COURSE GUIDE

CIT 855

ADVANCED CYBER SECURITY

Course Team

Prof. Olumide Babatope Longe (Developer/Writer)

NATIONAL OPEN UNIVERSITY OF NIGERIA

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

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

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

Printed 2022

ISBN:

Table of Contents

Introduction

In recent years, the phrase "Cyber Security" has been more often used by both professionals and governments. However, as is the case with many current slang terms, there seems to be little grasp of what the phrase means in reality. While this may not be a problem when the phrase is used informally, it might present significant issues in the context of an organization's strategy, corporate goals, or agreements with other countries across the world.

It is possible to preserve an organization's and its users' assets via the use of a variety of cyber security-related methods and instruments such as policies, procedures, security concepts, safeguards, guidelines, and risk management techniques.

Connected computer devices, employees, infrastructure, applications and services as well as telecommunications systems and the totality of information sent or stored in the cyber environment constitute the assets of an organization or individual user.

The goal of cybersecurity is to guarantee that the security properties of the business and the assets of its users are protected against relevant cyber threats.

What You Will Be Learning in this Course

This course consists of units and a course guide. This course guide tells you briefly what the course is about, what course material you will be using and how you can work through these materials. In addition, it advocates some general guidelines for the amount of time you are likely to spend on each unit of the course in order to complete it successfully.

It gives you guidance in respect of your Tutor-Marked Assignments which will be made available in the assignment file. There will be regular tutorial classes that are related to the course. It is advisable for you to attend these tutorial sessions.

The course will prepare you for the challenges you will meet in the understanding and application of cyber security.

Course Aim

The aim of the course is an introductive part of cyber security. CIT110 aims to furnish you with enough knowledge so as to understand basic principle of cyber security and cyberspace environment, both from the organization and user points of view.

Course Objectives

To achieve the aims set out, the course has a set of objectives. Each unit has specific objectives which are included at the beginning of 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 doing so, you would know whether you have followed the instruction 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 earlier stated, this course sets to achieve some objectives. Thus, after going through the course, you should be able to:

- Explain the concept of cyber security
- Describe the benefit of cyber security
- Explain cyber security counter measures
- Explain cyber space and cyber law
- Define Cyber Security
- Classify Cyber crimes
- Describe the types of cyber crime
- Explain the concept of cyber crime
- Understand who is a hacker
- Demonstrate cyber crime motivation
- Demonstrate the concept of firewall
- Explore the importance of firewalls
- Explain the concepts of VPNs
- Set up a simple VPN
- Explain the concept access control

- Manage access control
- Improve their data privacy through hardware protection
- Protect yourselves from software and internet attacks
- Explain the concept of computer forensics
- Explain the characteristics of digital forensics
- Explain digital forensics procedure
- Explain the advantages of computer forensics
- Disadvantages of computer forensics
- Explain the concept of Disk Forensics
- Explain the process of Disk Forensics
- Explain Network Forensics procedure
- Explain Network Forensics
- Explain Examinations of Network Forensics
- Explain Malware Forensics
- Explain the concept of Email Forensics
- Explain the concept of Memory Forensics
- Explain the concept of Mobile Phone Forensics
- Explain ddigital Forensic Examination Process
- Justify cyber crimes as sanctioned in cyber laws
- Demonstrate the concept of cyber law
- Understands laws binds to cyberspace
- Know their rights in data and privacy protection
- Learn from existing scenarios of cybercrimes in India
- Explain international laws and treaties
- Explain international cyber-attacks previously occurred
- Understand the use of ethical theories in ethical arguments.
- Articulate the ethical tradeoffs in a technical decision.
- Understand the role of professional codes of ethics.

Working through this course

To complete this course, you are required to read each study unit, read the textbooks and read other materials which may be provided by the National Open University of Nigeria.

Each unit contains self-assessment exercises and at certain point in the course you would be required to submit assignments for assessment purposes. At the end of the course there is a final examination. The course should take you about a total of 17 weeks to complete. Below you will find listed all the components of the course, what you have to do and how you should allocate your time to each unit in order to complete the course on time and successfully.

This course entails that you spend a lot time reading. I would advise that you avail yourself the opportunity of comparing your knowledge with that of other learners.

Course Material

The major components of the course are:

1. Course Guide
2. Study Units
3. Presentation Schedule
4. Tutor-Marked Assignments
5. References/Further Reading

Study Units

The study units in this course are as follows:

Module 1	**Cyber Security Fundamentals**
Unit 1	Cyber Security Fundamentals, Benefits, Cyber space and Cyber-Law
Unit 2	Cyber Crimes Classification and Types of Cyber Crimes
Unit 3	Scope of Cybercrimes
Module 2	**Cyber Threat Management**
Unit 1	Firewalls
Unit 2	Virtual Private Networks (VPN)
Unit 3	Security Control Management
Unit 4	Hardware and Software Prevention

Module 3	**Computer Forensics and Digital Investigation**
Unit 1	Computer Forensics
Unit 2	Network, Disk, Malware and Database Forensics
Unit 3	Email, Memory and Mobile Forensics
Unit 4	Malware Analysis

Module 4	**Introduction to Cyber Law and Ethics**
Unit 1	Concept of Cyber Law
Unit 2	The INDIA cyber-Acts
Unit 3	The International Laws
Unit 4	Cyber Ethics

The first module teaches the fundamentals of cyber security. It explains the cyber-crime world, who are cyber attackers, their motivations and benefits. The module further discusses the types of attacks carry out by attackers, the tools and techniques they use and how they explore their targets.

Module Two highlighted cyber threat prevention concepts. Most prevention techniques were discussed in this module. The importance of firewalls in traffic control, traffic diversion using VPN, access control management, protecting yourself from cyber-attack and hardware security implementation are all discussed in this module

In the module Three, we have discussed many computer investigation measures known as forensic analysis. When cyber guru is been suspected of cyber frauds act, the only means of verifying the claim is to carry out forensic analysis on the suspect operating computer. Why forensic analysis, importance of forensic analysis and types of forensic analysis are all discussed in this module.

The last module tries to look at law enforcement binding cyber activities. Strength, limits and rules that guide what one can do on the cyber space are discussed in this module. We discussed why we need cyber law and some law Acts that reflect cyber rule and regulation. Finally cyber ethics for professional cyber space usage was also addressed.

Each unit consists of one or two weeks' work and include an introduction, objectives, reading materials, exercises, conclusion, summary, tutor-marked assignments (TMAs), references and

other resources. The units direct you to work on exercises related to the required reading. In general, these exercises test you on the materials you have just covered or require you to apply it in some way and thereby assist you to evaluate your progress and to reinforce your comprehension of the material. Together with TMAs, these exercises will help you in achieving the stated learning objectives of the individual units and of the course as a whole.

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 guide against falling behind in your work.

Assessment

There are three aspects to the assessment of the course. First is made up of self-assessment 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 have gathered during the course. The assignments must be submitted to your facilitator for formal assessment in accordance with the deadline stated in the presentation schedule and the assessment file. The work you submit to your tutor for assessment will count for 30% of your total course mark. 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 (TMAs)

The TMA is a continuous assessment component of your course. It accounts for 30% of the total score. You will be given four TMAs to answer. Three of these must be answered before you are allowed to sit for end of course examination. The TMAs would be given to you by your facilitator and should be returned after you have done the assignment. Assignment questions for the units in this course are contained in the assignment file. You will be able to complete your assignments 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 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 in exceptional circumstances.

Final Examination and Grading

The end of course examination for Cyber Security 1 (CIT110) will be for three (2) hours and it has a value of 70% of the total course score. 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.

Use the time between finishing 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	For assignment, best three marks of the four counts at 10% each, i.e., 30% of Course Marks.
End of Course Examination	70% 0f the overall Course Marks.
Total	100% of Course Material.

Facilitators/Tutors and Tutorials

There are 16 hours of tutorials provided in support of this course. You will be notified of the dates, time, and location of these tutorials as well as the name and phone number of your facilitator, as soon as you are allocated to 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 Assignments 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 assigned readings
- You have difficulty with self-tests
- You have 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 to face contact with your course facilitator and to ask questions which may be answered instantly. You can raise any problem encountered in the course of your study.

To have more benefits from course tutorials, you are advised to prepare a list of questions before attending them. You will learn a lot from participating actively in discussions.

Summary

Cyber Security 1 is a course that intends to intimate the learner with basic facts on cyber space, crime, security, cyber regulations and professional ethics. Upon completing this course, you will be equipped with the knowledge of cyber security fundamentals, who are cyber attackers and what acts are classified as cybercrime, prevention means against cyber-attacks, cyber investigation and laws that regulate cyber activities.

I wish you success in the course and I hope you find it very interesting.

CONTENTS **PAGE**

Module 1: Cyber Security Fundamentals

Introduction of Module

As more human activities, financial, technical, and communication processes migrate into cyberspace, online vulnerability and cyber-attacks remain an issue that has continued to plague the online environment. Cyber security has always been an important aspect of computing systems but its importance has increased greatly in recent years. The curriculum covers areas where cyber security is of major importance, but have different security requirements and may be exposed to different threats and attacks. It also covers techniques and mechanisms used to secure computer systems and data to meet those requirements and protect them. The areas looked at include computer operating systems (and increasingly, distributed operating systems), distributed applications (such as electronic commerce over the Internet), embedded systems (ranging from smart cards to large industrial plant and telecommunications systems), and users. The techniques and mechanisms looked at include cryptography, authentication & authorization, and access control. Furthermore, the curriculum integrates the legal, ethical, and professional perspectives, for instance, to address concerns about data security, privacy, and societal impact of computing systems.

UNIT 1 CYBER SECURITY FUNDAMENTALS, BENEFITS, CYBER SPACE AND CYBER-LAW

CONTENTS

1.0 Introduction

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization. A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations.

2.0 Intended Learning Outcomes (ILOs)

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

- explain the concept of cyber security
- describe the benefit of cyber security
- explain cyber security counter measures
- explain cyber space and cyber law.

3.0 Main Content

3.1 Cyber security

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.Maintaining cybersecurity in a constantly evolving threat landscape is a challenge for all organizations. Traditional reactive approaches, in which resources were put toward protecting systems against the biggest

known threats, while lesser known threats were undefended, is no longer a sufficient tactic. To keep up with changing security risks, a more proactive and adaptive approach is necessary. Several key cybersecurity advisory organizations offer guidance. For example, the National Institute of Standards and Technology (NIST) recommends adopting continuous monitoring and real-time assessments as part of a risk assessment framework to defend against known and unknown threats.

3.2 Benefits of cybersecurity

The benefits of implementing and maintaining cybersecurity practices include

- Business protection against cyberattacks and data breaches.
- Protection for data and networks.
- Prevention of unauthorized user access.
- Improved recovery time after a breach.
- Protection for end users and endpoint devices.
- Regulatory Compliance
- Business continuity.
- Improved confidence in the company's reputation and trust for developers, partners, customers, stakeholders and employees.

3.3 Cyber security domains

A strong cybersecurity strategy has layers of protection to defend against cyber crime, including cyber attacks that attempt to access, change, or destroy data; extort money from users or the organization; or aim to disrupt normal business operations. Countermeasures should address

3.3.1 Critical infrastructure security

practices for protecting the computer systems, networks, and other assets that society relies upon for national security, economic health, and/or public safety. The National Institute of Standards and Technology (NIST) has created a cybersecurity framework to help

organizationsin this area, while the U.S. Department of Homeland Security (DHS) provides additional guidance.

3.3.2 Network security

Practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware

3.3.3 Application security

Processes that help protect applications operating on-premises and in the cloud. Security should be built into applications at the design stage, with considerations for how data is handled, user authentication, etc.

3.3.4 Cloud security

specifically, true confidential computing that encrypts cloud data at rest (in storage), in motion (as it travels to, from and within the cloud) and in use (during processing) to support customer privacy, business requirements and regulatory compliance standards.

Information security

Protects the integrity and privacy of data, both in storage and in transit.

3.4 Operational security

Includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

3.5 End-user education

Addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization. End-user education also helps in building security awareness across the organization to strengthen endpoint security. For example, users can be trained to delete suspicious email attachments, avoid using unknown USB devices, etc.

3.6 Disaster recovery / business continuity planning

Defines how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources

3.7 Storage security

This includes encryption and immutable and isolated data copies. These remain in the same pool so they can quickly be restored to support recovery, minimizing the impact of a cyber attack.

3.8 Cyberspace

Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol to aid in communication and data exchange activities. Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.

3.9 Cyber Laws

Cyber laws encompass all the legal issues related to the communicative, distributive and transactional aspects of network-related information devices and technologies. It is different from the Property Law or any other law. Unlike property law, it is not so distinct; it is broader since it covers several areas of laws and regulations. It encapsulates the statutory, legal and constitutional provisions related to computers and the internet. Cyber laws are related to individuals and institutions that

- Plays a crucial role in providing cyberspace access to people
- Generates software and/or hardware to allow people with entry into cyberspace, and
- Make use of their computer system to gain entry into cyberspace.

3.9 Cyber Laws and Cyber Security

In order to ensure that humans do not misuse cyber technologies, cyber laws are generated. The overall idea of the cyber law is to stop any person from violating the right of other persons in

cyberspace. Any kind of violation of cyber rights is considered to be a cyberspace violation and are deemed punishable under cyber laws. It is important to note that since cyberspace does not belong to the physical world, the physical laws do not apply to cyberspace crime. A separate set of cyber laws are formulated by the government to provide cybersecurity to cyber users. Such cyber laws are needed to monitor and prevent any immoral or illegal activities of humans. Some of the common cyberspace violation activities include hacking, theft, money laundering, terrorism, piracy, etc. Hackers can get hold of any internet account through the Domain Name Server (DNS), phishing, IP address, etc. to get entry into the computer system of any person and steal the data, or introduce computer bugs and render the system ineffective.

Discussion

Which of the security infrastructure is most critical and why?

4.0Self-Assessment Exercises

1. Define cyber security and what are the benefits of cyber security

Answer

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centres and other computerized systems

Benefits of cybersecurity

The benefits of implementing and maintaining cybersecurity practices include

- Business protection against cyberattacks and data breaches.
- Protection for data and networks.
- Prevention of unauthorized user access.
- Improved recovery time after a breach.
- Protection for end users and endpoint devices.
- Regulatory Compliance

- Business continuity

5.0 Conclusion

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats, Cyber security is also one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend critical organization infrastructure

6.0 Summary

In this unit, we have been able to define Cybersecurity, identify the benefits of cyber security, explain the concept of cyber security and explain cyber security counter measures

7.0 References/Further Reading

Andrew S., T., & David J., W. (2011). *COMPUTER NETWORKS* (M. Horton, H. Michael, D. Tracy, & H. Melinda (eds.); fifth). Pearson Education.

Joseph, M. K. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (fourth, Vol. 7, Issue 2). McFarland & Company, Inc. https://doi.org/10.1353/pla.2007.0017

Pande, J. (2017). *Introduction to Cyber Security (FCS)*. http://uou.ac.in

Stewart, J. M., Tittel, E., & Chapple, M. (2011). *CISSP: Certified Information Systems Security Professional Study Guide*. Wiley.

UNIT 2: CYBER CRIMES CLASSIFICATION AND TYPES OF CYBER CRIMES

CONTENTS

1.0 Introduction

Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services. The world of Cyber Security revolves around the industry standard of confidentiality, integrity, and availability, or CIA. Privacy means data can be accessed only by authorized parties; integrity means information can be added, altered, or removed only by authorized users; and availability means systems, functions, and data must be available on-demand according to agreed-upon parameters. The main element of Cyber Security is the use of authentication mechanisms. For example, a user name identifies an account that a user wants to access, while a password is a mechanism that proves the user is who he claims to be.

2.0 Intended Learning Outcomes (ILOs)

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

- define Cyber Security
- classify Cyber crimes
- describe the types of cyber crime.

3.0 Main Content

3.1 Classification of Cyber Crimes

The cyber-criminal could be internal or external to the organization facing the cyber attack. Based on this fact, the cyber crime could be categorized into two types:

3.1.1 Insider Attack

An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparatively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and wellness of the security system. Moreover, the attacker have an access to the network. Therefore, it is comparatively easy for an insider attacker to steel sensitive information, crash the network, etc. In most of the cases, the reason for insider attack is when an employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a vulnerability window for the attacker. The insider attack could be prevented by planning and installing an Internal intrusion detection system (IDS) in the organization

3.1.2 External Attack

When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information. An experienced network/security administrator keeps regular eye on the log generated by the firewalls as external attacks can be traced out by carefully analyzing these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

The cyber attacks can also be classified as structure attacks and unstructured attacks based on the level of maturity of the attacker.

3.1.3 Unstructured attacks

These attacks are generally performed by amateurs who do not have any predefined motive to perform the cyber attack. Usually, these amateurs try to test a tool readily available over the internet on the network of a random company

3.1.4 Structure Attack

These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind. They have access to sophisticated tools and technologies to gain access to other networks without being noticed by their Intrusion Detection Systems(IDSs). Moreover, these attacker have the necessary expertise to develop or modify the existing tools to satisfy their purpose. These types of attacks are usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

3.2 Types of Cyber Crimes

Cybercrime is any unauthorized activity involving a computer, device, or network. The three types are computer-assisted crimes, crimes where the computer itself is a target, and crimes where the computer is incidental to the crime rather than directly related to it. Cybercriminals usually try to profit off of their crimes using a variety of tactics, including:

3.2.1 Denial of Service, or DOS

These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.

3.2.2 Botnets

Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

3.2.3 Identity Theft

This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. They may do this by finding out user's passwords

through hacking, retrieving personal information from social media, or sending phishing emails.

3.2.3 Cyberstalking

This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically, cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.

3.2.4 Social Engineering

Social engineering involves criminals making direct contact with you usually by phone or email. They want to gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed. This is typically a password, the company you work for, or bank information. Cybercriminals will find out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name.

3.2.5 PUPs

PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download.

3.2.6 Phishing

This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access.

3.2.7 Prohibited/Illegal Content

This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity.

Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

3.2.8 Online Scams

These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

3.2.9 Exploit Kits

Exploit kits need a vulnerability (bug in the code of a software) in order to gain control of a user's computer. They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

Discussion

Why is the knowledge of cyber Security critical in securing organisational data?

