence and Analytics Advances in Intelligent Systems and Computing 928 Springer International Publishing.

Brook S. E. Schoenfield (2020). Secrets of a Cyber Security Architect, CRC Press.

Edward Griffor (2017). Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems Syngress advanced topics in information security, Syngress.

Tony Thomas, Athira P Vijayaraghavan, Sabu Emmanuel (2020). Machine Learning Approaches in Cyber Security Analytics, Springer.

MODULE 4 CYBER ATTACKS AND ATTACKERS

MODULE INTRODUCTION

This module consists of three units dealing with Types of Cyber Attacks and Attackers. It also examined in details the Man-in-the-Middle Attacks and Cyber Security associated with Wi-Fi Attacks.

UNIT 1 TYPES OF CYBER ATTACKS AND ATTACKERS

CONTENTS

1.0 INTRODUCTION

This unit covers the types of cyber-attacks. It starts with web-based attacks and describes how this type of attack evolved. This unit also present system-based attacks familiarizes you with much of the vocabulary you hear with regards to cyber-attacks.

This unit covers the types of cyber attackers. It will familiarize you with much of the vocabulary you hear with regards to cyber-attacks including cyber criminals, hacktivists, state-sponsored attackers and insider threats.

In computer and computer networks, an attacker is that organisation or individual who performs malicious activities with the intention to exploit illegal use of an asset through unauthorised access thereto and possibly expose, destroy, disable, alter or steal it.
As Internet access and use become more global worldwide, practically everyone spends extensive time on the internet/web. Surprisingly, the population of attackers on the web is additionally on the rise. With this

increase, attackers strive to obtain unauthorized access using every method and implements at their disposal.

There are four kinds of attackers which are described in this unit.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the types of cyber-attacks
- Describing the web-based attacks
- Explaining the system-based attacks
- Understanding the Types of Cyber Attackers
- Describing the Cyber Criminals and Hacktivists
- Explaining the problems of State-sponsored Attackers
- Understanding the Insider Threats

3.0 MAIN CONTENT

Categories of Cyber Attacks and Attackers
A cyber-attack is the manipulation of computer systems and networks using malicious code to change code, logic or data and cause cybercrimes, like information and personality fraud. We reside in a very digital era. In this age and time, many people use computer and the internet to transact their businesses. In line with this dependency on digital things, the illegal computer activity is also growing and changing like all variety of crime.

Cyber-attacks are often classified into these categories:

3.1 Web-based Attacks

These are the attacks which occur on a web site or web applications. A number of the important web-based attacks are as follows-

a. Injection Attacks
It is the attack within which some data are going to be injected into an online application to control the applying and fetch the specified information.
Examples of Injection attacks include: code Injection, log Injection, - SQL Injection, XML Injection etc.

b. DNS Spoofing
DNS Spoofing may be a form of computer security hacking whereby an information is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker’s computer or the other computer.

The DNS spoofing attacks can persist for a protracted period of your time without being detected and may cause serious security issues

c. Session Hijacking

Session hijacking is a security attack on a user time period over a secured network where web applications generate cookies to store the network state and user sessions. By stealing the cookies, an attacker can have access to any or all of the user data.

d. Phishing

Phishing may be a sort of attack which attempts to steal sensitive information like user login credentials and master card number. It occurs when an attacker is masquerading as a trustworthy entity in e-mails and message transmission.

e. Brute Force

It is a sort of attack which uses a trial-and-error method. This attack generates an oversized number of guesses and validates them to get actual data like user password and private personal identification details. This attack could also be employed by criminals to crack encrypted data, or by security, analysts to check an organization's network security.

f. Denial of Service

- Denial of service is an attack meant to render a server or network resource unavailable to the users. It achieves this by saturating the target with heavy traffic or directing a large volume of information to it that that can triggers a crash. It uses the only one system and only one internet connection to attack a server. It’s often classified into the following based on the different goals-
- Volume-based attacks - to saturate the bandwidth of the attacked site, and is measured in bit per second.
- Protocol attacks- to consume actual server resources measured in a packet.
- Application layer attacks- to crash the online server measured in request per second.

g. Dictionary Attacks

The dictionary attack stores the list of a frequently used password and validated them to extract the original password.

h. URL Interpretation

It is a sort of attack where we are able to change the certain parts of a URL, and one can make an internet server to deliver web content that he's not authorized to browse.

i. File Inclusion attacks

File inclusion attacks are a kind of attack that enables an attacker to access unauthorized or essential files which is offered on the

net server or to execute malicious files on the net server by making use of the include functionality.

j. Man in the Middle attacks

It is a kind of attack that permits an attacker to intercept the connection between client and server and acts as a bridge between them. Because of this, an attacker can easily read, insert and modify the information within the intercepted connection. This is examined in details in Unit 2 of this module.