4.0 Self-Assessment Exercise

1. Define Cyber Security

   Answer

   Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

2. List and explain different classification of cyber crimes

Answer

i. Insider Attack - An attack to the network or the computer system by some person with authorized system access is known as insider attack

ii. External attack - When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack

iii. Unstructured attacks - These attacks are generally performed by amateurs who don't have any predefined motives to perform the cyber attack

iv. Structure attack - These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind

5.0 Conclusion

Most attackers use proxies to hide their IP address and, therefore, their true physical location. In this way, attackers can conduct fraudulent financial transactions, launch attacks, or perform other actions with little risk. While law enforcement can visit a physical location identified by an IP address, attackers that use one (or multiple) proxies across country boundaries are more difficult to locate

6.0 Summary

By altering the host's file or browser configuration to use the proxy, the attacker redirects requests and captures confidential information. Some banking Trojans give attackers the ability to proxy requests through the victim's browser because conducting fraud from a legitimate user's IP address is less suspicious.

7.0 References/Further Reading

Andrew S., T., & David J., W. (2011). *COMPUTER NETWORKS* (M. Horton, H. Michael, D. Tracy, & H. Melinda (eds.); fifth). Pearson Education.

Joseph, M. K. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (fourth, Vol. 7, Issue 2). McFarland & Company, Inc. https://doi.org/10.1353/pla.2007.0017

Pande, J. (2017). *Introduction to Cyber Security (FCS)*. http://uou.ac.in

Stewart, J. M., Tittel, E., & Chapple, M. (2011). *CISSP: Certified Information Systems Security Professional Study Guide*. Wiley.

UNIT 3 SCOPE OF CYBERCRIMES

CONTENTS

1.0 Introduction

Cyber security has always been an important aspect of computing systems but its importance has increased greatly in recent years. The curriculum covers areas where cyber security is of major importance, but have different security requirements and may be exposed to different threats and attacks. It also covers techniques and mechanisms used to secure computer systems and data to meet those requirements and protect them. The areas looked at include computer operating systems (and increasingly, distributed operating systems), distributed applications (such as electronic commerce over the Internet), embedded systems (ranging from smart cards to large industrial plant and telecommunications systems), and users. The techniques and mechanisms looked at include cryptography, authentication &authorisation, and access control. Furthermore, the curriculum integrates the legal, ethical, and professional perspectives, for instance, to address concerns about data security, privacy, and societal impact of computing systems.

2.0 Intended Learning Outcomes (ILOs)

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

- explain the concept of cyber crime
- understand who is a hacker
- demonstrate cyber crime motivation.

3.0 Main Content

3.1 Nature and Scope of Cyber crime

Cyber crime is Transnational in nature. These crimes are committed without being physically present at the crime location. These crimes are committed in the im-palpable world of computer networks. To commit such crimes the only thing a person needs is a computer which is connected with the internet. With the advent of lightening fast internet, the time needed for

committing the cybercrime is decreasing. The cyberspace, being a boundary-less world has become a playground of the perpetrators where they commit crimes and remain conspicuously absent from the site of crime. It is an Open challenge to the law which derives its lifeblood from physical proofs and evidence. The cybercrime has spread to such proportion that a formal categorization of this crime is no more possible. Every single day gives birth to a new kind of cybercrime making every single effort to stop it almost a futile exercise. Identification possess major challenge for cybercrime. One thing which is common it comes to identification part in cybercrime is Anonymous identity. It is quite an easy task to create false identity and commit crime over internet using that identity. Cybercrime being technology driven evolves continuously and ingeniously making it difficult for cyber investigators in finding solution related to cyber law crimes. Crimes committed over internet are very different in nature when compared to the physical world. In crimes relating to cyber space there is nothing sort of physical foot prints, tangible traces or objects to track cyber criminals down. Cybercrimes possess huge amount complications when it comes to investigation.

3.2 Scope of Cybercrimes

Cybercrime can be basically categorized into three parts:

- Cybercrimes against persons
- Cybercrimes against property
- Cybercrimes against government.

3.2.1 Cybercrimes against persons

Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified.

3.2.2 Cybercrimes against property

The second category of Cyber-crimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes.

3.2.3 Cybercrimes against government

The third category of Cyber-crimes relate to Cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

- **Malware**
  Where victims are hit with a worm or virus that renders their devices useless

- **Man in the Middle**
  Where a hacker puts himself between a victim's machine and a router to sniff data packets

- **Phishing**
  Where a hacker sends a seemingly legitimate-looking email asking users to disclose personal information

Other types of cyberattacks include cross-site scripting attacks, password attacks, eavesdropping attacks (which can also be physical), SQL-injection attacks, and birthday attacks based on algorithm functions.

3.3 Cyber Criminals Motivation

The main motive behind the cybercrime is to disrupt regular business activity and critical infrastructure. Cybercriminals also commonly manipulate stolen data to benefit financially, cause financial loss, damage a reputation, achieve military objectives, and propagate religious or political beliefs. Some do not even need a motive and might hack for fun or simply to

showcase their skills. So, who are these cybercriminals? Here is a breakdown of the most common types:

3.3.1 Black-Hat Hackers

A black hat hacker is typically one that engages in cybercrime operations and uses hacking for financial gain, cyber espionage purposes or other malicious motives, like implanting malware into computer systems. Gray-Hat Hackers.

3.3.2 White-Hat Hackers

A white hat hacker, also called an ethical hacker, is the antithesis of a black hat hacker. White hat hackers are not cybercriminals, rather they are security specialists hired by organizations to conduct tasks such as penetration tests and vulnerability assessments on their systems to improve their security defenses. When working as pen testers, white hat hackers conduct tests and attacks on networks, websites and software in order to identify possible vulnerabilities. They also follow established rules, such as bug bounty policies. They will notify the affected organizations directly of any issues so that a patch can be released or other steps taken to fix the flaw.

3.3.3 Suicide Hackers

Suicide hackers are individuals who aim to bring down critical infrastructure for a “cause” and are not worried about facing jail terms or any other kind of punishment. They are similar to suicide bombers, who sacrifice their life for an attack and are thus not concerned with the consequences of their actions.

3.3.4 Script Kiddies

A derogatory term often used by amateur hackers who do not care much about the coding skills. These hackers usually download tools or use available hacking codes written by other developers and hackers. Their primary purpose is usually to impress their friends or gain attention. However, they do not care about learning. By using off-the-shelf codes and tools, these hackers may launch some attacks without bothering for the quality of the attack. Commonest cyber-attacks by script kiddies might include DoS and DDoS attacks.

3.3.5 Gray Hats Hackers

Gray hat hackers fall somewhere in between white hat and black hat hackers. While they will not use their skills for personal gain, they can, however, have both good and bad intentions. As an example, a hacker who hacks into a corporation and finds some vulnerability may leak it over the web or inform the organization about it. It all depends upon the hacker. Nevertheless, as soon as hackers use their hacking skills for personal gain they become black hat hackers. there's a fine line between these two.

3.3.6 Blue Hats Hackers

These are another form of novice hackers very similar to script kiddies whose main agenda is to require revenge on anyone who makes them angry. They need no desire for learning and should use simple cyber attacks like flooding your IP with overloaded packets which can result in **DoS attacks**. A script kiddie with a vengeful agenda are often considered a blue hat hacker.

3.3.7 Malicious Insider or Whistle blower

A malicious insider or a whistle blower could also be an employee with a grudge or a strategic employee compromised or hired by rivals to garner trade secrets of their opponents to remain on top of their game. These hackers may take privilege from their quick access to information and their role within the corporate to hack the system.

3.3.8 State/Nation Sponsored Hackers

State or Nation sponsored hackers are those that have been employed by their state or nation's government to snoop in and penetrate through full security to realize tip from other governments to stay at the highest online. they have an endless budget and extremely advanced tools at their disposal to target individuals, companies or rival nations.

3.3.9 Hacktivist Hackers

Hacktivist is when hackers break into government or corporate computer systems as an act of protest. Hacktivists use hacking to increase awareness of their social or political agendas, as well as themselves, in both the online and offline arenas. They are individuals who promote a political agenda by hacking, especially by defacing or disabling websites. Common hacktivist targets include government agencies, multinational corporations, or any other entity that they perceive as a threat. It remains a fact, however, that gaining unauthorized access is a crime, irrespective of their intentions.

Discussion

How can cybercrime be mitigated? Discuss.

4.0 Self-Assessment/Exercise

1. It has been expressed those cyber-attacks involving data breach are more dangerous than that of monetary. Why?

2. Why do we need a White hacker in cyber society?

5.0 Conclusion

While click fraud appears to be a problem with a scope limited to just advertisers and ad networks, fraudsters' use of infected computers to click ad links makes click fraud a problem for everyone with a computer. Being part of a click fraud botnet consumes a system's bandwidth and displays additional advertisements to the user, which is usually undesirable.

6.0 Summary

Systems connected to the Internet are at risk of infection from exposure to social-engineering attacks or vulnerability exploitation. Regardless of the infection vector, compromised machines can wait for commands from the attacker, which turns the system into a bot.

7.0 References/Further Reading

Andrew S., T., & David J., W. (2011). *COMPUTER NETWORKS* (M. Horton, H. Michael, D. Tracy, & H. Melinda (eds.); fifth). Pearson Education.

Joseph, M. K. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (fourth, Vol. 7, Issue 2). McFarland & Company, Inc. https://doi.org/10.1353/pla.2007.0017.

Pande, J. (2017). *Introduction to Cyber Security (FCS)*. http://uou.ac.in

Stewart, J. M., Tittel, E., & Chapple, M. (2011). *CISSP: Certified Information Systems Security Professional Study Guide*. Wiley.

Module 2: Cyber Threat Management

Introduction of Module

In network security, threat prevention refers to policies and tools that protect your corporate network.

In the past, threat prevention primarily focused on the perimeter. With an increasing array of threats such as malware and ransomware arriving via email spam and phishing attacks, advanced threat prevention requires an integrated, multilayered approach to security. This may include tools for intrusion threat detection and prevention, advanced malware protection, and additional endpoint security threat prevention.

This module will consist of four units are follows

Unit 1: Firewalls

Unit 2: Virtual Private Networks (VPN)

Unit 3: Security Control Management

Unit 4: Hardware and Software Prevention

UNIT 1 – FIREWALL

CONTENTS

1.0 Introduction

A firewall forms a barrier through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction. Firewall may be designed to operate as a filter at the level of IP packets, or may operate at a higher protocol layer.

2.0 Intended Learning Outcomes (ILOs)

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

- demonstrate the concept of firewall
- explore the importance of firewalls.

3.0 Main Content

3.1 What is Firewall

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. Firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out. Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.

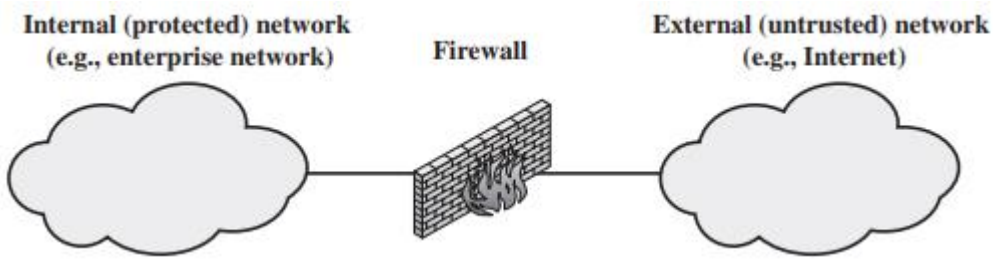

Figure 2.1: Firewall gateway

3.1.1 Characteristics of firewalls

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this chapter.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this chapter.
3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall and often required in government applications.

3.1.2 Needs for Firewall

Information systems in corporations, government agencies, and other organizations have undergone a steady evolution. The following are notable developments:

- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals.
- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe.
- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two.
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN).
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN.

3.1.3 Limitation of Firewall

1. The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
2. The firewall may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.

3. An improperly secured wireless LAN may be accessed from outside the organization. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall.
4. A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally.

3.2 Types of Firewalls

A firewall may act as a packet filter. It can operate as a positive filter, allowing to pass only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria. Depending on the type of firewall, it may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. In this section, we look at the principal types of firewalls.

Packet Filtering

Firewall A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The firewall is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

- **Source IP address**: The IP address of the system that originated the IP packet (e.g., 192.178.1.1)
- **Destination IP address**: The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)
- **Source and destination transport-level address**: The transport-level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET
- **IP protocol field**: Defines the transport protocol
- **Interface**: For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for

The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken. Two default policies are possible:

- **Default = discard**: That which is not expressly permitted is prohibited.
- **Default = forward**: That which is not expressly prohibited is permitted.

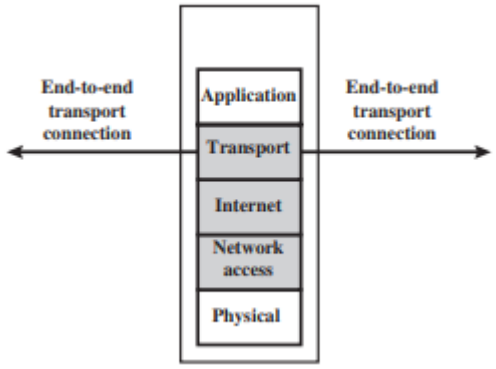

Figure 2.2: Packet filter mechanism

Stateful Inspection Firewalls

A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context.

- A simple packet filtering firewall must permit inbound network traffic on all these high-numbered ports for TCP-based traffic to occur. This creates a vulnerability that can be exploited by unauthorized users.
- A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections. There is an entry for each currently established connection. The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.
- A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections. Some stateful firewalls also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking. Some even inspect limited amounts of application data for some well-known protocols like FTP, IM and SIPS commands, in order to identify and track related connections.

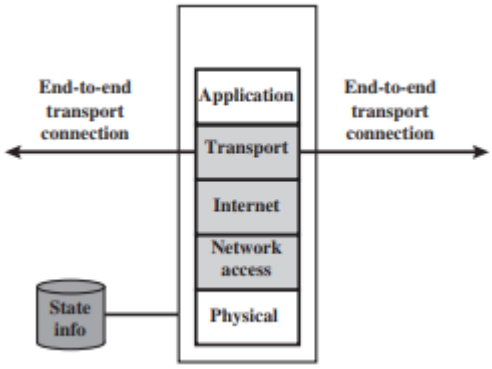

Figure 2.3: Stateful packet inspection

Application-Level Gateway

An application-level gateway, also called an application proxy, acts as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features. Application-level gateways tend to be more secure than packet filters. Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only scrutinize a few allowable applications. In addition, it is easy to log and audit all incoming traffic at the application level. A prime disadvantage of this type of gateway is the additional processing overhead on each connection. In effect, there are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examine and forward all traffic in both directions.

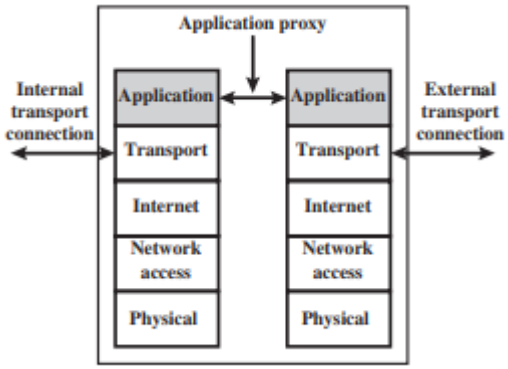

Figure 2.4: Application proxy firewall

Circuit-Level Gateway

A fourth type of firewall is the circuit-level gateway or circuit-level proxy. This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections. In this configuration, the gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.

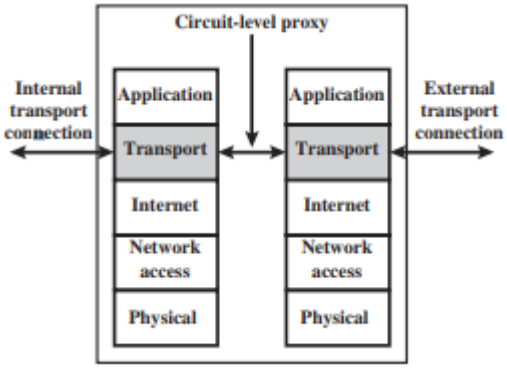

Figure 2.5: Circuit-level proxy

3.3 How firewalls work

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down

3.4 Cases/Example

An example of a personal firewall is the capability built in to the Mac OS X operating system. When the user enables the personal firewall in Mac OS X, all inbound connections are denied except for those the user explicitly permits. Figure 2.6 shows this simple interface. The list of inbound services that can be selectively reenabled, with their port numbers, includes the following:

- Personal file sharing (548, 427)
- Windows sharing (139)
- Personal Web sharing (80, 427)
- Remote login - SSH (22)
- FTP access (20-21, 1024-64535 from 20-21)
- Remote Apple events (3031)
- Printer sharing (631, 515)
- IChat Rendezvous (5297, 5298)
- ITunes Music Sharing (3869)
- CVS (2401)

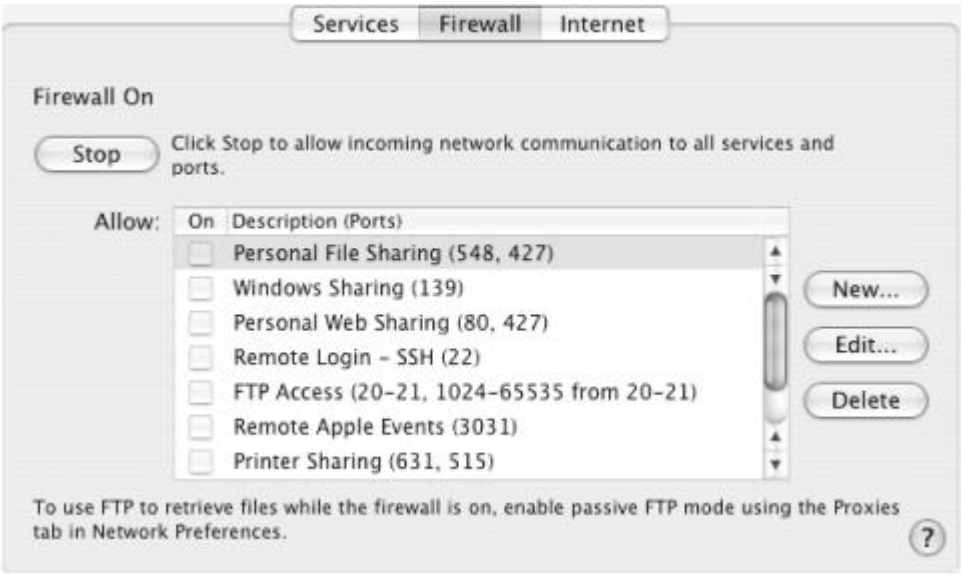

Figure 2.6: Example of Personal firewall interface on MAC

When FTP access is enabled, ports 20 and 21 on the local machine are opened for FTP; if others connect to this computer from ports 20 or 21, the ports 1024 through 64535 are open. For increased protection, advanced firewall features are available through easy-to-configure checkboxes. Stealth mode hides the Mac on the Internet by dropping unsolicited communication packets, making it appear as though no Mac is present. UDP packets can be

blocked, restricting network traffic to TCP packets only for open ports. The firewall also supports logging, an important tool for checking on unwanted activity

Discussion

What is the difference of firewalls at Application security and internet security?

4.0 Self-Assessment/Exercises

1. What is Personal Firewall

Answer

A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side. Personal firewall functionality can be used in the home environment and on corporate intranets. Typically, the personal firewall is a software module on the personal computer. In a home environment with multiple computers connected to the Internet, firewall functionality can also be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface.

1. **What are the benefits of host-based firewall?**

Answer

A host-based firewall is a software module used to secure an individual host. Such modules are available in many operating systems or can be provided as an add-on package. Like conventional stand-alone firewalls, host-resident firewalls filter and restrict the flow of packets. A common location for such firewalls is a server.

There are several benefits to the use of a server-based or workstation based firewall:

- Filtering rules can be tailored to the host environment. Specific corporate security policies for servers can be implemented, with different filters for servers used for different application.
- Protection is provided independent of topology. Thus both internal and external attacks must pass through the firewall.
- Used in conjunction with stand-alone firewalls, the host-based firewall provides an additional layer of protection.

A new type of server can be added to the network, with its own firewall, without the necessity of altering the network firewall configuration.

5.0 Conclusion

Internet connectivity is no longer optional for organizations. The information and services available are essential to the organization. Moreover, individual users within the organization want and need Internet access, and if this is not provided via their LAN, they will use dial-up capability from their PC to an Internet service provider (ISP). However, while Internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates a threat to the organization.

6.0 Summary

Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.

7.0 References/Further Reading

Andrew S., T., & David J., W. (2011). *COMPUTER NETWORKS* (M. Horton, H. Michael, D. Tracy, & H. Melinda (eds.); fifth). Pearson Education.

Joseph, M. K. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (fourth, Vol. 7, Issue 2). McFarland & Company, Inc. https://doi.org/10.1353/pla.2007.0017

Pande, J. (2017). *Introduction to Cyber Security (FCS)*. http://uou.ac.in

Stewart, J. M., Tittel, E., & Chapple, M. (2011). *CISSP: Certified Information Systems Security Professional Study Guide*. Wiley.

UNIT 2 VIRTUAL PRIVATE NETWORKS

CONTENTS

1.0 Introduction

The large number of terms used to categorize and describe the functionality of VPNs has led to a great deal of confusion about what exactly VPNs are and what they can do. The unit covers VPN devices, protocols, technologies, as well as VPN categories and models.

2.0 Intended Learning Outcomes (ILOs)

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

- explain the concepts of VPNs
- set up a simple VPN.

3.0 Main Content

3.1 What is Virtual Private Network?

VPN meaning that it is a private point-to-point connection between two machines or networks over a shared or public network such as the internet. A Virtual Private Network is a combination of software and hardware. VPN (Virtual Private Network) technology, can be use in organization to extend its safe encrypted connection over less secure internet to connect remote users, branch offices, and partner private, internal network. VPN turn the Internet into a simulated private WAN.

It uses “virtual” connections routed through the internet from a business’s private network to the remote site. A Virtual Private Network is a technology which creates a network, and that network is virtually private.

The letter V in VPN stands for “virtual” means that it shares physical circuits with other traffic and it has no corresponding physical network. A VPN client uses TCP/IP protocol, that is called tunneling protocols, to make a virtual call to VPN server.

3.1.1 Uses of Virtual Private Networks

VPNs are a fairly simple tool, but they can be used to do a wide variety of things:

- Access a Business Network While Traveling
- Access Your Home Network While Travelling
- Hide Your Browsing Activity From Your Local Network and ISP
- Access Geo-Blocked Websites
- Bypass Internet Censorship
- Downloading Files

3.1.2 Advantages of VPNs

The benefits of VPN are as follows:

- Security: The VPN should protect data while it's travelling on the public network. If intruders attempt to capture data, they should be unable to read or use it.
- Reliability: Employees and remote offices should be able to connect to VPN. The virtual network should provide the same quality of connection for each user even when it is handling the maximum number of simultaneous connections.
- Cost Savings: Its operational cost is less as it transfers the support burden to the service providers.
- It reduces the long-distance telephone charges.
- It cut technical support.
- It eliminates the need for expensive private or leased lines.
- Its management is straightforward.
- Scalability: growth is the flexible, i.e., we can easily add new locations to the VPN.
- It is efficient with broadband technology.
- By using VPN, the equipment cost is also reduced

3.1.3 Disadvantages of VPNs

The difficulties of VPN are as follows:

- For VPN network to establish, we require an in-depth understanding of the public network security issues.
- VPNs need to accommodate complicated protocols other than IP.
- There is a shortage of standardization. The product from different vendors may or may not work well together.
- The reliability and performance of an Internet-based private network depend on uncontrollable external factors, which is not under an organization's direct control.

3.2 Types of Virtual Private Network

VPN is of three kinds:

Remote access VPN (Virtual Private Network)

The VPN which allows individual users to establish secure connections with a remote computer network is known as remote-access VPN. There is a requirement of two components in a remote-access VPN which are as follows:

i. Network Access Server (NAS)
ii. Client software.

It enables the remote connectivity using any internet access technology. Here, the remote user launches the VPN client to create a VPN tunnel.

Intranet VPN (Virtual Private Network)

If a company has one or more remote locations and the company wants to join those locations into a single private network, then that company can create an intranet VPN so that they can connect LAN of one site to another one. Intranet VPN can link corporate headquarters, remote offices and branch offices over a shared infrastructure using dedicated connections. If we use intranet VPN, then it reduces the WAN bandwidth costs. The user can also connect new sites easily by using this network.

Extranet VPN (Virtual Private Network)

If a company has the close relationship with the other company (that company can be their customer, supplier, branch and another partner company), then those companies can build an extranet VPN so that they can connect LAN of one company to the other. It allows all of the companies to work in a shared environment.

3.3 VPN Technologies and Protocols

There are three network protocols used within VPN tunnels. These are:

Internet Protocol Security (IPSec)

We can make use of this protocol for encryption. It is used as a protocol suite. It is used as a "protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each packet of IP of a data stream." It requires expensive, time-consuming client installations, which is its most significant disadvantage.

Point-to-Point Tunneling Protocol (PPTP)

Generally, it is the most widely used VPN protocol among windows users. It was created by Microsoft in association with the other technology companies. The most significant disadvantage of PPTP is that it does not provide encryption. It relies on PPP (Point-to-Point Protocol). It is implemented for the security measures. It is also available for Linux and Mac users. As compared to other methods, PPTP is faster.

Layer 2 Tunneling Protocol (L2TP)

It is another tunnelling protocol which supports VPN. L2TP is created by Microsoft and Cisco as a combination between PPTP and L2F (Layer 2 Forwarding). L2TP also does not provide encryption as like as PPTP. The main difference between both of them is that L2TP delivers data confidentiality and data integrity.

Secure Socket Layer (SSL)

It is a VPN accessible via https over a web browser. Its most significant advantage is that it does not need any software installed because it uses the web browser as the client application. With the help of SSL VPN, the user's access can be restricted to specific claims instead of allowing access to the whole network.

3.4 How VPN works and Set Up

3.4.1 Working of VPN

When you connect your computer (or another device, such as a smartphone or tablet) to a VPN, the computer acts as if it's on the same local network as the VPN. All your network traffic is sent over a secure connection to the VPN. Because your computer behaves as if it's on the network, this allows you to securely access local network resources even when you're on the other side of the world. You'll also be able to use the Internet as if you were present at the VPN's location, which has some benefits if you're using pubic Wi-Fi or want to access geo-blocked websites. When you browse the web while connected to a VPN, your computer contacts the website through the encrypted VPN connection. The VPN forwards the request for you and forwards the response from the website back through the secure connection.

If you're using a USA-based VPN to access Netflix, Netflix will see your connection as coming from within the USA.

3.4.2 How to Setup a VPN

There are following two ways to create a VPN connection:

By dialing an Internet service provider (ISP)

If you dial-in to an ISP, your ISP then makes another call to the private network's remote access server to establish the PPTP or L2TP tunnel After authentication, you can access the private network.

By connecting directly to the Internet

If you are already connected to an Internet, on a local area network, a cable modem, or a digital subscriber line (DSL), you can make a tunnel through the Internet and connects directly to the remote access server. After authentication, you can access the corporate network.

3.5 Cases/Example

Suppose there is a company which has two locations, one in Noida and other in Pune. For both places to communicate efficiently, the company has the choice to set up private lines between the two locations. Although private lines would restrict public access and extend

the use of their bandwidth, it will cost the company a great deal of money since they would have to purchase the communication lines per mile. So, the more viable option is to implement a VPN. The company can hook their communication lines with a local ISP in both cities. Thus, the ISP would act as a middleman, connecting the two locations. This would create an affordable small area network for the company.

Discussion

How are Privacy, security and Encryption ensured using VPN

4.0 Self-Assessment/Exercises

What are the equipment used for VPN implementation?

Answer

Equipment having the VPN function includes routers and firewalls. Basically, communication is made via VPN equipment. Information is encrypted by the transmission VPN equipment before transmission and decoded by the receiving VPN equipment after receipt of information. The key for encrypt the data is set in VPN equipment in advance. The VPN equipment at receiving side decodes encrypted data before sending it to the receiving computer.

What are key Features of a Typical VPN solution

When the remote offices connect each other to share vital resources and secret information, the VPN solution must ensure the privacy and integrity of the data as it traverses the Internet. Therefore, a VPN solution must provide at least all of the following:

Keep data confidential (**encryption**)

- Data carried on the public network must be rendered unreadable to unauthorized clients on the network.

Ensure the identities of two parties communicating (**authentication**)

The solution must verify the user's identity and restrict VPN access to authorized users only. It must also provide audit and accounting records to show who accessed what information and when.

• Safeguard the identities of communicating parties (tunneling)

• Guard against packets being sent over and over (replay prevention)

• Ensure data is accurate and in its original form (non-repudiation)

Address Management. The solution must assign a client's address on the private net and ensure that private addresses are kept private.

Key Management. The solution must generate and refresh encryption keys for the client and the server.

Multiprotocol Support. The solution must handle common protocols used in the public network. These include IP, Internet Packet Exchange (IPX), and so on.

An Internet VPN solution based on the Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP) meets all of these basic requirements and takes advantage of the broad availability of the Internet. Other solutions, including the new IP Security Protocol (IPSec), meet only some of these requirements, but remain useful for specific situations.

5.0 Conclusion

Virtual private network extends a private network across public networks. VPN allows users working at home or office to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public inter-network (such as the Internet). From the user's perspective, the VPN is a **point-to-point connection** between the user's computer and a corporate server. The nature of the intermediate inter-network is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

6.0 Summary

A virtual private network (VPN) allows the provisioning of private network services for an organization or organizations over a public or shared infrastructure such as the Internet or service provider backbone network. The shared service provider backbone network is known as the VPN backbone and is used to transport traffic for multiple VPNs, as well as possibly non-VPN traffic.

7.0 References/Further Reading

Andrew S., T., & David J., W. (2011). *COMPUTER NETWORKS* (M. Horton, H. Michael, D. Tracy, & H. Melinda (eds.); fifth). Pearson Education.

Joseph, M. K. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (fourth, Vol. 7, Issue 2). McFarland & Company, Inc. https://doi.org/10.1353/pla.2007.0017.

Pande, J. (2017). *Introduction to Cyber Security (FCS)*. http://uou.ac.in

Stewart, J. M., Tittel, E., & Chapple, M. (2011). *CISSP: Certified Information Systems Security Professional Study Guide*. Wiley.

NetworkChatter (April, 2020). *ENSA Module 8 – Virtual Private Networks (VPN) Lecture Notes.* http://www.networkchatter.com/ensa-module-8-virtual-private-networks-vpn-lecture-notes/ last accessed: 30, December, 2021.

Dinesh Thakur. *What is VPN (Virtual Private Network)? Definition.* https://ecomputernotes.com/computernetworkingnotes/security/virtual-private-network#Types_of_VPN_(Virtual_Private_Network). Last accessed: 28 December, 2021.

UNIT 3 SECURITY CONTROL MANAGEMENT

CONTENTS

1.0 Introduction

As long as you are carrying an access card or ID badge, it means that your office uses an access system. How does it really work? It's difficult since most people have never seen an access system. Most people believe it is just a card reader on the wall. Of course there is a little bit more to it in reality. It's not very difficult though, there are just a few parts behind the scenes that make the magic of easily unlocking a door every time.

This unit will give you a full and comprehensive understanding how access control systems, how it work, control list and AAA framework.

2.0 Intended Learning Outcomes (ILOs)

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

- explain the concept access control
- manage access control.

3.0 Main Content

3.1 Access Control

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings, as well as alarms and lockdown capabilities, to prevent unauthorized access or operations.

Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication (MFA), which requires two or more authentication factors, is often an important part of a layered defense to protect access control systems.

3.1.1 Why is access control important?

The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information (PII) and intellectual property.

Access control systems are complex and can be challenging to manage in dynamic IT environments that involve on-premises systems and cloud services. After some high-profile breaches, technology vendors have shifted away from single sign-on (SSO) systems to unified access management, which offers access controls for on-premises and cloud environments.

3.1.2 How access control works

These security controls work by identifying an individual or entity, verifying that the person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or Internet Protocol (IP) address. Directory services and protocols, including Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML), provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers.

Organizations use different access control models depending on their compliance requirements and the security levels of information technology (IT) they are trying to protect.

3.2 Types of Access control

Access control can be split into two groups designed to improve physical security or cybersecurity:

- **Physical access control**: limits access to campuses, building and other physical assets, e.g., a proximity card to unlock a door.
- **Logical access control**: limits access to computers, networks, files and other sensitive data, e.g., a username and password.

Access control Models

The main models of access control are:

•**Attribute-based Access Control (ABAC):** In this model, access is granted or declined by evaluating a set of rules, policies, and relationships using the attributes of users, systems and environmental conditions.

•**Discretionary Access Control (DAC)**: In DAC, the owner of data determines who can access specific resources.

•**History-Based Access Control (HBAC)**: Access is granted or declined by evaluating the history of activities of the inquiring party that includes behavior, the time between requests and content of requests.

• **Identity-Based Access Control (IBAC)**: By using this model network administrators can more effectively manage activity and access based on individual requirements.

•**Mandatory Access Control (MAC)**: A control model in which access rights are regulated by a central authority based on multiple levels of security. Security Enhanced Linux is implemented using MAC on the Linux operating system.

•**Organization-Based Access control (OrBAC)**: This model allows the policy designer to define a security policy independently of the implementation.

•**Role-Based Access Control (RBAC)**: RBAC allows access based on the job title. RBAC eliminates discretion on a large scale when providing access to objects. For example, there should not be permissions for human resources specialist to create network accounts.

•**Rule-Based Access Control (RAC)**: RAC method is largely context based. Example of this would be only allowing students to use the labs during a certain time of day.

3.3 Access control Lists

Another way of simplifying access rights management is to store the access control matrix a column at a time, along with the resource to which the column refers. This is called an access control list, or ACL. ACLs have a number of advantages and disadvantages as a means of managing security state. These can be divided into general properties of ACLs and specific properties of particular implementations. ACLs are widely used in environments where users manage their own file security, such as the Unix systems common in universities and science labs. Where access control policy is set centrally, they are suited to environments where protection is data oriented; they are less suited where the user population is large and constantly changing, or where users want to be able to delegate their authority to run a particular program to another user for some set period of time. ACLs are simple to implement, but are not efficient as a means of doing security checking at runtime, as the typical operating system knows which user is running a particular program, rather than which files it has been authorized to access since it was invoked. The operating system must either check the ACL at each file access or keep track of the active access rights in some other way.

Finally, distributing the access rules into ACLs can make it tedious to find all the files to which a user has access. Revoking the access of an employee who has just been fired, for example, will usually have to be done by cancelling their password or other authentication mechanism. It may also be tedious to run systemwide checks, such as verifying that no files have been left world-writable. This could involve checking ACLs on millions of user files.

3.3.1 Access control Groups

Access control groups (ACGs) are groupings of access privileges for objects (catalogs, hierarchies, collaboration areas, and import jobs) that are treated at the same level in the Collaboration Server system. ACG is defined on a group of objects to which you can assign a level of access based on a role. For example, an ACG can be defined on one catalog, one hierarchy, and two collaboration areas. You can assign and edit

privileges to this group of objects to users in Role A and view privileges to users in Role B.

3.3.2 Access control roles

Access control roles (ACRs) are set of privileges that are defines following organization defined policies. These roles assigned to different users based on their access rights according to their job role in the organization.

Some people use the words group and role interchangeably, and with many systems they are; but the more careful definition is that a group is a list of principals, while a role is a fixed set of access permissions that one or more principals may assume for a period of time using some defined procedure.

3.4 AAA Framework

AAA is a standard-based framework used to control who is permitted to use network resources (through **Authentication**), what they are authorized to do (through **Authorization**), and capture the actions performed while accessing the network (through **Accounting**).

The administrator can take access to a router or a device through a console but it is very inconvenient if he is sitting far from the place of that device. So, eventually, he has to take remote access to that device.

But as remote access will be available by using an IP address, therefore, it is possible that an unauthorized user can take access using that same IP address therefore for security measures, we have to put authentication. Also, the packets exchanged between the device should be encrypted so that any other person should not be able to capture that sensitive information. Therefore, a framework called **A**uthentication, **A**uthorization and **A**ccounting shorthand **AAA** is used to provide that extra level of security.

3.4.1 Authentication

The process by which it can be identified that the user, which wants to access the network resources, valid or not by asking some credentials such as username and password.

As network administrators, we can control how a user is authenticated if someone wants to access the network.

3.4.2 Authorization

It provides capabilities to enforce policies on network resources after the user has gained access to the network resources through authentication. After the authentication is successful, authorization can be used to determine what resources is the user allowed to access and the operations that can be performed.