3.2 System-Based Attacks

These are the attacks which are intended to compromise a computer or a network. A number of the important system-based attacks is listed as follows-

a. **Virus**

It is a kind of malicious software program that spread throughout the personal computer's or other devices' files without the knowledge of a user. It's a self-replicating malicious program that replicates by inserting copies of itself into other computer programs when executed. It may execute instructions that cause harm to the system.

b. **Worm**

The worm is a sort of malware whose primary function is to copy itself to spread to uninfected computers. It works in the same way as the virus and often they are initiated from email attachments that appear to be from trustworthy senders.

c. **Trojan Horse**

It is a bug that causes unexpected changes to computer setting and weird activity, even when the machine or device should be idle. It misleads the user of its true intent. It appears to be a standard application but when opened/executed some malicious code will run within the background.

d. **Backdoors**

It is a technique that bypasses the traditional authentication process. A developer may create a backdoor in order that an application or package will be accessed for troubleshooting or other purposes.

e. **Bots**

A bot (short for "robot") is an automatic process that interacts with other network services. Some bots program run automatically, while others only execute commands after they receive specific input. Common samples of bots program are the crawler, chatroom bots, and malicious bots.

3.3 Hacktivists

Hacktivists are individuals or groups of hackers who do malicious activity to market a political agenda, belief, or social ideology. consistent with Dan Lohrmann,(https://cybersecurityventures.com/top-30-cybersecurity-experts-you-should-follow-in-2021/) chief security officer for Security Mentor, a national security training firm that works with states said "Hacktivism could be a digital disobedience. It's hacking for a cause." Hacktivists aren't like cybercriminals who hack computer networks to steal data for the cash. they're individuals or groups of hackers who work together and see themselves as fighting injustice.

3.4 State-Sponsored Attackers

State-sponsored attackers have particular objectives aligned with either the political, commercial or military interests of their country of origin. These sort of attackers aren't in a haste though most government organizations have highly skilled hackers who are focused on detecting vulnerabilities and exploiting these before the holes are patched. It's very challenging to defeat these attackers, thanks to the vast resources at their disposal.

3.5 Insider Threats

The insider threat could be a threat to an organisation's security or data that comes from within. These kinds of threats usually occurred from employees or former employees, but can also arise from third parties, including contractors, temporary workers, employees, or customers.
Insider threats are often categorized below-

a. Malicious

Malicious threats are attempts by an insider to access and potentially harm an organization's data, systems or IT infrastructure. These insider threats are often attributed to dissatisfied employees or ex-employees who believe that the organisation was doing something wrong with them in how, and that they feel justified in seeking revenge.

Insiders might also become threats after they are disguised by malicious outsiders, either through financial incentives or extortion.

b. Accidental

Accidental threats are threats which are accidently done by insider employees. During this sort of threats, an employee might accidentally delete a crucial file or inadvertently share confidential data with a business partner going beyond company’s policy or legal requirements.

c. Negligent

These are the threats within which employees try and avoid the policies of a corporation put in situ to shield endpoints and valuable data. as an example, if the organisation has strict policies for external file sharing, employees might try and share work on public cloud applications in order that they will work on it at home. There's nothing wrong with these acts, but they will open up to dangerous threats, nonetheless.

In-Text Question(s)

1. Enumerate web-based attacks

Answer:
Web based attacks are attacks occurring on the net/web. Some of these are: Injection attacks; DNS proofing; Session hijacking; phishing; brute force; denial of service; dictionary attack; URL interpretation; file inclusion attack and man-in-the-middle attacks.

2. Who is an attacker in terms of cyber security?

Answer:
An attacker is regarded as a process or person that attempts to access information, data, functions, or other restricted areas of the system without authorisation, possibly with malicious intents.

SELF-ASSESSMENT EXERCISE(S)

i. Differentiate between web-based attack and system-based attack.
ii. Discuss the current trend of attackers' methods.

Answer:

The hackers currently are employing all the available new technologies to perpetrate frauds and increase threat to the cyber space. This is noticeable with:

- Putting the Potentials of Artificial Intelligence (AI) into use.
- Increased target of Mobile devices.
- Potential Vulnerability of the Cloud.
- Prime target of Data Breaches.
- New Era of Technology and associated Risks with IoT and 5G Network
- Increased level of Automation and Integration
- Era of Targeted Ransomware.

4.0 CONCLUSION

In this unit, we learnt that cybersecurity attack is any form of malicious activity that targets information technology systems, or the people using them, to gain unauthorised access to the systems and the data or information they contain. In most cases, the cyber-attackers are criminals looking to exploit the attack for financial gain. about the types of cyber-attacks and how different types of attack evolved. The unit presented web-based attacks and system-based attacks while explaining the associated problems of representative attacks and attackers such as State-sponsored Attackers and the Insider Threats.

5.0 SUMMARY

In this unit we have learnt about:

- the types of cyber attacks
- the web-based attacks
- the system-based attacks
- the types of Cyber Attackers
- the problems of State-sponsored attackers
- the Insider threats

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Brook S. E. Schoenfield. (2020) Secrets of a Cyber Security Architect, CRC Press

Cybersecurity Breakthrough Award 'CISO of the Year' for global security product and services companies (2017). See: https://cybersecuritybreakthrough.com/2017-winners/

Edward Griffor. (2017) Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems Syngress advanced topics in information security, Syngress

Nicholas J. Daras. (2019) Cyber-Security and Information Warfare, Cybercrime and Cybersecurity Research, Nova Science Publishers.