3.4.3 Accounting

It provides means of monitoring and capturing the events done by the user while accessing the network resources. It even monitors how long the user has access to the network. The administrator can create an accounting method list to specify what should be accounted for and to whom the accounting records should be sent.

3.4 Cases/Example

An administrator can take access to a router or a device through a console but it is very inconvenient if he is sitting far from the place of that device. So, eventually, he has to take remote access to that device. But as remote access will be available by using an IP address, therefore, it is possible that an unauthorized user can take access using that same IP address therefore for security measures, we have to put authentication. Also, the packets exchanged between the device should be encrypted so that any other person should not be able to capture that sensitive information.

 **Discussion**

Discuss all possible policies attached to accessing resources in your school

4.0 Self-Assessment/Exercises

1. Who is system administrator?

Answer

The SysAdmin, or Systems Administrator, is the person responsible for configuring and managing a company's entire infrastructure, including all of the hardware, software, and operating systems that are necessary to support the running of the business.

The sysadmin is responsible for Configuring and managing company infrastructure, managing user access and permissions to all systems and data, perform daily security backups and restored, manage all monitoring and alerting throughout company applications and infrastructure; solve and troubleshoot problems.

2. What happens to organizations that does not have access control implementation?

Answer

Everyone in the organization, no matter what their title, would have access to all the company's information on all of their systems and applications. Employees would be able to make changes to secure data, such as the payroll and customer information. The scary part is that many organizations often have minimal access management structures in place or they believe they are managing their access rights correctly, when they may actually not be. Without proper access management, security risks are high, and it is easy lose track of who has access to what, easily leading to a security breach.

5.0 Conclusion

It is important also for an enterprise to develop the security system that secure the information system against external threats. Very important stage of data protection building in information system is the creation of high level model, independent from the software, satisfying the needs of protection and security of a system. Security policies of information systems determine that it is necessary to define for each user a set of operations that it could be perform. Due to it the set of permissions should be defined for each system's user. It suffices to determine the permissions for execution of particular methods on each object accessible for that user. It is existing the need to create the tool, designated mainly for security administrator who could manage one of the security aspects of information systems, namely the control of users' access to data stored in a system.

6.0 Summary

One of the basic concepts of protection models is access control. The purpose of access control to data in information system is a limitation of actions or operations that the system's users can execute. The access control based on role concept represents interesting alternative in relation to traditional systems of DAC (Discretionary Access Control) type or MAC (Mandatory Access Control) type. RBAC (Role-Based Access Control) model based on a role concept defines the user's access to information basing on activities that the user can perform in a system.

7.0 References/Further Reading

Are3na (2021, December). *Access control and AAA for Data and Services.* https://joinup.ec.europa.eu/collection/are3na/access-control-and-aaa-data-and-services

Geeks for Geeks (2021, October). *Computer Network: AAA (Authentication, Authorization and Accounting*). https://www.geeksforgeeks.org/computer-network-aaa-authentication-authorization-and-accounting/

Messaoud Benantar (2016*). Access Control System: Security Identity Management and Trust Models*. Springer. ISBN-10: 0-387-00445-9.

Dudley, A., Braman, J., & Vincenti, G. (2011). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices: Issues, Impacts and Practices* (Issue January). https://books.google.com/books?hl=en&lr=&id=_-aeBQAAQBAJ&pgis=1

Trachtman, J. P. (2013). Cyberspace and Cybersecurity. In *The Future of International Law*. https://doi.org/10.1017/cbo9781139565585.006

UNIT 4 HARDWARE AND SOFTWARE PROTECTION

CONTENTS

1.0 Introduction

Despite all security measures discussed above, an organization is prone to security breach if its employees lack security caution and awareness on their working computers. These computers contain sensitive organization details and information and therefore need to implement security measures to protect their data. Threats such as unauthorized access, internet fraudsters, viruses and spyware can cause a lot of damages to organization through employees' computer. This unit will address measures on hardware and software based to prevent potential attack or damage of organization data.

2.0 Intended Learning Outcomes (ILOs)

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

- improve their data privacy through hardware protection
- protect their selves from software and internet attacks.

3.0 Main Content

3.1 Hardware Protection

A computer contains various hardware like processor, RAM, monitor etc. So, OS must ensure that these devices remain intact (not directly accessible by the user).

3.1.1 CPU Protection

CPU protection is referred to as we cannot give CPU to a process forever, it should be for some limited time otherwise other processes will not get the chance to execute the process. So, for that, a timer is used to get over from this situation. Which will basically give a certain amount of time a process and after the timer execution, a signal will be sent to the process to leave the CPU. hence process will not hold CPU for more time.

3.1.2 Memory Protection

In memory protection, we are talking about the situation when two or more processes are in memory and one process may access the other process memory to protect this situation. We are using two registers as:

1. Base register
2. Limit register

Basically, Base register store the starting address of program and limit register store the size of the process, so when a process wants to access the memory then it is checked that it can access or cannot access the memory.

3.1.3 I/O Protection

When we ensure the I/O protection, then some cases will never have occurred in the system as:

1. Termination I/O of other process
2. View I/O of other process
3. Giving priority to a particular process I/O If an application process wants to access any I/O device then it will be done through system call so that OS will monitor the task. Like In C language write() and read() is a system call to read and write on file.

There are two modes in instruction execute:

- **User mode** - The system performs a task on behalf of user application this instruction. In this mode, the user cannot directly access hardware and reference memory.
- **Kernel mode** - Whenever a direct access to hardware is required a system call is used by the application program. We know that when an application process wants to access any I/O device, it should be done through system call so that the Operating system will monitor the task.

3.2 Software and OS protection

Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability. It refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it.

So, a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc. OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised. OS security may be approached in many ways, including adherence to the following:

- Performing regular OS patch updates
- Installing updated antivirus engines and software
- Scrutinizing all incoming and outgoing network traffic through a firewall
- Creating secure accounts with required privileges only (i.e., user management)

3.2.1 Authentication

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

- **Username / Password** − User need to enter a registered username and password with Operating system to login into the system.
- **User card/key** − User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.
- **User attribute** - fingerprint/ eye retina pattern/ signature − User need to pass his/her attribute via designated input device used by operating system to login into the system.

3.2.2 One Time Password

One Time passwords - One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password are implemented in various ways.

- **Random numbers** − Users are provided cards having numbers printed along with corresponding alphabets. System asks for numbers corresponding to few alphabets randomly chosen.
- **Secret key** − User are provided a hardware device which can create a secret id mapped with user id. System asks for such secret id which is to be generated every time prior to login.
- **Network password** − Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

3.2.3 Program Threat

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as Program Threats. One of the common examples of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. e.g. Trojan Horse, trap door, logic bomb, virus, etc.

3.2.4 System Threat

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. e.g. worm, port scanning, DoS, etc.

3.3 Cases/Examples

Software patching such as updating Operating system, obsolete applications are good practice of software prevention. To update your Windows 7, 8, 8.1, and 10 Operating System, the following steps are advice:

1. Open Windows Update by clicking the **Start** button in the lower-left corner. In the search box, type **Update**, and then, in the list of results, click either **Windows Update** or **Check for updates**

2. Click the **Check for updates** button and then wait while Windows looks for the latest updates for your computer
3. If you see a message telling you that important updates are available, or telling you to review important updates, click the message to view and select the important updates to download or install
4. In the list, click the important updates for more information. Select the checkboxes for any updates that you want to install, and then click **OK**
5. Click **Install updates**

Note: It is important that you **do not shut your computer off or allow it to run out of battery** during the update process. Doing so can cause a corruption of the operating system, which can often only be fixed by reformatting the computer.

Discussion

Is it possible to implement One Time Password on system logon security?

5.0 Conclusion

Computer systems face a number of security threats. One of the basic threats is data loss, which means that parts of a database can no longer be retrieved. This could be the result of physical damage to the storage medium (like fire or water damage), human error or hardware failures.

Another security threat is unauthorized access. Many computer systems contain sensitive information, and it could be very harmful if it were to fall in the wrong hands. Imagine someone getting a hold of your social security number, date of birth, address and bank information. Getting unauthorized access to computer systems is known as cracking.

6.0 Summary

The objective of system security is the protection of information and property from theft, corruption and other types of damage, while allowing the information and property to remain accessible and productive. System security includes the development and implementation of security countermeasures. There are a number of different approaches to computer system security, including the use of a firewall, data encryption, passwords and biometrics.

7.0 References/Further Reading

Andrew S., T., & David J., W. (2011). *COMPUTER NETWORKS* (M. Horton, H. Michael, D. Tracy, & H. Melinda (eds.); fifth). Pearson Education.

Joseph, M. K. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (fourth, Vol. 7, Issue 2). McFarland & Company, Inc. https://doi.org/10.1353/pla.2007.0017

Pande, J. (2017). *Introduction to Cyber Security (FCS)*. http://uou.ac.in

Stewart, J. M., Tittel, E., & Chapple, M. (2011). *CISSP: Certified Information Systems Security Professional Study Guide*. Wiley.

Module 3: Computer Forensics and Digital Investigation

Introduction of Module

Digital devices such as cell phones, tablets, gaming consoles, laptop and desktop computers have become indispensable part of the modern society. With the proliferation of these devices in our everyday lives, there is the tendency to use information derived from them for criminal activities. Crimes such as fraud, drug trafficking, homicide, hacking, forgery, and terrorism often involve computers. To fight computer crimes, digital forensics (DF) originated in law enforcement, computer security, and national defense. Law enforcement agencies, financial institutions, and investment firms are incorporating digital forensics into their infrastructure. Digital forensics is used to help investigate cybercrime or identify direct evidence of a computer-assisted crime. The concept of digital forensics dates back to late 1990s and early2000s when it was considered as computer forensics. The legal profession, law enforcement, policy makers, the business community, education, and government all have a vested interest in DF. Digital forensics is often used in both criminal law and private investigation. It has been traditionally associated with criminal law. It requires rigorous standards to stand up to cross examination in court

This module will consist of four units are follows
Unit 1: Computer Forensics
Unit 2: Network, Disk, Malware and Database Forensics
Unit 3: Email, Memory and Mobile Forensics
Unit 4: Malware Analysis

UNIT 1 COMPUTER FORENSICS

CONTENTS

1.0 Introduction

Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from the digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it. Crimes committed within electronic or digital domains, particularly within cyberspace, have become extremely common these days. Criminals are using technology to a great extent in committing various digital offences and creating new challenges for law enforcement agents, attorneys, judges, military, and security professionals. Digital forensics has become an incredibly useful and invaluable tool in the detection of criminal activities, identifying and solving computer-based and computer-assisted crimes.

2.0 Intended Learning Outcomes (ILOs)

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

- explain the concept of computer forensics
- explain the characteristics of digital forensics
- explain digital forensics procedure
- explain the advantages of computer forensics
- disadvantages of computer forensics.

3.0 Main Content

3.1 Computer Forensics History

It is difficult to pinpoint when computer forensics history began. Most experts agree that the field of computer forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. Government personnel charged with protecting important, confidential, and certainly secret information conducted forensic examinations in response to potential security breaches to not only investigate the particular breach, but to learn how to prevent future potential breaches. Ultimately, the fields of information security, which focuses on protecting information and assets, and computer forensics, which focuses on the response to hi-tech offenses, started to intertwine.

Over the next decades, and up to today, the field has exploded. Law enforcement and the military continue to have a large presence in the information security and computer forensic field at the local, state, and federal level. Private organizations and corporations have followed suit – employing internal information security and computer forensic professionals or contracting such professionals or firms on an as-needed basis. Significantly, the private legal industry has more recently seen the need for computer forensic examinations in civil legal disputes, causing an explosion in the e-discovery field. The computer forensic field continues to grow on a daily basis. More and more large forensic firms, boutique firms, and private investigators are gaining knowledge and experience in the field. Software companies continue to produce newer and more robust forensic software programs. And law enforcement and the military continue to identify and train more and more of their personnel in the response to crimes involving technology.

3.2 Definition of Computer Forensics

Computer Forensics, also known as Cyber Forensics refers to the analysis of information in the computer systems, with the objective of finding any digital evidence that can be used for legal proceedings, but also to discover the cause of an incident. Computer forensics is the process of extracting data and information from computer systems to function as digital evidence for civic

purposes, or in most cases to prove and legally impeach cybercrime. The purpose of computer forensics is to provide forensic practices, legal processes, and ethical principles to assure reliable and detailed digital evidence that can be used for the courtroom needs. The objective of computer forensics is to guarantee a well-structured investigation and a follow-up of processes in order to resolve incidents and malfunctions in an organization.

3.2.1 Objectives of computer forensics

Here are the essential objectives of using Computer forensics:

- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

3.2.2 Characteristics of Digital Forensics

- Identification: Identifying what evidence is present, where it is stored, how it is stored (in which format). Electronic devices can be personal computers, Mobile phones, PDAs, etc.
- Preservation: Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
- Analysis: Forensic lab personnel reconstruct fragment of data and draw conclusions based on evidence.

- Documentation: A record of all the visible data is created. It helps in recreating and reviewing the crime scene. All the findings from the investigations are documented.
- Presentation: All the documented findings are produced in a court of law for further investigations.

3.2.3 **Digital Forensics**Procedure

The procedure starts with identifying the devices used and collecting the preliminary evidence on the crime scene. Then the court warrant is obtained for the seizures of the evidences which leads to the seizure of the evidences. The evidences are then transported to the **forensics lab** for further investigations and the procedure of transportation of the evidence from the crime scene to labs are called chain of custody. The evidences are then copied for analysis and the original evidence is kept safe because analysis are always done on the copied evidence and not the original evidences. The analysis is then done on the copied evidence for suspicious activities and accordingly the findings are documented in a non-technical tone. The documented findings are then presented in the court of law for further investigations.

3.2.4 Advantages of Computer Forensics

- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies gather important information on their computer systems or networks potentially being compromised.
- Efficiently tracks down cyber criminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

3.2.5 Disadvantages of Computer Forensics

- Before the digital evidence is accepted into court it must be proved that it is not tampered with.
- Producing and keeping the electronic records safe are expensive.
- Legal practitioners must have extensive computer knowledge.
- Need to produce authentic and convincing evidence.

- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result.

3.2.6 Limitation of Digital forensic investigation

Digital forensic investigation offers certain limitations listed below

- Need to produce convincing evidences

  One of the major setbacks of digital forensics investigation is that the examiner must have to comply with standards that are required for the evidence in the court of law, as the data can be easily tampered. On the other hand, computer forensic investigator must have complete knowledge of legal requirements, evidence handling and documentation procedures to present convincing evidences in the court of law.

- Investigating Tools

  The effectiveness of digital investigation entirely lies on the expertise of digital forensics examiner and the selection of proper investigation tool. If the tool used is not according to specified standards then in the court of law, the evidences can be denied by the judge.

- Lack of technical knowledge among the audience

  Another limitation is that some individuals are not completely familiar with computer forensics; therefore, many people do not understand this field. Investigators have to be sure to communicate their findings with the courts in such a way to help everyone understand the results.

- Cost

  Producing digital evidences and preserving them is very costly. Hence this process may not be chosen by many people who cannot afford the cost.

3.2.7 Applications of Digital Forensics

Digital forensics deals with gathering, analyzing and preserving the evidences that are contained in any digital device. The use of digital forensics depends on the application. Itis used mainly in the following two applications

- **Criminal Law**

In criminal law, the evidence is collected to support or oppose a hypothesis in the court. Forensics procedures are very much similar to those used in criminal investigations but with different legal requirements and limitations.

- **Private Investigation**

Mainly corporate world uses digital forensics for private investigation. It is used when companies are suspicious that employees may be performing an illegal activity on their computers that is against company policy. Digital forensics provides one of the best routes for company or person to take when investigating someone for digital misconduct.

3.3 Digital forensics Application

In recent time, commercial organizations have used digital forensics in following a type of cases

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concern with the regulatory compliance

4.0 Self-Assessment Exercises

2. Define Computer Forensics and what are the Characteristics of Digital Forensics
   Answer

Computer forensics is the process of extracting data and information from computer systems to function as digital evidence for civic purposes, or in most cases to prove and legally impeach cybercrime.

Characteristics of Digital Forensics

- Identification:
- Preservation
- Analysis
- Documentation
- Presentation

5.0 Conclusion

Digital forensics involves the process of identifying, collecting, acquiring, preserving, analysing, and presenting of digital evidence. Digital evidence must be authenticated to ensure its admissibility in a court of law. Ultimately, the forensic artefacts and forensic methods used (e.g., static or live acquisition) depend on the device, its operating system, and its security features.

6.0 Summary

In this unit, we have been able to outline computer forensics history, characteristics of digital forensics, digital forensics procedure, advantages of computer forensics and disadvantages of computer forensics.

7.0 References/Further Reading

https://www.techtarget.com/searchsecurity/definition/computer-forensics

Årnes, A. (Ed.). (2017). *Digital forensics*. John Wiley & Sons.

Kävrestad, J. (2020). *Fundamentals of Digital Forensics*. Springer International Publishing.

Easttom, C. (2021). *Digital Forensics, Investigation, and Response*. Jones & Bartlett Learning.

Nelson, B., Phillips, A., &Steuart, C. (2019). Guide to Computer Forensics and Investigations, 2019. *structure*, *10*, 26.

Dafoulas, G. A., & Neilson, D. (2019, October). An overview of digital forensics education. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)* (pp. 1-7). IEEE.

Pachghare, V. K. (2019). *Cryptography and information security*. PHI Learning Pvt. Ltd..

Lin, X., Lin, X., &Lagerstrom-Fife. (2018). *Introductory Computer Forensics*. Springer International Publishing.

Whitman, M. E., &Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

UNIT 2 NETWORK, DISK, MALWARE AND DATABASE FORENSICS

CONTENTS

1.0 Introduction

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases. Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

2.0 Intended Learning Outcomes (ILOs)

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

- explain the concept of Disk Forensics
- explain the process of Disk Forensics
- explain Network Forensics procedure
- explain Network Forensics
- explain Examinations of Network Forensics
- explain Malware Forensics.

3.0 Main Content

3.1 Types of Digital Forensics

3.1.1 Disk Forensics

Disk forensics deals with extracting raw data from primary or secondary storage of the device by searching active, modified, or deleted files. Disk forensics is also the science of extracting forensic information from digital storage media like Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc. The process of Disk Forensics are:

i. Identify digital evidence

First step in Disk Forensics is identification of storage devices at the scene of crime like hard disks with IDE/SATA/SCSI interfaces, CD, DVD, Floppy disk, Mobiles, PDAs, flash cards, SIM, USB/ Fire wire disks, Magnetic Tapes, Zip drives, Jazz drives etc. These are some of the sources of digital evidence.

ii. Authenticate the evidence

Authentication of the evidence is carried out in Cyber Forensics laboratory. Hash values of both source and destination media will be compared to make sure that both the values are same, which ensures that the content of destination media is an exact copy of the source media.

iii. Seize & Acquire the evidence

Next step is seizing the storage media for digital evidence collection. This step is performed at the scene of crime. In this step, a hash value of the storage media to be seized is computed using appropriate cyber forensics tool. Hash value is a unique signature generated by a mathematical hashing algorithm based on the content of the storage media. After computing the hash value, the storage media is securely sealed and taken for further processing.

One of the cardinal rules of Cyber Forensics is “Never work on original evidence”. To ensure this rule, an exact copy of the original evidence is to be created for analysis and digital evidence collection. Acquisition is the process of creating this exact copy, where original storage media will be write protected and bit stream copying is made to ensure complete data is copied into the destination media. Acquisition of source media is usually done in a Cyber Forensics laboratory.

iv. Preserve the evidence

Electronic evidences might be altered or tampered without trace. Once the acquisition and authentication have been done, the original evidence should be placed in secure storage keeping away from highly magnetic and radiation sources. One more copy of image should be taken and it needs to be stored into appropriate media or reliable mass storage. Optical media can be used as the mass storage. It is reliable, fast, longer life span and reusable.

v. Analyze the evidence

Verification of evidence before starting analysis is an important step in Cyber Forensics process. This is done in Cyber Forensics laboratory before commencing analysis. Hash value of the evidence is computed and compared it with the hash value taken at the time of acquisition. If both the values are same, there is no change in the content of the evidence. If both are different, there is some change in the content. The result of verification should be properly documented.

Analysis is the process of collecting digital evidence from the content of the storage media depending upon the nature of the case being examined. This involves searching for keywords, picture analysis, time line analysis, registry analysis, mailbox analysis, database analysis, cookies, temporary and Internet history files analysis, recovery of deleted items and analysis, data carving and analysis, format recovery and analysis, partition recovery and analysis, etc.

vi. Report the findings

Case analysis report should be prepared based on the nature of examination requested by a court or investigation agency. It should contain nature of the case, details of examination requested, details of material objects and hash values, result of evidence verification, details of analysis conducted and digital evidence collected, observations of the examiner and conclusion. Presentation of the report should be in simple terms and precise way so that non-technical persons should be able to understand the content of the report.

vii. Documenting

Documentation is very important in every step of the Cyber Forensics process. Everything should be appropriately documented to make a case admissible in a court of law. Documentation should be started from the planning of case investigation and continue through searching in scene of crime, seizure of material objects, chain of custody, authentication and acquisition of evidence, verification and analysis of evidence, collection of digital evidence and reporting, preservation of material objects and up to the closing of a case.

3.1.2 Network Forensics

Network forensics, unsurprisingly, refers to the investigation and analysis of all traffic going across a network suspected of use in cyber crime, say the spread of data-stealing malware or the analysis of cyber attacks. Network forensics is also a subset of digital forensics that deals

with the collection and analysis of network traffic with the goal of better understanding and avoiding cybercrime. The importance of network forensics has grown in recent years, according to a report from the European Union Agency for Cybersecurity (ENISA), with the emergence and popularity of network-based services such as e-mails, Directory services, World Wide Web, and others. Using network forensics, the entire contents of e-mails, instant messages, web browsing operations, and file transfers can be recovered and rebuilt to reveal the original transaction. The payload inside the highest-layer packet may end up on disc, but the envelope that delivered it is only captured in network traffic. For the investigator, the network protocol data that surrounded each conversation is often highly valuable.

There are two methods of overarching network forensics, the first being the **"catch it as you can" method**, which involves capturing all network traffic for analysis, which can be a long process and requires a lot of storage. The second technique is the **"stop, look and listen" method,** which involves analysing each data packet flowing across the network and only capturing what is deemed as suspicious and worthy of extra analysis; this approach can require a lot of processing power but does not need as much storage space.

3.1.2.1 Methods of Network Forensics

“Stop, look, and listen” method: Administrators monitor each data packet that passes through the network, but only capture what is deemed suspicious and warrants further investigation. While this technique does not take up a lot of space, it does require a lot of processing power.

All network traffic is captured using the "catch it as you can" technique. It ensures that no significant network events are overlooked. This is a time-consuming process that reduces storage efficiency as storage volume increases.

3.1.2.2 Examinations of Network Forensics

The steps involve in network forensics investigation are as follows:

- **Recognition**

Because this step is the path to the case's conclusion, the identification process has a significant effect on the subsequent steps. The process of identifying and assessing an incident based on network indicators is included in this step.

- **Safeguarding**

In the second step, the examiner would isolate the data for preservation and security purposes, preventing others from accessing the digital device and tampering with the digital evidence. Many software tools, such as Autopsy and Encase, are available for data preservation.

- **Accumulating**

The act of documenting the physical scene and duplicating digital evidence using standardized processes and procedures is known as accumulating.

- **Observation**

This procedure entails keeping track of all visible data. Many pieces of metadata from data may be discovered by the examiner, which may be useful in court.

- **Investigation**

The investigation agents can reconstruct data fragments after recognizing and safeguarding the evidence (data). The agent draws a conclusion based on the evidence after analyzing the data. SIEM (Security Information and Event Management) software keeps track of what happens in the IT environment. With security information management (SIM), which gathers, analyses, and reports on log data, SIEM tools analyze log and event data in real-time to provide threat monitoring, event correlation, and incident response.

- **Documentation**

Forensic is a legal term that means "to bring to the court". The procedure for summarizing and explaining conclusions has been completed. This should be written in layman's terms with abstracted terminologies, with all abstract terminologies referring to precise details.

- **Incident Response**

The information gathered to validate and assess the incident led to the detection of an intrusion.

3.1.2.3 Database Forensics

Database servers store sensitive information. Database forensics refers to the branch of digital forensic science specifically related to the study of databases and the data they keep. Database forensics look at who access the database and what actions are performed. Large data security breaches are a large problem, and criminal investigators search for related information. Modern criminal investigations often involve database forensics as investigators search for motive and method and try to identify suspects.

A forensic examination of a database may investigate the timestamps relating to the update time of a row in a relational table in order to verify the actions of a database user. Another database forensics case might examine all transactions within a database system or application over a specific period of time in order to identify any fraudulent transactions. Experts in database forensics need to be well-versed in almost all aspects of database development and use, as they have to preserve, authenticate, analyze and output data from large, custom-built databases that cannot just be copied and taken back to the office for further investigation.

Sometimes, a database may be perfectly healthy but suspicious activities and results may have raised questions from a customer that prompted a forensic investigation. The following scenarios would require the intervention of a database forensic specialist.

- Failure of a database
- Deletion of information from database
- Inconsistencies in the data of a database
- Detection of suspicious behavior of users

A database forensics expert will normally use a read-only method or an identical forensic copy of the data when interfacing with a database to ensure that no data is compromised. They will run a series of diagnostic tools to help them to:

- Create a forensic copy of a database for analysis
- Reconstruct missing data and/or log files associated with the deletion
- Decipher data and ascertain possible causes of corruption
- Audit user activities and isolate suspicious and illegal behavior

3.1.2.4 Malware Forensics

It is a way of finding, analyzing & investigating various properties of malware to seek out the culprits and reason for the attack. the method also includes tasks like checking out the malicious code, determining its entry, method of propagation, impact on the system, ports it tries to use etc. investigators conduct forensic investigation using different techniques and tools.

3.1.2.5 Types of Malware

The category of malware is predicated upon different parameters like how it affects the system, functionality or the intent of the program, spreading mechanism, and whether the program asks for user's permission or consent before performing certain operations. a number of the commonly encountered malwares are:

- Backdoor
- Botnet
- Downloader
- Launcher
- Rootkit
- HackTool
- Rogue application
- Scareware
- Worm or Virus
- Credential-stealing program, etc.

3.1.2.6 Symptoms of Infected Systems

- System could be come unstable and respond slowly as malware might be utilizing system resources.
- Unknown new executables found on the system.
- Unexpected network traffic to the sites that you simply don't expect to attach with.
- Altered system settings like browser homepage without your consent.
- Random pop-ups are shown as advertisement.

Recent additions to the set are alerts shown by fake security applications which you never installed. Messages like "Your computer is infected" are displayed and it asks the user to register the program to get rid of the detected threat. Overall, your system will showcase unexpected & unpredictable behavior.

3.1.2.7 Different Ways Malware Can Get Into System:

- Instant messenger applications
- Internet relay chat
- Removable devices
- Links and attachments in emails
- Legitimate "shrink-wrapped" software packaged by disgruntled employee
- Browser and email software bugs
- NetBIOS (File sharing)
- Fake programs
- Untrusted sites & freeware software
- Downloading files, games screensavers from websites

4.0 Self-Assessment Exercises

1. Explain the following:
    i. Disk Forensics
    ii. Network Forensics
    iii. Methods of Network Forensic
    iv. Database Forensics
    v. Malware Forensics
3. Explain the symptoms of infected systems.
4. Explain different ways malware can get into system.

5.0 Conclusion

The forensic examination of electronic systems has undoubtedly been a huge success in the identification of cyber and computer-assisted crime. Organisations are placing an increasing importance on the need to be equipped with appropriate incident management capabilities to

handle misuse of systems. Computer forensics is an invaluable tool in the process. The domain of computer forensics has grown considerably in the last decade. Driven by industry, focus was initially placed upon developing tools and techniques to assist in the practical application of the technology

6.0 Summary

- Digital Forensics is the preservation, identification, extraction, and documentation of computer evidence which can be used in the court of law
- Process of Digital forensics includes 1) Identification, 2) Preservation, 3) Analysis, 4) Documentation and, 5) Presentation
- Different types of Digital Forensics are Disk Forensics, Network Forensics, Wireless Forensics, Database Forensics, Malware Forensics, Email Forensics, Memory Forensics, etc.

Digital forensic Science can be used for cases like 1) Intellectual Property theft, 2) Industrial espionage 3) Employment disputes, 4) Fraud investigations

7.0 References/Further Reading

https://www.techtarget.com/searchsecurity/definition/computer-forensics

Kävrestad, J. (2020). *Fundamentals of Digital Forensics*. Springer International Publishing.

Easttom, C. (2021). *Digital Forensics, Investigation, and Response*. Jones & Bartlett Learning.

Nelson, B., Phillips, A., & Steuart, C. (2019). Guide to Computer Forensics and Investigations, 2019. *structure*, *10*, 26.

Dafoulas, G. A., & Neilson, D. (2019, October). An overview of digital forensics education. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)* (pp. 1-7). IEEE.

Pachghare, V. K. (2019). *Cryptography and information security*. PHI Learning Pvt. Ltd.

Lin, X., Lin, X., & Lagerstrom-Fife. (2018). *Introductory Computer Forensics*. Springer International Publishing.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

UNIT 3 EMAIL, MEMORY AND MOBILE FORENSICS

CONTENTS

1.0 Introduction

The Internet is a very easy way to reach any system. If confidential data is not properly protected, then it becomes opens to vulnerable access and misuse. Cyber-crime can cause varying degrees of damage by hackers. So, detailed forensic analysis is required to come to a conclusion about an incident and to prove or disprove someone's guilt. Some criminal activities like child pornography, hacking, and identity theft can be traced and the criminals can be punished if proper evidence is found against them. Email communication is also on target. Because it is one of the most popular and commonalty used means of online communication, for both prospects individuals and businesses, emails are normally used by organizations to exchange most simple information, such as meeting schedules, document distribution and some sensitive information

2.0 Intended Learning Outcomes (ILOs)

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

- explain the concept of Email Forensics
- explain the concept of Memory Forensics
- explain the concept of Mobile Phone Forensics
- explain ddigital Forensic Examination Process.

3.0 Main Content

3.1 Email Forensics

Email forensics is the analysis of source and content of the email message, identification of sender and receiver, date and time of email and the analysis of all the entities involved. Email forensics also reforms to the forensics of client or server systems suspected in an email forgery.

3.1.1 Email Header Analysis

Email forensics starts with the study of email **header** as it contains a vast amount of information about the email message. This analysis consists of both the study of the content body and the email header containing the info about the given email. Email header analysis helps in identifying most of the email related crimes like spear phishing, spamming, email spoofing etc. Spoofing is a technique using which one can pretend to be someone else, and a normal user would think for a moment that it's his friend or some person he already knows. It's just that someone is sending emails from their friend's spoofed email address, and it is not that their account is hacked.

3.1.2 Challenges in Email Forensics

Email forensics play a very important role in investigation as most of the communication in present era relies on emails. However, an email forensic investigator may face the following challenges during the investigation

- Fake Emails

The biggest challenge in email forensics is the use of fake e-mails that are created by manipulating and scripting headers etc. In this category criminals also use temporary email which is a service that allows a registered user to receive email at a temporary address that expires after a certain time period.

- Spoofing

Another challenge in email forensics is spoofing in which criminals used to present an email as someone else's. In this case the machine will receive both fake as well as original IP address.

- Anonymous Re-emailing

Here, the Email server strips identifying information from the email message before forwarding it further. This leads to another big challenge for email investigations

3.1.3 Techniques Used in Email Forensic Investigation

Email forensics is the study of source and content of email as evidence to identify the actual sender and recipient of a message along with some other information such as date/time of

transmission and intention of sender. It involves investigating metadata, port scanning as well as keyword searching.

Some of the common techniques which can be used for email forensic investigation are

- Header Analysis
- Server investigation
- Network Device Investigation
- Sender Mailer Fingerprints
- Software Embedded Identifiers

3.2 Memory Forensics

Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analysing it for further investigation. Memory forensics is a vital form of cyber investigation that allows an investigator to identify unauthorized and anomalous activity on a target computer or server. This is usually achieved by running special software that captures the current state of the system's memory as a snapshot file, also known as a memory dump. This file can then be taken offsite and searched by the investigator.

Memory Forensics is useful because of the way in which processes, files and programs are run in memory, and once a snapshot has been captured, many important facts can be ascertained by the investigator, such as:

- Processes running
- Executable files that are running
- Open ports, IP addresses and other networking information
- Users that are logged into the system, and from where
- Files that are open and by whom

3.3 Mobile Phone Forensics

Mobile Phone Forensics mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc. and other data present in it. Mobile forensics is a subset of digital forensics, the retrieval of data

from an electronic source. Specifically, mobile forensics deals with recovery evidence from mobile devices such as smartphones and tablets. Today, because individuals rely on mobile devices for so much of their sending, receiving and searching of data, it stands to reason that these devices hold a vast quantity of evidence that might be applicable to investigators. Mobile devices can provide all types of important data, ranging from call logs and text messages to web search history and location data that shows where the device owner might have been at a given time.

3.3.1 Mobile Device Forensic Examination Process

Digital evidence is fragile and volatile. Improper handling of a mobile phone can alter or destroy the evidence contained on the device. Further, if the mobile phone is not handled following digital forensics best practices, it can be impossible to determine what data was changed and if those changes were intentional or unintentional. To protect the evidence and prevent spoilation, mobile devices need to be analyzed by a trained examiner using mobile device forensic tools.

The initial handling of digital evidence can be divided into four phases: identification, collection, acquisition, and preservation.

3.3.1.1 Identification

The identification phase's purpose and scope are to identify the digital evidence relevant to the case. It is possible that this evidence will span multiple devices, systems, servers, and cloud accounts. With a mobile phone, the data is not isolated only to the device. The data contained in the device can be synced to cloud storage or another mobile device or backed up onto a computer.

Identification also requires comprehensive documentation. Documentation is critical throughout the entire investigative process, but especially in the beginning, as any mistakes can taint the evidence. The acquisition phase gives us a perfect snapshot in time (forensic copy) of how the data exists. Since identification is the first step and before acquisition, mistakes made here are carried out throughout the process.

3.3.1.2 Collection

The collection phase involves gathering physical devices, such as the smartphone and other mobile devices. Since digital evidence can span multiple devices, systems, and servers, collecting it can become more complicated than securing more traditional forensic evidence. There are vital functions that should be performed to protect the evidence.

- **Isolating Device Users**

The primary goal of the collection process, other than ensuring all relevant electronic items are collected, is to protect digital evidence from contamination. One way this is done is by isolating the devices from their respective users until a forensic acquisition of the mobile device can be performed. While in their custody, the user could delete, create, or change data before the forensic acquisition (the perfect snapshot in time of the mobile phone data) is performed. They could also factory reset or wipe the device, permanently destroying some data or potentially everything on the mobile phone.

- **Isolating Devices**

Along with isolating the mobile phone from the user, we also need to isolate the device itself. By design, mobile phones are intended for communication, and they are continually sending and receiving data even when they are on the bedside table charging overnight. If data transmission occurs, even with no person physically touching the phone, data can be lost, changed, or destroyed.

Isolation of the device itself is achieved by eliminating all forms of data transmission, including the cellular network, Bluetooth, wireless networks, and infrared connections. By isolating the phone from all networks, the mobile phone is prevented from receiving any new data that would cause other data to be deleted or overwritten.

3.3.1.3 Acquisition

The acquisition process is where a digital forensic examiner acquires, or forensically copies, the data from a mobile device using a variety of methods.

- **Logical Extraction**

A logical extraction of data from a mobile phone collects the files and folders contained on the device without any unallocated space. While what is commonly called "deleted space" is not recovered, deleted data on a mobile phone can be recovered using forensic tools and methods via a logical extraction. This data comes in the form of various database files, especially SQLite. Typically, data collected via a logical extraction includes messaging, pictures, video, audio, contacts, application data, some location data, internet history, search history, social media, and more.

- **File System Extraction**

A file system extraction is an extension of a logical extraction. It collects much of the same data as a logical extraction along with additional file system data. During a file system extraction, the forensic tool accesses the internal memory of the mobile phone, which means that the forensic software can collect system files, logs, and database files from the device that a logical acquisition cannot.

Most applications store their data in database files on a mobile phone. Since a file system extraction recovers more of these database files, more deleted data like database files and data related to application usage on the device can be recovered.