Tony Thomas, Athira P Vijayaraghavan, Sabu Emmanuel. (2020) Machine Learning Approaches in Cyber Security Analytics, Springer.

Zheng Xu, Kim-Kwang Raymond Choo, Ali Dehghantanha, Reza Parizi, Mohammad Hammoudeh. (2020) Cyber Security Intelligence and Analytics Advances in Intelligent Systems and Computing 928 Springer International Publishing.

https://cybersecurityventures.com/top-30-cybersecurity-experts-you-should-follow-in-2021/

https://www.reflectiz.com/blog/top-cybersecurity-experts-to-follow/

UNIT 2 MAN-IN-THE-MIDDLE ATTACKS

CONTENTS

1.0 INTRODUCTION

This unit covers the Man-in-the-Middle Attacks. The unit explains how the MITM work. It details the types of MITM attacks and the detection mechanism of Man-in-the-Middle Attack. Finally, it explores the preventions of Mani-in-the-Middle Attack.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the Man-in-the-Middle Attacks
- Describing how MITM work
- Explaining the types of MITM Attacks
- Understanding how to detect Man-in-the-Middle Attack
- Explaining the preventions of Mani-in-the-Middle Attack

3.0 MAIN CONTENT

Man-in-the-Middle Attack

A MITM attack may be a style of cyber-attack where a user is introduced with some reasonably meeting between the 2 parties by a malicious individual, manipulates both parties and achieves access to the information that the 2 people were trying to deliver to every other. A man-in-the-middle attack also helps a malicious attacker, with none quite participant recognizing till it's too late, to hack the transmission of information intended for somebody else and not alleged to be sent in the least.

In certain aspects, this manner of assault comes in some ways, for example, for an intruder to intercept financial login credentials,

fraudulent banking websites are often used. Between the user and also the real bank webpage, the fake sites lie "in between - in the middle."

3.1 How does MITM work?

There are several reasons and techniques for hackers to use a MITM attack as shown in Figure 4.1. Usually, like master card numbers or user login details, they fight to access anything. They also spy on private meetings, which can include corporate secrets or other useful information.

The feature that nearly every attack has, in general, is that the attacker pretends to be somebody you trust (or a webpage).

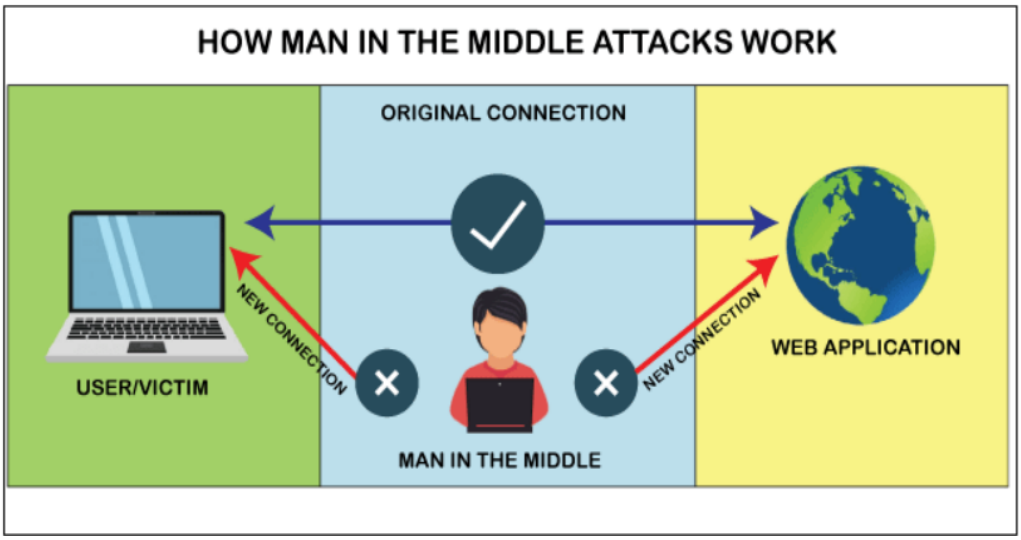

Figure 4.1: How MITM works

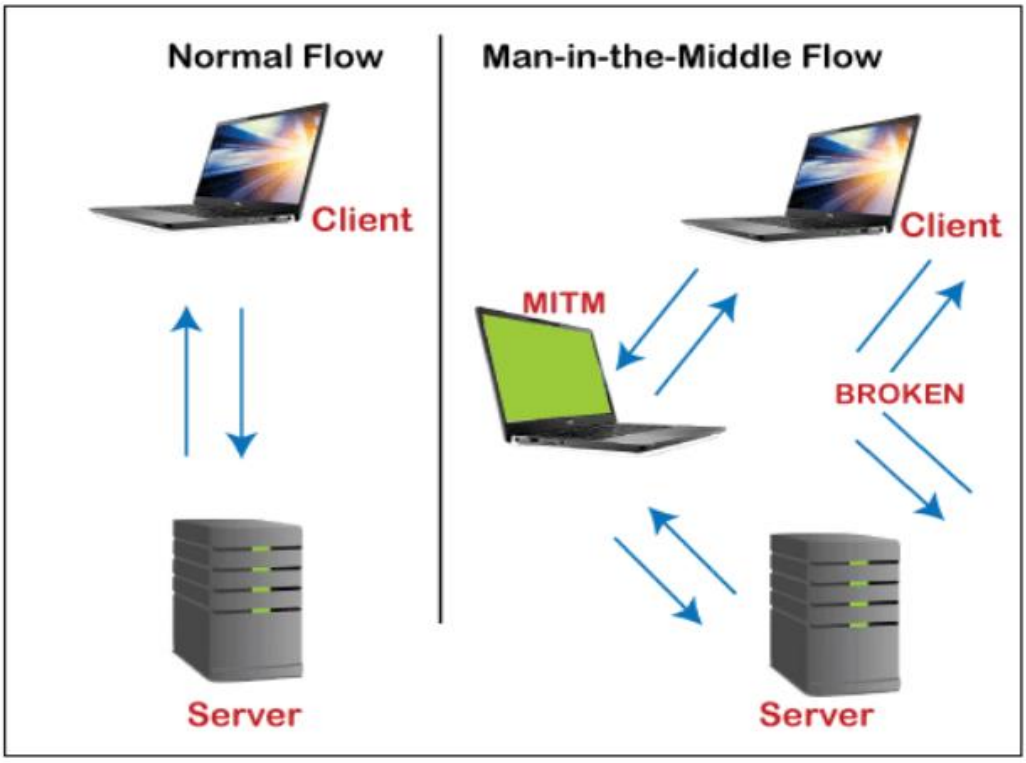

Figure 4.2: Real life Instances of MITM attack

In Figure 4.2, it is seen that the intruder positioned himself in between the client and server to intercept the confidential data or manipulate the wrong information of them.

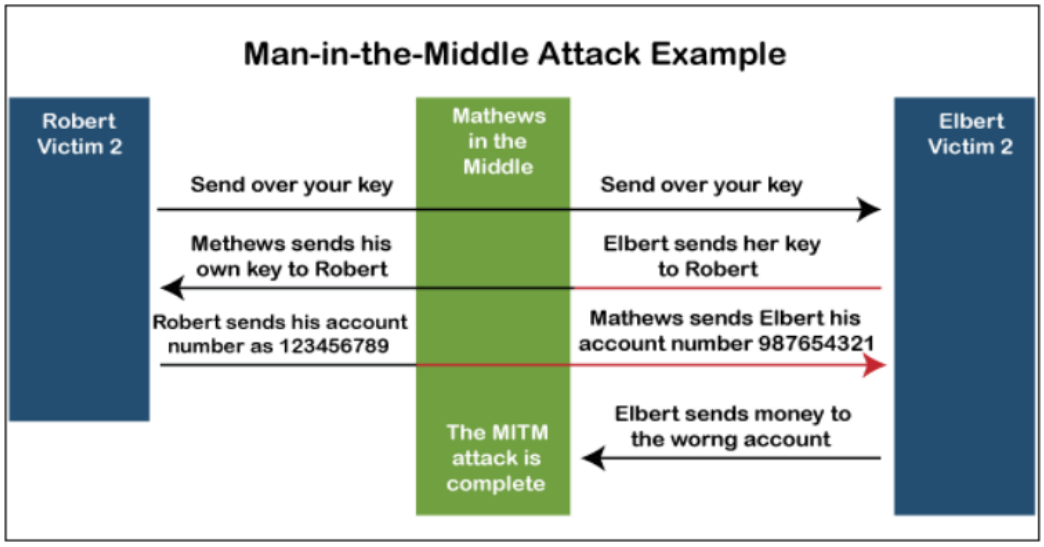

Figure 4.3: An Instance of MITM attack

As shown in Figure 4.3, to get access to banking transaction, the attacker is trying to imitate each side of the discussion. This instance is accurate for the client and therefore the server discussions and also person-to-person discussions. Shown during this instance, the attacker retrieves a public key and might modulate his own passwords to control the audience to simply accept that they're safely communicating with one another at either end.