- **Physical Extraction**

The physical extraction of a mobile phone captures the entirety of the device's data, including all files, user content, deleted data, and unallocated space. While this extraction method is the most extensive, it is also the least supported. Like the forensic imaging of a computer hard drive, a physical extraction creates a bit-by-bit copy of the mobile phone's entire contents.

With a bit-by-bit copy, the logical and file system data are recovered, as well as unallocated space. This extraction method allows for the recovery of deleted data that would otherwise be inaccessible to a forensic examiner, including location information, email, messages, videos, photos, audio, applications, and almost any other data contained on a mobile phone.

- **Cloud Data**

Mobile phone forensic companies have developed tools that allow for accessing and acquiring data in the cloud. Cellebrite, the leading mobile phone forensic tool provider, can collect cloud

data from cloud backups and the actual cloud-based applications themselves. While a forensic image of a mobile phone is a potential gold mine of evidence, the ability to use the mobile phone information to find even more evidence in the cloud is a significant force multiplier.

3.3.1.4 Preservation

The mobile phone's integrity and the data on it need to be established to ensure that evidence is admissible in court.

- **Chain of Custody**

Evidence preservation aims to protect digital evidence from modification. This protection begins by ensuring that first responders, investigators, crime scene technicians, digital forensic experts, or anyone else who touches the device handles it properly. A chain of custody must be maintained throughout the entire life cycle of a case.

- **Mathematical Hashing Algorithm**

The forensic data collection process from the mobile device is better called a "forensics extraction," as data is extracted from the device instead of a perfect bit-for-bit copy of the evidence item. With the mobile phone powered on, the forensic software cannot access some areas of data. However, data that is inaccessible because the mobile device is powered on is usually of little to no value evidentiarily. Following the forensic copying comes the hashing process. A mathematical algorithm is run against the copied data, producing a unique hash value. This hash value can be thought of as a digital fingerprint, uniquely identifying the copied evidence exactly as it exists at that point in time.

3.3.1.5 Reporting

If requested by the client, a report will be prepared of the data contained on the mobile device. Sometimes, it makes the most sense for our examiners to export all of the data from a cell phone for counsel's review. We format this export in such a way that makes it as accessible as possible, with the ability to search and filter the data.

Sometimes, when timelines, data types, or types of particular forensic artifacts need to be explained in order to tell the story of what happened in a case, a more in-depth report is needed.

3.3.1.6 Expert Testimony

Expert testimony is the culmination of everything that goes into a mobile device forensic examination. Selecting the expert with the appropriate technical expertise and experience is vital. It is also important that the expert is able to explain technical concepts, forensic procedures, and digital artifacts in plain language, as the use of jargon and acronyms can be detrimental to the triers of fact. Ultimately, if an expert has an airtight analysis but cannot communicate it effectively to a judge and jury, their words are meaningless. When selecting an expert, choose the one you can have a conversation with. If that expert cannot explain technical details to you in an accessible way, they likely don't understand what they are talking about themselves.

4.0 Self-Assessment Exercises

1. Explain email forensics

Email forensics is the analysis of source and content of the email message, identification of sender and receiver, date and time of email and the analysis of all the entities involved. Email forensics also reforms to the forensics of client or server systems suspected in an email forgery.

2. What is the purpose of email header analysis

Email header analysis helps in identifying most of the email related crimes like spear phishing, spamming, email spoofing etc. Spoofing is a technique using which one can pretend to be someone else, and a normal user would think for a moment that it’s his friend or some person he already knows

3. List the common techniques used in email forensic investigation
    - Header Analysis
    - Server investigation
    - Network Device Investigation
    - Sender Mailer Fingerprints
    - Software Embedded Identifiers

5.0 Conclusion

Email evidence often plays a pivotal role in digital forensics investigations and eDiscovery. When preserving emails from the cloud, forensics experts have to consider issues such as multi-factor authentication, running-in-place searches on the server before the acquisition, handling server errors and throttling, privacy issues, and time constraints.

6.0 Summary

In this unit, we have been able to outline email forensics, email header analysis, mobile forensics and mobile device forensics examination process.

7.0 References/Further Reading

https://www.techtarget.com/searchsecurity/definition/computer-forensics

Årnes, A. (Ed.). (2017). *Digital forensics*. John Wiley & Sons.

Kävrestad, J. (2020). *Fundamentals of Digital Forensics*. Springer International Publishing.

Easttom, C. (2021). *Digital Forensics, Investigation, and Response*. Jones & Bartlett Learning.

Nelson, B., Phillips, A., & Steuart, C. (2019). Guide to Computer Forensics and Investigations, 2019. *structure*, *10*, 26.

Dafoulas, G. A., & Neilson, D. (2019, October). An overview of digital forensics education. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)* (pp. 1-7). IEEE.

Pachghare, V. K. (2019). *Cryptography and information security*. PHI Learning Pvt. Ltd..

Lin, X., Lin, X., & Lagerstrom-Fife. (2018). *Introductory Computer Forensics*. Springer International Publishing.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

UNIT 4 MALWARE ANALYSIS

CONTENTS

1.0 Introduction

We live in a very technologically advanced society. Technology and the use computers have become a part of our everyday life. Because of the increased knowledge and abundance of computer use, viruses have become a huge problem for users. Viruses are destructive programs that attack the computer and interfere with the operations of the computer. A virus can easily corrupt or delete data from your computer, which can become very costly to the owner of the computer. It is important that we learn about how viruses work so that we can avoid them at all cost.

Malware is any piece of software which is intended to cause harm to your system or network. Malware is different from normal programs in a way that they most of them have the ability to spread itself in the network, remain undetectable, cause changes/damage to the infected system or network, persistence. They have the ability to bring down the machine's performance to knees and can cause a destruction of the network. Consider the case when the computer becomes infected and is no longer usable, the data inside becomes unavailable – these are some of the malware damage scenarios. Malware attacks can be traced back to the time, even before the internet became widespread.

2.0 Intended Learning Outcomes (ILOs)

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

- explain Malware Analysis
- explain the Types of Malwares
- explain the Types of Malware Analysis.

3.1 Malware Analysis

Malware analysis is the process of determining the purpose and functionality of a piece of malware. This process will reveal what type of harmful program has infected your network, the damage it is capable of causing, and most importantly how to remove it. Malware analysis used to be performed manually by experts in a time-consuming and cumbersome process.

Today, there are a number of open-source malware analysis tools that can perform this process automatically.

The first step in malware analysis is to identify the suspicious file(s). The file should then be run through malware analysis software to figure out how it works. While malware analysis is crucial for recovering from cyberattacks, it can also be used preemptively. By safely examining emerging malware programs, security experts determine how best to protect against them.

3.1.1 Types of Malwares

Malware can take many forms and comes in many variations. I don't want to end up here with a lengthy post, so I'm going to keep the following list short. I have listed here the most common malware types that you should know about.

- **Virus**: Viruses are pieces of malware that require human intervention to propagate to other machines. Think of this intervention as a user installing a malicious program from a website or a phishing email. Virus is the first category of malware to appear on the horizon of computer security. It is self-replicating in nature and is referred to as a parasitic infector. It does not have a separate existence; instead, it inserts its code into existing files on the system. It could be an executable programor script of different programming languages like VBScript, JavaScript, Perl, etc.
- **Worm**: Unlike Viruses, Worms do not need the help of humans to move to other machines. They can spread easily and can infect a high number of machines in a short amount of time. Worms are also self-replicating; however, they are stand alone malware strains. They do not modify other files to spread; instead, they make copies of themselves over network shares or on other systems. Worms are further classified based upon the spreading mechanism used such as email, P2P, IRC, etc.
- **Trojan**: These appear to be normal programs that have a legitimate function, like a game or a utility program. But underneath the innocent-looking user interface, a Trojan performs malicious tasks without the user being aware. A Trojan always disguised as useful software and tempts a user to install it and it is also bundled with hidden malicious functionality. It is non-replicating in nature, i.e. it does not spread in a similar manner as viruses or worms.
- **Spyware**:
  Spywareissoftwarethatgatherspersonalorconfidentialinformationfromusersystemswith

outtheirknowledge. It includes monitoring the systems to collect information such as browsing habits, recently visited sites, passwords, credit card information, and other confidential information. Once spyware is installed, it does not show any visible notifications to indicate that it is monitoring user activities. It instantly sends this information to the configured remote server.

- **Keylogger**: This is a special type of spyware. It is specialized in recording the keystrokes made by the user. Keyloggers are a particularly insidious type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device. The term keylogger, or "keystroke logger," is self-explanatory: Software that logs what you type on your keyboard. However, keyloggers can also enable cybercriminals to eavesdrop on you, watch you on your system camera, or listen over your smartphone's microphone
- **Ransomware**: Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

3.1.2 Types of Malware Analysis

3.1.2.1 Static analysis

Static analysis examines a malware file without actually running the program. This is the safest way to analyze malware, as executing the code could infect your system. In its most basic form, static analysis gleans information from malware without even viewing the code. Metadata such as file name, type, and size can yield clues about the nature of the malware. MD5 checksums or hashes can be compared with a database to determine if the malware has been previously recognized. And scanning with antivirus software can reveal what malware you're dealing with.

Advanced static analysis—also known as code analysis—dissects the binary file to study each component, still without executing it. One method is to reverse engineer the code using a disassembler. Machine code is translated into assembly code, which is readable and understandable. By looking at the assembly instructions, an analyst can tell what the program is meant to do. A file's headers, functions, and strings can provide important details. Unfortunately, modern hackers are adept at evading this technique. By embedding certain

syntax errors into their code, they can misdirect disassemblers and ensure the malicious code still runs. Because static malware analysis can be more easily foiled, dynamic malware analysis is also necessary, here are some examples of valuable information that we can extract using static analysis.

- File Headers

Depending on the target operating system, malware files can be one of two types : Portable Executable(PE) or Executable and Linkable Format (ELF). The latter is used in Linux, whereas the former is the standard format used by Windows executable files.

Since Windows is more targeted by malware than Linux, you will encounter PE-based malware files more often than their ELF-based counterparts.

It would therefore be more rewarding to learn about PE format first and to understand how you could retrieve useful information by examining certain sections of the file.

For example, by examining the PE header, you can obtain information about which functions from other libraries does the malware call, or at what memory address does the program execution starts.

- Hash

A Hash is a unique string of a fixed length that can be generated based on an input. No matter the size of this input, the hash value will always be of a fixed length.

A hash is used to check for the integrity of files. If the content of the file changes, then its hash value will also change.

Now, by calculating the hash value of a file, we can verify if it's a known malware by searching for this hash and see if it exists on a malware database such as Virus total.

- Strings

Strings is a tool that you can use to extract the ASCII text from a program file. It does this by searching for any series of consecutive ASCII characters.

Very often, you will find interesting stuff using this tool, such as a hidden code or a domain name address.

- Code Analysis

Programs are executed in a special series of operations called opcodes (operation codes). These are special binary instructions that are generally represented in hexadecimal. They can be interpreted by computers and are far less understandable by us humans.

Disassembly is the process of extracting Assembly code from these opcodes. Although Assembly isn't an easy language either, it is much more approachable compared to opcodes.

By performing disassembly, a malware analyst can peek into the instructions of the malware to understand what it does, where the malicious portions of the program are, and what hidden information they can retrieve.

Another way to reverse engineer malware is to go one step further and use a Decompiler instead of a Disassembler. While the latter outputs the assembly code, the former presents a much better alternative by providing the source code in a high-level language that is friendlier and easier to understand for humans.

3.1.2.2 Dynamic analysis

Dynamic analysis also called malware behavior analysis runs the malware program to examine its behavior. Of course, running a piece of malware always carries some risk, so dynamic analysis must be performed in a safe environment. A "sandbox" environment is a virtual system that is isolated from the rest of the network and can run malware without risk to production systems. After the analysis is done, the sandbox can be rolled back to its original state without permanent damage.

When a piece of malware is run, technical indicators appear and provide a detection signature that dynamic analysis can identify. Dynamic analysis software monitors the sandbox system to see how the malware modifies it. Modifications may include new registry keys, IP addresses, domain names, and file path locations. Dynamic analysis will also reveal whether the malware is communicating with a hacker's external server. Debugging is another useful dynamic analysis technique. As the malware is running, a debugger can zero in on each step of the program's behavior while the instructions are being processed.

As with static analysis, cybercriminals have developed techniques to foil dynamic analysis. Malware may refuse to run if it detects a virtual environment or debugger. The program may delay the execution of its harmful payload or require certain user input. To reach the best understanding of a particular malware threat, a combination of static and dynamic analysis is

most effective. This method is obviously less safe than static analysis because basically, you would willingly be infecting your machine. It is a good practice to perform it on a sandbox environment, such as a virtual machine, or even better, a completely separate physical machine isolated from any network.

- **Debugging**

A debugger is a powerful tool that any malware analyst should know how to use. It allows you to follow the flow of the program as it executes, and provides useful features that give you better control over the execution of a program.

For example, you can set breakpoints on certain instructions where you want the execution to pause. You can also examine the contents of registers and specific memory addresses, and even better, you can modify their values while the program is running.

4.0 Self-Assessment Exercises

i. Define Malware Analysis

Malware analysis is the process of determining the purpose and functionality of a piece of malware. This process will reveal what type of harmful program has infected your network, the damage it's capable of causing, and most importantly how to remove it.

ii. List and explain Types of Malwares

- **Virus**: Viruses are pieces of malware that require human intervention to propagate to other machines.
- **Worm**: Unlike Viruses, Worms do not need the help of humans to move to other machines. They can spread easily and can infect a high number of machines in a short amount of time.
- **Trojan**: These appear to be normal programs that have a legitimate function, like a game or a utility program. But underneath the innocent looking user interface, a Trojan performs malicious tasks without the user being aware.
- **Spyware**: Spywareissoftwarethatgatherspersonalorconfidentialinformationfromusersystemswithouttheirknowledge.

- **Keylogger**: This is a special type of spyware. It is specialized in recording the keystrokes made by the user.
- **Ransomware**: Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

iii. Explain Static and Dynamic Analysis

Dynamic analysis also called malware behavior analysis runs the malware program to examine its behavior, while Static analysis examines a malware file without actually running the program.

5.0 Conclusion

Viruses are very destructive programs that can be devastating to companies and individual.The best defense against malware is a combination of vigilant and sensible behavior on the Internet, proper computer usage, and anti-malware software. By erring on the side of caution when surfing the web, not opening strange links or emails from unknown senders, and regularly updating and running an anti-malware program, you'll be relatively safe from the manifold dangers of the Internet.

6.0 Summary

In this unit, we have been able to outline malware analysis, types of malwares and malware analysis.

7.0 References/Further Reading

https://www.techtarget.com/searchsecurity/definition/computer-forensics

Årnes, A. (Ed.). (2017). *Digital forensics*. John Wiley & Sons.

Kävrestad, J. (2020). *Fundamentals of Digital Forensics*. Springer International Publishing.

Easttom, C. (2021). *Digital Forensics, Investigation, and Response*. Jones & Bartlett Learning.

Nelson, B., Phillips, A., & Steuart, C. (2019). Guide to Computer Forensics and Investigations, 2019. *structure*, *10*, 26.

Dafoulas, G. A., & Neilson, D. (2019, October). An overview of digital forensics education. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)* (pp. 1-7). IEEE.

Pachghare, V. K. (2019). *Cryptography and information security*. PHI Learning Pvt. Ltd..

Lin, X., Lin, X., & Lagerstrom-Fife. (2018). *Introductory Computer Forensics*. Springer International Publishing.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

Module 4: Introduction to Cyber Law and Ethics

Introduction to Module

As soon as cyberspace and e-commerce were created in the mid-1990s, cybercrime flourished on a parallel track. Today, cybercrime has been doubling every single year in the number of incidents, as well as monetary losses. It is impossible to truly quantify cybercrime because most victims only see further losses in publicizing their inability to defend themselves from this modern day menace. The interesting note is that, of the cybercriminals who have been caught, the vast majority have pleaded guilty. The word ethics comes from the ancient Greek word eché, which means character. Every human society practices ethics in some way because every society attaches a value on a continuum of good to bad, right to wrong, to an individual's actions according to where that individual's actions fall within the domain of that society's rules and canons. In this module, Cyber crime Acts will be address which provide legal backings to human data and privacy.

Unit 1: Concept of Cyber Law

Unit 2: The INDIA cyber-Acts

Unit 3: The International Laws

Unit 4: Cyber Ethics

UNIT 1 CONCEPT OF CYBER LAWS

CONTENTS

1.0 Introduction

Technology has engendered new types of lawsuits or modified old ones. As, for example, the next generation of offences arose within the field of computer crimes (e.g., identity thefts), technology impacted on traditional rights such as copyright (1709) and privacy (1890), turning them into a matter of access, control, and protection over information in digital environments. This unit we explain the concepts of cyber law, the need of cyber law in the IT world and why is important to actually address cyber crime issues.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, student will able to

- justify cyber crimes as sanctioned in cyber laws
- demonstrate the concept of cyber law.

3.0 Main Content

3.1 What is Cyber Law

Cyber Law or IT Law is referred to as the Law of the Internet. The Cyber law definition says it is a legal system designed to deal with the Internet, computing, Cyberspace, and related legal issues. The apt introduction to Cyber Law is: It is ‘paper laws’ in the ‘paperless world’.

Cyber law encompasses aspects of intellectual property, contract, jurisdiction, data protection laws, privacy, and freedom of expression. It directs the digital circulation of software, information, online security, and e-commerce. The area of Cyber Law provides legal recognition to e-documents. It also creates a structure for e-commerce transactions and e-filling. Hence, to simply understand the Cyber law’s meaning, it is a legal infrastructure to deal with Cybercrimes. An increase in the usage of E-commerce has made it pivotal that there are proper regulatory practices set up to ensure no malpractices take place.

The laws implemented for cybersecurity largely vary from country to country and their respective jurisdiction. The punishments for the same also vary from fine to imprisonment based on the crime committed. It is very important for citizens to know the cyber laws of their respective countries to make sure they are well aware of all information regarding cybersecurity. The first cyber law to ever exist was the Computer Fraud and Abuse Act in 1986 that prohibited Unauthorized access to computers and illegal usage of digital information

3.1.1 Categories of Cyber Law

Individual- Cybercrimes against individuals involve crimes like online harassment, distribution and trafficking of child pornography, manipulation of personal information, use of obscene data, and identity theft for personal benefit.

Property- Usage, and transmission of harmful programs, theft of information and data from financial institutions, trespassing cyberspace, computer vandalism, and unauthorized possession of information digitally are some of the crimes under the property.