3.2 Types of MITM Attacks

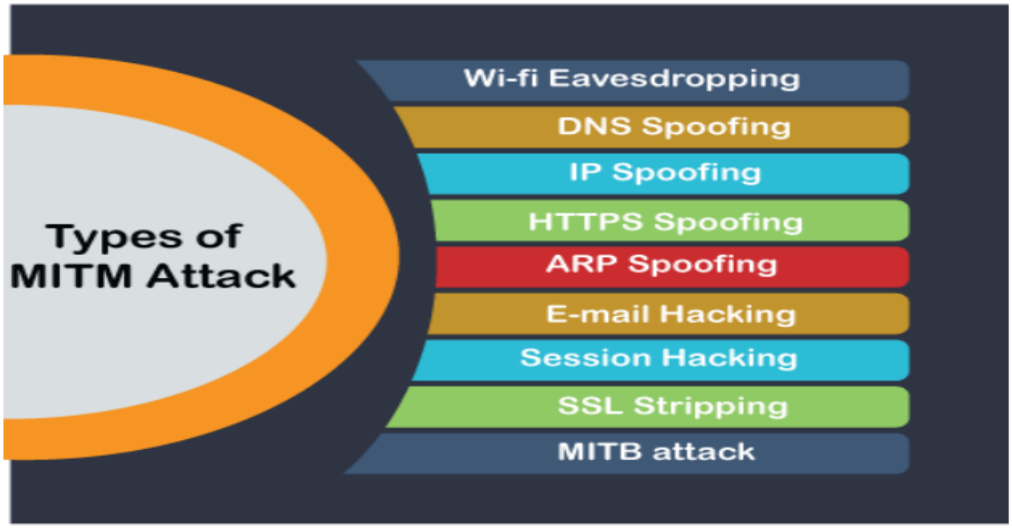

Figure 4.4: Types of MITM Attacks

1. **Wi-Fi Eavesdropping**
   You may have seen a notification that implies, "This connection isn't safe," if you've used a machine in a public internet cafe. Public Wi-Fi is usually offer "as-is," with no promises of service quality. The unencrypted Wi-Fi networks are easy to look at. Although, it's a bit like having a debate during a public place-anybody can take part. Figure 4.4 depicts all the types of MITM attacks.

   Wi-Fi snooping attack occurs when an attacker establishes his own "Evil Twin" Wi-Fi hotspot similar to the public Wi-Fi. Attackers make the link, through the network Address and passwords, appear similar to the original ones. Users will link to the "evil twin" unintentionally or automatically, enabling the attacker to intrude into their actions.
2. **DNS Spoofing**
   The Site operates with numeric IP addresses like 208.113.216.59 is one amongst National Open University of Nigeria IP addresses. For example, a server is employed by several sites to interpret the address to a recognizable title: noun.edu.ng. A DNS server, or DNS, is that the server that transforms 208.113.216.59 to noun.edu.ng.
   A fraudulent Web server are often developed by an attacker. The fraudulent server transports a selected web address to a singular IP address, which is termed as "spoofing."
3. **IP Spoofing**
   Many devices connected to the identical network contains an IP address, as we all know. Each device is supplied with its IP address in several enterprise internal web networks. In IP

spoofing, the attackers replicate an appropriate console's IP address. For a network, it appears even as the system is permitted, however, this can be causing the network or system to be exploited by unauthorized access. Here, users have to be careful and have to stay quiet and track the actions, or a Denial of Service (DoS) attack can also be released by the attackers. In a very extreme cases, a Middle-in-the-man attack or IP spoofing may additionally be utilized by placing between two devices. The IBM X-Force 's Threat Intelligence 2018 Reports. It is represented in the Pie chart shown in Figure 4.5.

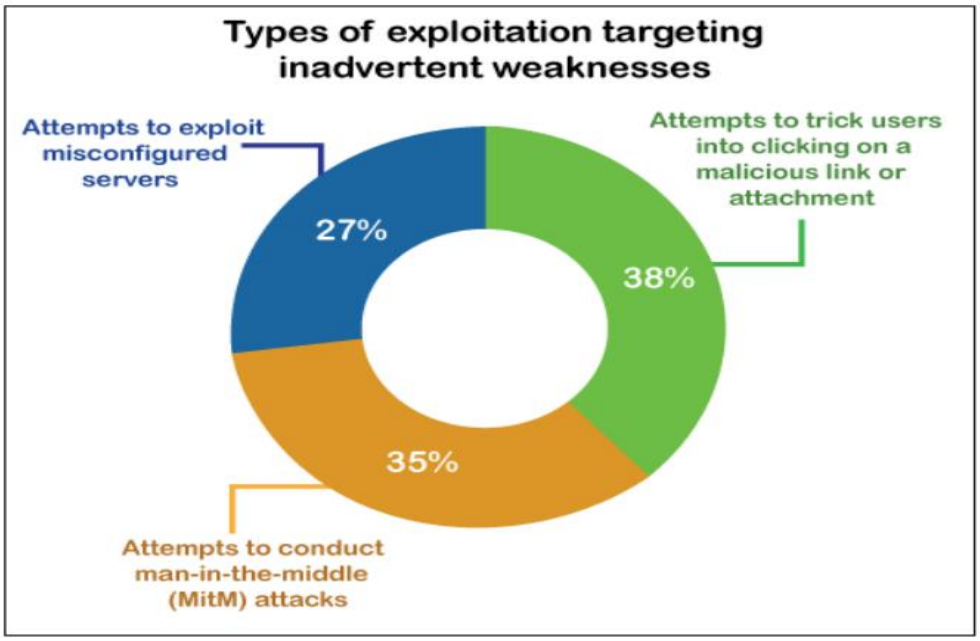

Figure 4.5: Exploitation targeting inadvertent weaknesses

4. HTTPS Spoofing

Duplicating an HTTPS webpage isn't currently possible, however hackers and attackers are circumventing HTTPS by creating an authoritative address. It uses letters of international alphabets instead of standard scripts. This acts as phishing emails with unusual characters that you simply could have used. Adekunle is also written Adékunlé, as an example.

5. ARP Spoofing

ARP refers to the Protocol on Address Resolution. An ARP request is shipped out by a client, and an attacker produces a fraudulent response. The attacker is sort of a computer modem during this situation, which enables the attacker to access the traffic flow. Usually, this is often restricted to local area networks (LAN) that use the ARP protocol.

6. E-mail Hacking

An attacker exploits the e-mail system of a user in this form of cybersecurity intrusion where he eavesdrops on the discussion via email and watches quietly while collecting data. The Attackers

may have a scan pattern that searches for targeted keywords, like "financial" or "hidden democratic policies."

Through Social Engineering, email hacking operates perfectly. To imitate a web friend, the attackers might use relevant data from some quite hijacked email address. Spear-phishing may be accustomed trick a user into downloading malicious apps.

7. **Session Hacking**

Usually, this manner of MITM attack is usually wont to hack social media platforms. The webpage contains a "session browser cookie" on the victim's machine for many social media platforms. It can occur if a user exploits an XSS cross-scripting intrusion, during which the hacker injects malicious script into a site that's commonly visited.

8. **SSL Stripping**

SSL refers to Secure Socket Layer. SSL is that the security standard used if you see https:/ next to an internet site address, not http:/. The user tries to link to an internet site that's secured. within the account of the client, the attacker encrypts and links to the secured website. The victim thinks that they need signed on to the traditional website, but actually they signed in to a hacker's website. The attacker does have the SSL certificate "stripped" from the information connection of the victim.

9. **MITB attack**

This is a kind of attack that leverages internet browser security flaws. The malicious attacks are Trojans, desktop worms, Java vulnerabilities, SQL injection attacks, and web browsing add-ons. These are commonly wont to collect financial information.

Malware steals their passwords because the user signs in to their checking account. In certain instances, malware scripts may move money also altering the receipt of the transaction to hide the transaction.

3.3 Detection of Man-in-the-Middle Attack

It is harder to spot a MITM attack without taking the acceptable measures. A Man-in-the-middle assault will theoretically proceed unchecked till it's too late once there is no conscious evaluation need to determine if your communications are being monitored. Usually, the major technique for identifying a potential-attacks is usually looking for adequate page authorization and introducing some type of temper authentication; however, these approaches may have further forensic investigation after-the-fact.

Instead of trying to spot attacks after they are operational, it's necessary to manage precautionary measures to avoid MITM attacks whenever they occur. To sustain a secure environment, being mindful of your

surfing habits and identifying possibly hazardous environments is important.

3.4 Preventions of Man-in-the-Middle Attack

Here, we've discussed some prevention techniques to avoid the interactions being compromised by MITM attacks.

1. **Wireless access point (WAP) Encryption**
   Creating a robust protection feature on access points eliminates legitimate access just from being closer from accessing the system. A vulnerable system of protection will enable an intruder to brute-force his way into the system and begin attacking the MITM.
2. **Use a VPN**

- Use a Virtual Private Network (VPN)
  Be prepared to stop data loss; have a cybersecurity incident response plan. This can be in the form of an encrypted VPN that severely limits a hacker's ability to read or modify web traffic.
- Network Security
  Secure your network with an intrusion detection system through regular analysis of traffic patterns to identify unusual behaviour. Here, Network administrators should be ready to mitigate a man-in-the-middle attack. by using proper network sanitisation.

3. **Public Key Pair Authentication**
   In numerous layers of the protocol stack, public key pair authentication like RSA is employed to confirm that the objects you communicate therewith are essentially the objects you wish to speak with. This will prevent spoofing in the network.
4. **Strong Network User Credentials**
   Ensuring that the first email login is modified is extremely important. This should be done not only for the login details for Wi-Fi but also for the password hashes for the router. When a hacker detects the wireless router login details, they'll switch the fraudulent servers to the DNS servers.
5. **Communication Security**
   Communication security help the users to be guarded from unauthorized messages and provides secure encoding.
   Enabling two-factor authentication is the most powerful method to avoid account hacking. It implies that you're going to need to give another protection factor, in contrast together with your login credentials. One instance is that conjunction of a login credential and a text to your device from Gmail.

6. Using proper hygiene for network protection on all platforms,

The use of smartphone apps on the network is a good practice for proper network protection hygiene.

Since phishing emails are the foremost popular attack vectors, be cautious and on the lookout before or when opening a spam email. Reduce the prospect of exploits to disprove persistent cookies by logging out inactive accounts and execute a security scan if you anticipate a secure link but don't have one.