Government- The crimes that come under this are cyber terrorism, manipulation, threats, and misuse of power against the Government and citizens. Groups or Individuals terrorizing Government websites is when this form of cyber terrorism occurs.

3.1.2 Components of Cyber Law

Safeguarding data and privacy– Both private and professional information and data must be secured thoroughly. Personal and financial information always attracts cybercriminals. Misuse of this information by any other person is illegal and that is where these laws come into play. The basic steps to safeguard your data and privacy is elaborated below

- Two-factor authentication for financial platforms and any other forums that provide this function.
- Initiate Virus protection software.
- Use only verified payment methods on reputed websites.
- Avoid giving out personal information

Cybercrimes- These crimes are any illegal activities that occur on a networked technological device. These crimes include online and network attacks, extortion, harassment, money laundering, hacking, and many more.

Intellectual property- Intellectual property is basically an individual or group's work, designs, symbols, inventions, or anything owned by them which are intangible and are usually patented or copyrighted. Now cyber theft would mean the stealing or illegal use of the same intangible items.

Electronic and digital signatures- Nowadays most individuals and companies use electronic signatures to verify electronic records. This has become reliable and regular. The wrong usage by another of this signature is illegal and hence a cybercrime.

3.1.3 Importance of Cyber Law

Cyber laws are important to punish criminals who commit serious crimes related to the computer such as hacking, online harassment, data theft, disrupting the online workflow of any enterprise, attacking another individual or website.

- Cyber laws decide different forms of punishment depending on the type of law you broke, who you offended, where you violated the law, and where you live.
- It is important to bring criminal behind the bars, as most cybercrimes do not enter the category of common crime and it may lead to denial of justice.
- These crimes may endanger the confidentiality and financial security of a nation therefore these problems should be addressed lawfully

3.2 Types of Cyber Laws

The law has rules dictating behavior while using computers and the internet. It also prevents unscrupulous activities online. Some major types of Cyber Law are:

- **Copyright:** These days' copyright violations come under Cyber law. It protects the rights of companies and individuals to get profit from their creative work. In earlier days, online copyright violation was easier. But due to the introduction of Cyber law, it has become difficult to violate copyright. Which is very good!
- **Defamation:** Generally, people use the internet to speak out their minds. But in the case of fake public statements on the internet that are bound to hamper someone's business and reputation, that is when defamation law comes into the picture. Defamation Laws are a kind of civil law.

- **Fraud:** What is Cybercrime law? The major motive of this law is to protect people from online fraud. Consumers these days depend on Cyber Law to prevent online fraud. IT law prevents credit card theft, identity theft, and other money-related crimes that are bound to happen online. People who commit online fraud, face state criminal charges. They may also witness a civil action by the victim.
- **Harassment and Stalking:** Some statements made by people can violate criminal law that refuses stalking and harassment online. When somebody posts threatening statements repeatedly about somebody else, this violates both criminal and civil laws. Cyber lawyers fight and defend people when online stalking occurs.
- **Freedom of Speech:** The internet is used as a medium of free speech. But there are laws to avoid free speech that may cause immorality online. Cyber lawyers should advise their clients about the amount of free speech allowed online. Sometimes the Cyber lawyers fight cases for their clients where they debate whether their client's actions are within the permissible limit of free speech.
- **Trade Secrets:** Businesses depend on Cyber laws to preserve their trade secrets. For example, some organizations might steal online algorithms or features designed by another firm. In this case, Cyber laws empower the victim organization to take legal action to protect its secrets.
- **Contracts and Employment Laws:** You might have agreed upon many terms and conditions while opening a website or downloading some software. This is where the Cyber law is used. These Terms & Conditions are designed for online privacy concerns.

3.3 Why do we need Cyber Laws

As of early 2021, the number of people that use the internet is over 4.66 Billion. With that number increasing by 7% annually. This also means every day can account for almost 8,75,000 new users. Given this swift increase in the use of Cyberspace, implementation and the usage of strict cyber rules helps establish a safe and secure environment for the users. Living in a rapidly progressing world, the one thing to keep pace with it is the Internet. Although it initially started off as an information tool, today it helps with communication and commerce. Being highly sophisticated and developing every single day, the usage of cyberspaces has become common, hence the increase in cybercrimes is inevitable. Cyber laws provide sanctions to those that break the cyber rules making the cyber space a safe place to certain extent to operate.

 **Discussion**

What is biggest crime ever committed in the cyber space?

4.0 Self-Assessment/Exercises

Explain the different sources of law

Answer

a) **Legislation**: - It is the formal enactment of law by the legislature created or authorized by the constitution. It stands in contrasted with judge made law. Legislation consists of written laws, as contrasted with judge made law or common law. It also stans in contrasted to customary law.

b) **Common Law**: - It comprises the body of principle, which derive their authority solely from the decisions of courts. It is a body of law that develops and derives through judicial decisions different from legislative enactments. Its principals do not derive their validity from formal law making by anybody, but from their enunciation through decisions of courts.

c) **Custom**: - Custom‟ denotes a usage or practice of the people (including a particular social group or a group residing in a particular locality) which by common adoption and acquiescence and by long and unvarying habit, has become compulsory and has acquired the force of law with respect to the place or subject matter to which it relates.

 **5.0 Conclusion**

Cyberlaw does concern you. As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyber legal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails, to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyberlaw issues involved.

6.0 Summary

Cyber law describes the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields. Cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

7.0 References/Further Reading

Dudley, A., Braman, J., & Vincenti, G. (2011). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices: Issues, Impacts and Practices* (Issue January). https://books.google.com/books?hl=en&lr=&id=_-aeBQAAQBAJ&pgis=1

IshaUpadhyay (September, 2020). *Cyber Law: A Comprehensive Guide For 2021. https://www.jigsawacademy.com/blogs/cyber-security/what-is-cyber-law/.* Last accessed: December, 2021.

Joseph, M. K. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (fourth, Vol. 7, Issue 2). McFarland & Company, Inc. https://doi.org/10.1353/pla.2007.0017.

Pande, J. (2017). *Introduction to Cyber Security (FCS)*. http://uou.ac.in\

Trachtman, J. P. (2013). Cyberspace and Cybersecurity. In *The Future of International Law*. https://doi.org/10.1017/cbo9781139565585.006.

Vikaspedia. *Cyber Laws*.https://vikaspedia.in/education/digital-litercy/information-security/cyber-laws. Last accessed: 30 December, 2021.

UNIT 2 The INDIA Cyber Acts

CONTENTS

1.0 Introduction

The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it. India as a nation has encountered several cyber-attacks which forced the government to impose cyber law that regulates the code and conducts of the people of India and international on the cyberspace. In this unit, we will discuss some of the regulations such as ITA 2000, IPC, National Cyber security policy and review some of the scenarios of cybercrime in India

2.0 Intended Learning Outcomes (ILOs)

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

- explain laws binds to cyberspace
- discuss their rights in data and privacy protection
- explain from existing scenarios of cybercrimes in India.

3.0 Main Content

3.1 The India IT Act

The Information Technology Act, 2000 also Known as an IT Act is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce. The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from ‘section 91 – section 94’, deals with the revisions to the Indian Penal Code 1860.

The IT Act, 2000 has two schedules:

- **First Schedule** – Deals with documents to which the Act shall not apply.
- **Second Schedule** – Deals with electronic signature or electronic authentication method

The offences and the punishments in IT Act 2000:

The offences and the punishments that falls under the IT Act, 2000 are as follows:

1. Tampering with the computer source documents.
2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information which is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.
7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offences.
10. Protected System.
11. Penalties for confiscation not to interfere with other punishments.
12. Act to apply for offence or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

Sections and Punishments under Information Technology Act, 2000 are as follows :

Section 43 - Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.

Section 66 - Applicable in case a person is found to dishonestly or fraudulently committing any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.

Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by Rs. 1 lakh fine, depending upon the severity.

Section 66C - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs.1 lakh fine.

Section 66 D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

Section 66E - This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years imprisonment or 2,00,000 fine or both.

Section 66F - This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.

Section 67 - This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine or Rs. 10,00,000 or both.

3.2 Indian Penal Code (IPC) 1980

Apart from punishments in IT Act, 2000, there are certain crimes that are attracted by IPC provisions as well. The following is the enumeration of the IPC provisions along with various cybercrimes that are attracted by respective Sections and the punishment for the same.

- **Section 292 of IPC**: Although this Section was drafted to deal with the sale of obscene material, it has evolved in the current digital era to be concerned with various cybercrimes. The publication and transmission of obscene material or sexually explicit act or exploit acts containing children, etc which are in electronic form are also governed by this section. Though the crimes mentioned above seem to be alike, they are recognized as different crimes by the IT Act and IPC. The punishment imposed upon the commission of such acts is imprisonment and fine up to 2 years and Rs. 2000. If any of the aforementioned crimes are committed for the second time, the imprisonment could be up to 5 years and the fine could be imposed up to Rs. 5000.
- **Section 354C of IPC:** The cybercrime dealt with under this provision is capturing or publication of a picture of private parts or acts of a woman without such person's consent. This section exclusively deals with the crime of 'voyeurism' which also

recognizes watching such acts of a woman as a crime. If the essentials of this Section (such as gender) are not satisfied, Section 292 of IPC and Section 66E of IT Act, 2000 is broad enough to take the offenses of a similar kind into consideration. The punishment includes 1 to 3 years of imprisonment for first-time offenders and 3 to 7 years for second time offenders.

- **Section 354D of IPC**: This section describes and punishes 'stalking' including both physical and cyberstalking. If the woman is being monitored through electronic communication, internet, or email or is being bothered by a person to interact or contact despite her disinterest, it amounts to cyberstalking. The latter part of the Section states the punishment for this offense as imprisonment extending up to 3 years for the first time and 5 years for the second time along with a fine imposed in both the instances. In the case of Kalandi Charan Lenka v. The State of Odisha, the victim received certain obscene messages from an unknown number which are damaging her character. Moreover, emails were sent and the fake Facebook account was created by the accused which contained morphed pictures of the victim. Hence, the accused was found prima facie guilty for cyberstalking by the High Court under various provisions of IT Act and Section 354D of IPC
- **Section 379 of IPC**: If a mobile phone, the data from that mobile or the computer hardware is stolen, Section 379 comes into the picture and the punishment for such crime can go up to 3 years of imprisonment or fine or both. But the attention must be given to the fact that these provisions cannot be applied in case the special law i.e. IT Act, 2000 provisions are attracted. In this regard, in the case of Gagan Harsh Sharma v. The State of Maharashtra, one of the employers found that the software and data were stolen and someone has breached the computers and gave access to sensitive information to the employees. The employer gave information to the police and they filed a case under Section 379, 408, and Section 420 of IPC and various other IT Act provisions. The question in front of the court is whether the police can file a case under IPC or not. The court decided that the case cannot be filed based on the IPC provisions as the IT Act has an overriding effect.
- **Section 411 of IPC**: This deals with a crime that follows the offenses committed and punished under Section 379. If anyone receives a stolen mobile phone, computer, or data from the same, they will be punished in accordance with Section 411 of IPC. It is not necessary that the thief must possess the material. Even if it is held by a third party

knowing it to be others, this provision will be attracted. The punishment can be imposed in the form of imprisonment which can be extended up to 3 years or fine or both.

- **Section 419 and Section 420 of IPC**: These are related provisions as they deal with frauds. The crimes of password theft for the purpose of meeting fraudulent objectives or the creation of bogus websites and commission of cyber frauds are certain crimes that are extensively dealt with by these two sections of IPC. On the other hand, email phishing by assuming someone's identity demanding password is exclusively concerned with Section 419 of IPC. The punishments under these provisions are different based upon the gravity of the committed cybercrime. Section 419 carries a punishment up to 3 years of imprisonment or fine and Section 420 carries up to 7 years of imprisonment or fine.
- **Section 465 of IPC**: In the usual scenario, the punishment for forgery is dealt with in this provision. In cyberspace, the offenses like email spoofing and preparation of false documents are dealt with and punished under this Section which imbibes the imprisonment reaching up to 2 years or fine or both. In the case of Anil Kumar Srivastava v. Addl Director, MHFW, the petitioner electronically forged signature of AD and later filed a case making false allegations about the same person. The Court held that the petitioner was liable under Section 465 as well as under Section 471 of IPC as the petitioner also tried to use it as a genuine document.
- **Section 468 of IPC**: If the offenses of email spoofing or the online forgery are committed for the purpose of committing other serious offenses i.e cheating, Section 468 comes into the picture which contains the punishment of seven years of imprisonment or fine or both.
- **Section 469 of IPC**: If the forgery is committed by anyone solely for the purpose of disreputing a particular person or knowing that such forgery harms the reputation of a person, either in the form of a physical document or through online, electronic forms, he/she can be imposed with the imprisonment up to three years as well as fine.
- **Section 500 of IPC**: This provision penalizes the defamation of any person. With respect to cybercrimes, sending any kind of defamatory content or abusive messages through email will be attracted by Section 500 of IPC. The imprisonment carried with this Section extends up to 2 years along with fine.
- **Section 504 of IPC**: If anyone threatens, insults, or tries to provoke another person with the intention of effecting peace through email or any other electronic form, it amounts

to an offense under Section 504 of IPC. The punishment for this offense extends up to 2 years of imprisonment or fine or both.

- **Section 506 of IPC**: If a person tries to criminally intimidate another person either physically or through electronic means with respect to the life of a person, property destruction through fire or chastity of a woman, it will amount to an offense under Section 506 of IPC and punishment of imprisonment where the maximum period is extended up to seven years or fine or both.
- **Section 509 of IPC**: This Section deals with the offense of uttering a word, showing a gesture, and committing an act that has the potential to harm the modesty of a woman. It also includes the sounds made and the acts committed infringing the privacy of a woman. If this offense is committed either physically or through electronic modes, Section 509 gets attracted and the punishment would be imprisonment of a maximum period of one year or fine or both.

3.3 India Cyberspace

Indian cyberspace was born in 1975 with the establishment of National Informatics Centre (NIC) with an aim to provide govt with IT solutions. Three networks (NWs) were set up between 1986 and 1988 to connect various agencies of govt. These NWs were, INDONET which connected the IBM mainframe installations that made up India's computer infrastructure, NICNET (the NIC NW) a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central govt with the state govts and district administrations, the third NW setup was ERNET (the Education and Research Network), to serve the academic and research communities. New Internet Policy of 1998 paved the way for services from multiple Internet service providers (ISPs) and gave boost to the Internet user base grow from 1.4 million in 1999 to over 150 million by Dec 2012. Exponential growth rate is attributed to increasing Internet access through mobile phones and tablets. Govt is making a determined push to increase broadband penetration from its present level of about 6%1. The target for broadband is 160 million households by 2016 under the National Broadband Plan.

3.4 National Cyber Security Policy

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology. It aims at protecting the public and private infrastructure from cyberattacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyberspace as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

3.5 Cases/Examples

Cybercrime Scenarios

(i) Frios vs State of Kerala

Facts : In this case it was declared that the FRIENDS application software as protected system. The author of the application challenged the notification and the constitutional validity of software under Section 70. The court upheld the validity of both. It included tampering with source code. Computer source code the electronic form, it can be printed on paper.

Held : The court held that tampering with Source code are punishable with three years jail and or two lakh rupees fine of rupees two lakh rupees for altering, concealing and destroying the source code.

(ii). R vs. Whiteley

In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users. Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and ‘made alteration in the computer database pertaining to broadband Internet user accounts’ of the subscribers. The CBI had registered a cyber crime case against Kumar and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorised use of broadband Internet. The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar’s wrongful act. He used to ‘hack’ sites from Bangalore, Chennai and other cities too, they said. Verdict: The Additional Chief Metropolitan Magistrate, Egmore,

Chennai, sentenced N G Arun Kumar, the techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offense).

Discussion

Discuss any two cybercrimes in your country.

4.0 Self-Assessment/Exercises

Discuss the classification of crimes under the IT Act 2000.

Answer

The following acts are cyber crime in the I.T. Act 2000:- Without permission of the authorized user

i) Accessing or securing access to computer system or network.
ii) Downloading, coping or extracting any data or information.
iii) Introducing any computer, virus or contaminant in the computer.
iv) Disrupting the working of the computer.
v) Disrupting the access of the computer of an authorized user.
vi) Providing assistance to ensure unauthorized access to the computer.
vii) Tampering with computer source documents.
viii) Hacking of computer system.
ix) Carring on activities that are not in compliance with the provisions of the Act.

What are the amendments to the Indian Penal Code?

Answer

The Indian Panel Code (IPC) details actions that constitute a crime and the punishments prescribed for such actions. It elaborately classifies crimes based on interests that are intended to be protected. The classification includes :-

i) Offences against body
ii) Offences against property
iii) Offences against marriage
iv) Offences against public tranquility

v) Offences against state Some important aspects have to be weighed while determining whether a crime has been committed or not.

5.0 Conclusion

Cybercrimes are a new class of crimes which are increasing day by day due to extensive use of internet these days.

6.0 Summary

Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cybercrimes.

7.0 References/Further Reading

Alfreda D. et al. (2012). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts, and Practices.* Information Science Reference, USA. ISBN 978-1-61350-133-7

B.Tech III Year (2020). *Digital notes on Cyber security*. DEPARTMENT OF INFORMATION TECHNOLOGY MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY, INDIA

ICSI(2016). *Cyber crime Law and Practice.* THE INSTITUTE OF COMPANY SCRETARIES OF INDIA. ISBN : 978-93-82207795.

Joseph, M. K. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (fourth, Vol. 7, Issue 2). McFarland & Company, Inc. https://doi.org/10.1353/pla.2007.0017

Trachtman, J. P. (2013). Cyberspace and Cybersecurity. In *The Future of International Law*. https://doi.org/10.1017/cbo9781139565585.006

UNIT 3 THE INTERNATIONAL LAWS

CONTENTS

1.0 Introduction

Cybercrime is "international" that there are ‘no cyber-borders between countries’ λ The complexity in types and forms of cybercrime increases the difficulty to fight back, fighting cybercrime calls for international cooperation λ. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale.

2.0 Intended Learning Outcomes (ILOs)

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

- explain international laws and treaties
- explain international cyber-attacks previously occurred.