7. Avoid Using Public Wi-Fi

Configure your phone to require a manual link if you're using public Wi-Fi. It can be hard to identify MITM attacks as they are occurring. The easiest way to remain secure is to regularly incorporate all of the above prevention for security. Be conscious that such attacks are a part of social engineering. Take a couple of minutes to dig deeper if anything doesn't seem normal about social media and email.

In-Text Question(s)

1. Enumerate five MITM attacks

Answer:
MITM are manifested in any of the following forms: Wi-Fi Eavesdropping; DNS Spoofing; IP Spoofing; HTTPS Spoofing; ARP Spoofing; Email hacking; Session hacking, SSL Stripping and MTB attack.

2. What is the main leverage of most information systems attacks?

Answer:
Most of the information systems attacks leverage on the security flaws in the applications, systems, browsers and users' security lapses.

SELF-ASSESSMENT EXERCISE(S)

i. Differentiate between web-based attack and system-based attack.

Answer:
In web based, criminals exploit vulnerabilities in coding to gain access to a server or database, these types of cyber security threats are known as application-layer attacks. In system based, the criminals run a type of malicious software program that spread throughout the computer files without the knowledge of the user. These are self-replicating malicious computer programs that replicate by inserting copies of themselves into other computer programs when executed.

4.0 CONCLUSION

In this unit, we learnt about the categories of cyber-attacks and the way differing types of attack evolved. The unit presented web-based attacks and system-based attacks familiarises you with much of the vocabulary you hear with regards to cyber-attacks.

5.0 SUMMARY

In this unit we have learnt about:

- the types of cyber attacks
- the web-based attacks
- the system-based attacks

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Brook S. E. Schoenfield. (2020) Secrets of a Cyber Security Architect, CRC Press.

Edward Griffor. (2017) Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems Syngress advanced topics in information security, Syngress.

Nicholas J. Daras. (2019) Cyber-Security and Information Warfare, Cybercrime and Cybersecurity Research, Nova Science Publishers.

Tony Thomas, Athira P Vijayaraghavan, Sabu Emmanuel. (2020) Machine Learning Approaches in Cyber Security Analytics, Springer.

Zheng Xu, Kim-Kwang Raymond Choo, Ali Dehghantanha, Reza Parizi, Mohammad Hammoudeh. (2020) Cyber Security Intelligence and Analytics Advances in Intelligent Systems and Computing 928 Springer International Publishing.

https://www.ibm.com/downloads/cas/ADLMYLAZ

UNIT 3 CYBER SECURITY WI-FI ATTACKS

CONTENTS

1.0 INTRODUCTION

Wireless networks (Wi-Fi) have come to be an integral part of how businesses are conducted all over the world. The Wi-Fi security vulnerabilities permit attackers to change smart switches. This unit looks at some attack scenarios include intercepting users' authentication credentials and MAC addressing filtering. The attackers could also exploit the vulnerabilities as a “stepping stone to blast-off advanced attacks.

2.0 INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the Wi-Fi security
- Describing how Wi-Fi security works
- Explaining the hidden SSID
- Understanding how MAC Address filtering works
- Explaining the enterprise authentication of Wi-Fi
- Identifying Fake Wi-Fi Access points

3.0 MAIN CONTENT

Cyber Security Wi-Fi Attacks

A powerful and essential area to computer security is WIFI. Devices and systems aren't any longer required to be interconnected via physical cables, but can instead be reached by anyone within signal radius. WIFI has enabled a number of new devices to be capable of networking. WIFI

as most of the people are aware of it stems from the IEEE 802.11 protocol. Other protocols using radio for signalling include:

- ✓ Bluetooth, for communicating with devices we feature, typically smartphones, headphones etc.
- ✓ NFC ("Near Field Communications"), implemented in access badges and credit cards for wireless transmission of information.
- ✓ RFID ("Radio Frequency Identification"), used for access cards and other devices, for instance a car which might wirelessly transmit its identifier to a toll-road system.
- ✓ ZigBee and Z-Wave, used for enterprise and residential automation.

Wireless communication is usually done via an Access Point (AP), a wireless base station which acts as a switch and router between clients that wish to speak. Peer-to-peer communications also are possible, but less typical.

The name of a wireless network is thought because the SSID ("Service Set Identifier").

Because WIFI signals reach everyone within the vicinity it enables attackers to simply use an antenna to "sniff" communications for anyone transmitting. Sniffing simply means to concentrate for packets which the network interface can see.

WIFI sometimes allow users to achieve internal applications, increasing attack potential. Furthermore, WIFI devices have management interfaces and firmware which may hold vulnerabilities, sometimes not always patched as timely as other assets within the enterprise.

3.1 WIFI Security

WIFI have the choice of

- No security
- Access list supported MAC addresses
- Pre-Shared Key (PSK)
- Enterprise authentication

Many WIFI attacks depend on network cards with two primary features, namely:

- Monitor Mode: Makes the network card forward packets destined to any or all MAC addresses to the OS, not just its own.
- Packet Injection: The network card supports crafting packets with a special source MAC address than its own.

An open WIFI network could be a network with no password thereon. Communication between AP and Clients isn't encrypted and everybody has got to depend upon their own sources of encryption to guard their traffic. These varieties of networks are very convenient and accessible for users, but give room for security compromises.
An attacker on these varieties of networks can easily see what everyone else is doing by simply sniffing packets. Such packets can contain sensitive details or just details about what the users do on the network.

3.2 Hidden SSID

AP's can often shut down broadcasting the name of the wireless network, requiring users to demonstrate knowledge of the SSID to connect to the network. It's not considered best-practice to enable hidden SSID, because the name of the network is exposed anytime a client joins. Furthermore, the clients now have to ask and broadcast information about the network they need to affix, everywhere they travel. An attacker could then sniff the WIFI traffic of clients and potentially learn more information about whom the clients are and where they need joined networks before.

3.3 MAC Address Filtering

Some AP's support access control supported MAC Addresses. The AP can create an allow-list of which MAC addresses should be allowed to affix and communicate on the network.

This approach is in-secure since an experienced attacker can sniff and detect other systems communicating on the network, record their MAC addresses and update his/her own MAC address to be one which is already allowed. This effectively bypasses the MAC Address Filtering requirement.

3.4 Pre-Shared Key (PSK)

Pre-Shared Key basically means the network is designed with a password. PSK protection is often implemented via a protocol called WIFI Protected Access (WPA). Older protocols for authentication also can be used, for instance Wired Equivalent Privacy (WEP) but has for the recent past been considered obsolete because it is extremely in-secure and straightforward for attackers to crack.

WPA comes in numerous forms with WPA3 being the most recent standard as of the year 2021. WPA isn't entirely safe against attackers either, but offers rather more protection than WEP. to interrupt into a WPA enabled network the attacker must attempt to crack the password

with a password cracker. this is often considered an upscale process in terms of your time if the password in all fairness strong.

If an attacker can observe (sniff) anyone whom authenticates to the network, they need enough to interact in password cracking activities. Tools like aircrack-ng (https://www.aircrack-ng.org/) supports cracking WIFI passwords.

3.5 Enterprise Authentication

Enterprise Access Points may also support authenticating clients supported certificates, which needs PKI ("Public Key Infrastructure") or enterprise credentials by integrating to a centralized authentication service.

There are some benefits here, especially, with the concept of key management. The natural challenge in managing a PSK network is how passwords are distributed, rotated and revoked.

While Enterprise Authentication offers better security management with regards to keys, it likewise involves a more sophisticated infrastructure and provides other opportunities for attackers.

3.6 Fake WIFI Access Points

Attackers can effortlessly start broadcasting networks pretending to be additional networks. Often clients will automatically hook up with networks in range if they present themselves with the acceptable SSID. This enables attackers to force clients connect to the attackers' network, allowing them to detect and alter traffic according to the attacker's wishes.

In-Text Question(s)

1. Enumerate the protocols using radio for signaling

Answer:
Bluetooth; NFC; RFID; ZigBee and Z-Wave.

2. Explain the acronyms WPA and WEP

Answer:
(WPA) - WIFI Protected Access
WEP - Wired Equivalent Privacy

SELF-ASSESSMENT EXERCISE(S)

i. Discuss the best practices in dealing with Wi-Fi attacks.

Answer:
Some of the best practices in dealing with Wi-Fi attacks are: Separating Internal and Guest Users on the network; Using Wi-Fi Protected Access; Physically Securing Access Points; Limiting WiFi Signal Strength; Using Rogue Access Point Detection devices; Using Wireless Intrusion Prevention Systems and Practicing of Mobile Device Management. The following are also recommended for use: Firewalls; Intrusion Detection; Content Filtering; Authentication and Data Encryption.

4.0 CONCLUSION

Wireless networks (Wi-Fi) have come to be an integral part of how businesses are conducted all over the world. The Wi-Fi security vulnerabilities permit attackers to change smart switches. In this unit, we have seen that cyber security of Wi-Fi is essential since it is a powerful and essential area to computer and information security. Devices and systems aren't any longer required to be interconnected via physical cables, but can instead be reached by anyone within signal radius.

5.0 SUMMARY

In this unit we have learnt about:

- the Wi-Fi Security
- how the hidden SSID works
- the types of MAC address filtering
- how to use enterprise authentication
- how to determine and prevent use of fake Wi-Fi points

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Nicholas J. Daras. (2019) Cyber-Security and Information Warfare, Cybercrime and Cybersecurity Research, Nova Science Publishers

Zheng Xu, Kim-Kwang Raymond Choo, Ali Dehghantanha, Reza Parizi, Mohammad Hammoudeh. (2020) Cyber Security Intelligence and Analytics Advances in Intelligent Systems and Computing 928 Springer International Publishing.

Brook S. E. Schoenfield. (2020) Secrets of a Cyber Security Architect, CRC Press.

Edward Griffor. (2017) Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems Syngress advanced topics in information security, Syngress.

Tony Thomas, Athira P Vijayaraghavan, Sabu Emmanuel (2020). Machine Learning Approaches in Cyber Security Analytics, Springer.