3.0 Main Content

3.1 NIST Compliance

The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cybersecurity as the most reliable global certifying body. NIST Cybersecurity Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly. This framework is prioritized on flexibility and cost-effectiveness. It promotes the resilience and protection of critical infrastructure by:

- Allowing better interpretation, management, and reduction of cybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs.
- Determining the most important activities and critical operations - to focus on securing them.
- Demonstrates the trust-worthiness of organizations who secure critical assets.

- Helps to prioritize investments to maximize the cybersecurity ROI Addresses regulatory and contractual obligations.

Supports the wider information security program By combining the NIST CSF framework with ISO/IEC 27001 - cybersecurity risk management becomes simplified. It also makes communication easier throughout the organization and across the supply chains via a common cybersecurity directive laid by NIST. Final Thoughts, as human dependence on technology intensifies, cyber laws in India and across the globe need constant up-gradation and refinements. The pandemic has also pushed much of the workforce into a remote working module increasing the need for app security. Lawmakers have to go the extra mile to stay ahead of the impostors, in order to block them at their advent. Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users. Only the prudent efforts of these stakeholders, ensuring their confinement to the law of the cyberland - can bring about online safety and resilience.

3.2 Europe

In Europe, in 2004 the Council of Europe accepted a draft of a Treaty on Cybercrime, which was offered to countries worldwide. While many countries became signatories to the treaty, only a few have actually promulgated national laws compatible to the treaty. It is of interest that the treaty in Article 47 states: “Denunciation: Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.” And Article 27 states: “Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. The requested Party may refuse assistance”. Later in 2006, a controversial addendum was appended to the treaty that attracted a reduced number of signatory countries. The addendum was referring to fear of xenophobic concern surfacing on the Internet. All in all, the initiative of the Council of Europe opened the way for national legislation on cybercrime in many countries and was used as a motivation for a similar treaty at the United Nations.

3.3 United Nations

The United Nations (UN) in 2010 received a proposal recommending a Cyberspace Treaty for the UN members. After extensive debate, the proposal was rejected because it contained unacceptable articles. Most of the controversy was created by the following articles: • Article 2 of the proposal indicated supremacy of such treaty over national laws, stating that "Serious crimes against peace and security in cyberspace should be established as crimes under international law through a Cyberspace Treaty on the United Nations level, whether or not they were punishable under national law". This passage was considered ambiguous and offensive to national sovereignty.

- **Article 3.8.3**, referring to the European Union treaty counterpart, stated that "Data… of Internet traffic and transaction data, usually of telecommunications, emails, and websites visited [be retained] The purpose for data retention is traffic data analysis and mass surveillance of data…." The proposal implied that data be retained "for a period of between six months and two years." This article found the opposition of many local and international civil liberties organizations that found the wording offensive, especially the "mass surveillance of data," and clear violation of the fundamental civil rights, the cornerstone of which is privacy in personal communications.
- **Article 4** was the most controversial. In effect, the article is asking member-nations to accept the International Criminal

3.4 Impediments to Cyber Law Enforcement

International treaties can be drafted and signed and hopefully followed by the promulgation of national laws that effectively address cybercrime. This is only part one in the endless fight against cybercrime.

Part two is the actual removal of the cybercriminals from society. Presently, in this there are several areas that need definition or improvement, with some listed below.

- National bureaucracy. In most countries the court systems are overloaded, and cases are scheduled to be heard one or two years after the accusation has been formalized and deposited. Until then the accused, if guilty, may be free to commit more cybercrime.
- Cyber-skilled judges. Most often, crimes committed in cyberspace involve network intrusions and security violations that are part of highly sophisticated fraud

schemes. Judges without special and continuous training may not understand why the accused is guilty or innocent of the charges.

- Authentication of evidence. If the header of an email has the email address of the accused, that in itself is not necessarily proof of guilt or innocence.
- Loss of evidence. With a long gap between the commitment of the alleged crime and the court hearing of the case, electronic evidence may be lost or altered.
- Access to evidence. Evidence may be in servers in a foreign country, and special data extradition procedures may be required.
- Comprehensive legislation. With cybercrime schemes ahead of law enforcement by several months, added delays are introduced into the process.
- Cybercrime investigators. With the Internet explosion and the parallel explosion in cybercrime, there is no country in the world that has sufficient cyber police personnel to pursue each and every case of alleged cybercrime.

3.5 Cases/Example

Three people held guilty in on line credit card scam. Customer's credit card details w ere misused through online means for booking air-tickets. These culprits were caught by the city Cyber Crime Investigation Cell in Pune. It was found that details misused were belonging to 100 people. Mr. Parvesh Chauhan, ICICI Prudential Life Insurance officer had complained on behalf of one of his customer. In this regard Mr. Sanjeet Mahavir Singh Lukkad, Dharmendra Bhika Kale and Ahmead Sikandar Shaikh were arrested. Lukkad being employed at a private institution, Kale was his friend. Sheikh was employed in one of the branches of State Bank of India. According to the information provided by the authorities, one of the customers received a SMS based alert for purchasing of the ticket even when the credit card was being held by him. Customer was alert and came to know something was fishy; he enquired and came to know about the misuse. He contacted the Bank in this regard. Police observed involvement of many Bank's in this reference. The tickets were book through online means. Police requested for the log details and got the information of the Private Institution. Investigation revealed that the details were obtained from State Bank of India. Sheikh was working in the credit card department; due to this he had access to credit card details of some customers. He gave that information to Kale. Kale in return passed this information to his friend Lukkad. Using the information obtained from Kale, Lukkad booked tickets. He used to sell

these tickets to customers and get money for the same. He had given few tickets to various other institutions. Cyber Cell was involved in eight days of investigation and finally caught the culprits. In this regard various Banks have been contacted; also four airline industries were contacted and alerted.

Discussion

What section of the Information Technology Act (ITA) that sanction internet fraudsters? Explain the consequence according to the Act.

5.0 Conclusion

A country's participation in a particular international agreement becomes effective only if domestic laws are drafted and approved that legislate the intent of the signed international agreement.

6.0 Summary

Lawmakers and law enforcement agencies, around the world, advocate the need for cyber laws that are written in the cyber language. That is, laws that explicitly define cyber offenses and fully support the acceptance of cyber evidence. International bodies, responding to this call, have convened and produced treaties and conventions that, unfortunately, have fallen short of receiving total acceptance by the member countries.

7.0 References/Further Reading

Alfreda D. et al. (2012). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts, and Practices.* Information Science Reference, USA. ISBN 978-1-61350-133-7.

B.Tech III Year (2020). *Digital notes on Cyber security*. DEPARTMENT OF INFORMATION TECHNOLOGY MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY, INDIA.

ICSI(2016). *Cybercrime Law and Practice.* THE INSTITUTE OF COMPANY SCRETARIES OF INDIA. ISBN : 978-93-82207795.

Joseph, M. K. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (fourth, Vol. 7, Issue 2). McFarland & Company, Inc. https://doi.org/10.1353/pla.2007.0017.

Trachtman, J. P. (2013). Cyberspace and Cybersecurity. In *The Future of International Law*. https://doi.org/10.1017/cbo9781139565585.006.

UNIT 4 CYBER ETHICS

CONTENTS

1.0 Introduction

Ethics is, therefore, the study of right and wrong in human conduct. Ethics can also be defined as a theoretical examination of morality or "theory of morals." Other philosophers have defined ethics in a variety of ways. Robert C. Solomon, in Morality and the Good Life, defines ethics as a set of "theories of value, virtue, or of right (valuable) action." O.J. Johnson, on the other hand, defines ethics as a set of theories "that provide general rules or principles to be used in making moral decisions and, unlike ordinary intuitions, provides a justification for those rules." The word ethics comes from the ancient Greek word eché, which means character. Every human society practices ethics in some way because every society attaches a value on a continuum of good to bad, right to wrong, to an individual's actions according to where that individual's actions fall within the domain of that society's rules and canons.

2.0 Intended Learning Outcomes (ILOs)

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

- discuss the use of ethical theories in ethical arguments
- articulate the ethical tradeoffs in a technical decision
- explain the role of professional codes of ethics.

3.0 Main Content

3.1 Ethical Theories

Since the dawn of humanity, human actions have been judged good or bad, right or wrong based on theories or systems of justice developed, tested, revised, and debated by philosophers and elders in each society. Such theories are commonly known as ethical theories. An ethical theory determines if an action or set of actions is morally right or wrong. Codes of ethics have been drawn up based on these ethical theories. The processes of reasoning, explanation, and justification used in ethics are based on these theories. Ethical theories fall into two categories:

those based on one choosing his or her action based on the expected maximum value or values as a consequence of the action and those based on one choosing his or her action based on one's obligation or requirements of duty. The Greeks called the first category of theories telos, meaning purpose or aim. We now call these teleological or consequentialist theories. The Greeks called the second category of theories deon, meaning binding or necessary. Today, we call them deontological theories.

3.1.1 Consequentialist Theories

We think of the right action as that which produces good consequences. If an act produces good consequences, then it is the right thing to do. Those who subscribe to this position are called consequentialists. Consequentialist theories judge human actions as good or bad, right or wrong, based on the best attainable results of such actions—a desirable result denotes a good action, and vice versa. According to Richard T. Hull, consequentialist theories "have three parts: a theory of value, a principle of utility, and a decision procedure." Within these are further theories.

For example, in the theory of value there are several other theories held by consequentialists including :

- Hedonism, which equates good with pleasure, bad or evil with pain.
- Eudamonism, which equates good with happiness, bad or evil with unhappiness.
- Agathism, which views good as an indefinable, intrinsic feature of various situations and states. Evil is seen as either an indefinable, intrinsic feature of other situations and states, or simply as the absence of good.
- Agapeism, which equates good with live, bad with hate.
- Values pluralism, which holds that there are many kinds of good, including pleasure and happiness, but also knowledge, friendship, love, and so forth. These may or may not be viewed as differing in importance or priority.

There are three commonly discussed types of consequentialist theory:

i. Egoism puts an individual's interests and happiness above everything else. With egoism, any action is good as long as it maximizes an individual's overall happiness. There are two kinds of egoism: ethical egoism, which states how people ought to behave as they pursue their own interests, and psychological egoism, which describes how people actually behave.

ii. Utilitarianism, unlike egoism, puts a group's interest and happiness above those of an individual, for the good of many. Thus, an action is good if it benefits the maximum number of people. Among the forms of utilitarianism are the following:
    - Act utilitarianism tells one to consider seriously the consequences of all actions before choosing that with the best overall advantage, happiness in this case, for the maximum number of people.
    - Rule utilitarianism tells one to obey those rules that bring the maximum happiness to the greatest number of people. Rule utilitarianism maintains that a behavioral code or rule is good if the consequences of adopting that rule are favorable to the greatest number of people.

iii. Altruism states that an action is right if the consequences of that action are favorable to all except the actor

3.1.2 Deontological Theories

The theory of deontological reason does not concern itself with the consequences of the action but rather with the will of the action. An action is good or bad depending on the will inherent in it. According to deontological theory, an act is considered good if the individual committing it had a good reason to do so. This theory has a duty attached to it. For example, we know that killing is bad, but if an armed intruder enters your house and you kill him, your action is good, according to deontologists. You did it because you had a duty to protect your family and property. Deontologists fall into two categories: act deontologists and rule deontologists.

- Act deontologists consider every judgment of moral obligation to be based on its own merit. We decide separately in each particular situation what is the right thing to do.
- Rule deontologists consider that one's duty in any situation is to act within rules.

All other contemporary ethical theories, as Richard T. Hull contends, are hybrids of utilitarianist and deontologist theories. The process of ethical reasoning takes several steps, which we refer to as layers of reasoning, before one can justify to someone else the goodness or badness, rightness or wrongness of one's action. For example, if someone wants to convince you to own a concealed gun, he or she needs to explain to you why it is good to have a concealed gun. In such an exercise, the person may start by explaining to you that we are living in difficult times and that no one is safe. You may then ask why no one is safe, to which the person might reply that there are many bad people out there in possession of high- powered guns waiting to

fire them for various and very often unbelievable reasons. So owning a gun will level the playing field. Then you may ask why owning a gun levels the playing field, to which the answer would be that if the bad guys suspect that you own a gun just like theirs, they will think twice before attacking you. You may further ask why this is so; the answer may be that if they attack you, they themselves can get killed in the action. Therefore, because of this fear, you are not likely to be attacked. Hence, owning a gun may save your life and enable you to continue pursuing the ultimate concept of the good life: happiness.

On the other hand, to convince somebody not to own a concealed gun also needs a plausible explanation and several layers of reasoning to demonstrate why owning a gun is bad. Why is it a bad thing, you would ask, and the answer would be because bad guys will always get guns. And if they do, the possibility of everyone having a concealed gun may make those bad guys trigger- happy to get you fast before you get them. It also evokes an imageof the Wild West filled with gun- toting people daring everyone in order to get a kick out of what may be a boring life. You would then ask why is this situation dangerous if no one fires? The reply might be because it creates a situation in which innocent people may get hurt, denying them happiness and the good life. The explanation and reasoning process can go on and on for several more layers before one is convinced that owning a gun is good or bad. The act of owning a gun is a human act that can be judged as either good or bad, right or wrong depending on the moral and ethical principles used.

3.2 Codes of Ethics

The main domains in which ethics is defined are governed by a particular and definitive regiment of guidelines and rules of thumb called codes of ethics. These rules, guidelines, canons, advisories, or whatever you want to call them, are usually followed by members of the respective domains. For example, your family has an ethical set of rules that every member of the family must observe. Your school has a set of conduct rules that all students, staff and faculty must observe. And, your college has a set of rules that govern the use of college computers. So depending on the domain, ethical codes can take any of the following forms:

- principles, which may act as guidelines, references, or bases for some document;
- public policies, which may include aspects of acceptable behavior, norms, and practices of a society or group;
- codes of conduct, which may include ethical principles; and
- legal instruments, which enforce good conduct through courts.

Although the use of ethical codes is still limited to professions and high visibility institutions and businesses, there is a growing movement toward widespread use. The wording, content, and target of codes can differ greatly. Some codes are written purposely for the public, others target employees, and yet others are for professionals only. This unit is referred to the codes of the Association of Computing Machinery (ACM) and the Institute of Electric and Electronics Engineers' Computer Society (IEEE Computer), both professional organizations. Codes for the ACM can be found at and those for IEEE Computer at www.ieee.org.

Objectives of Codes of Ethics

Different domains and groups of people formulate different codes of ethics, but they all have the following objectives:

- **Disciplinary**: By instilling discipline, the group or profession ensures professionalism and integrity of its members.
- **Advisory**: Codes are usually a good source of tips for members, offering advice and guidance in areas where moral issues are fuzzy.
- **Educational**: Ethical codes are good educational tools for members of the domain, especially new members who have to learn the dos and don'ts of the profession. The codes are also a good resource for existing members needing to refresh and polish their possibly waning morals.
- **Inspirational**: Besides being disciplinary, advisory, and educational, codes should also carry subliminal messages to those using them to inspire them to be good.
- **Publicity**: One way for professions to create a good clientele is to show that they have a strong code of ethics and, therefore, their members are committed to basic values and are responsible.

Discussion

Why is ethics relevant in the cyberspace?

4.0 Self-Assessment/Exercises

1. What are the ten commandments for computer ethics?

Answer

i. Thou shalt not use a computer to harm other people.
ii. Thou shalt not interfere with other people's computer work.
iii. Thou shalt not snoop around in other people's files.
iv. Thou shalt not use a computer to steal.
v. Thou shalt not use a computer to bear false witness.
vi. Thou shalt not use of copy software for which you have not paid.
vii. Thou shalt not use other people's computer resources without authorization.
viii. Thou shalt not appropriate other people's intellectual output.
ix. Thou shalt think about the social consequences of the program u write.
x. Thou shalt use a computer in ways to show consideration and respect.

2. Explain the three levels of computer ethics.

Answer

- **First level**: - It is the basic level where computer ethics tries to sensitize people to the fact that computer technology has social and ethical consequences. Newspaper, TV news program, and magazines have highlighted the topic of computer ethics by reporting on events relating to computer viruses, software ownership law suits, computer aided bank robbery, computer malfunction etc.
- **Second level**: It consists of someone who takes interest in computer ethics cases, collects examples, clarifies them, looks for similarities and differences reads related works, attends relevant events to make preliminary assessments and after comparing them.
- **Third level**: It referred to as „theoretical" computer ethics applies scholarly theories to computer ethics cases and concepts in order to deepen the understanding of issues. All three level of analysis are important to the goal of advancing and defending human values.

5.0 Conclusion

The role of ethics is to help societies distinguish between right and wrong and to give each society a basis for justifying the judgment of human actions. Ethics is, therefore, a field of inquiry whose subject is human actions, collectively called human conduct, that are taken consciously, willfully, and for which one can be held responsible. According to Fr. Austin Fagothey, such acts must have knowledge, which signifies the presence of a motive, be voluntary, and have freedom to signify the presence of free choice to act or not to act.

6.0 Summary

The purpose of ethics is to interpret human conduct, acknowledging and distinguishing between right and wrong. The interpretation is based on a system which uses a mixture of induction and deduction. In most cases, these arguments are based on historical schools of thought called ethical theories. There are many different kinds of ethical theories, and within each theory there may be different versions of that theory. Let us discuss these next.

7.0 References/Further Reading

Alfreda D. et al. (2012). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts, and Practices.* Information Science Reference, USA. ISBN 978-1-61350-133-7

Baldini, Gianmarco, Botterman, Maarten, Neisse, Ricardo, and Tallacchini, Mariachiara (2016) "Ethical Design in the Internet of Things," *Science and Engineering Ethics*, 1-21.

Bustard, John D. (2017), "Improving Student Engagement in the Study of Professional Ethics: Concepts and an Example in Cyber Security" Science and Engineering Ethics, 1-16.

Dipert, Randall R. (2010) "The Ethics of Cyberwarfare," Journal of Military Ethics 9:4, 384-410.

ICSI(2016). *Cybercrime Law and Practice.* THE INSTITUTE OF COMPANY SCRETARIES OF INDIA. ISBN : 978-93-82207795.

Joseph, M. K. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (fourth, Vol. 7, Issue 2). McFarland & Company, Inc. https://doi.org/10.1353/pla.2007.0017.

Manjikian, Mary (2017) Cybersecurity Ethics: An Introduction, Routledge; 240 pp. Taddeo.

Mariarosaria and Glorioso, Ludovica (2017) Ethics and Policies for Cyber Operations, Springer. EC Council (2016) Ethical Hacking and Countermeasures (Book Series, 4 volumes), Cengage Learning.