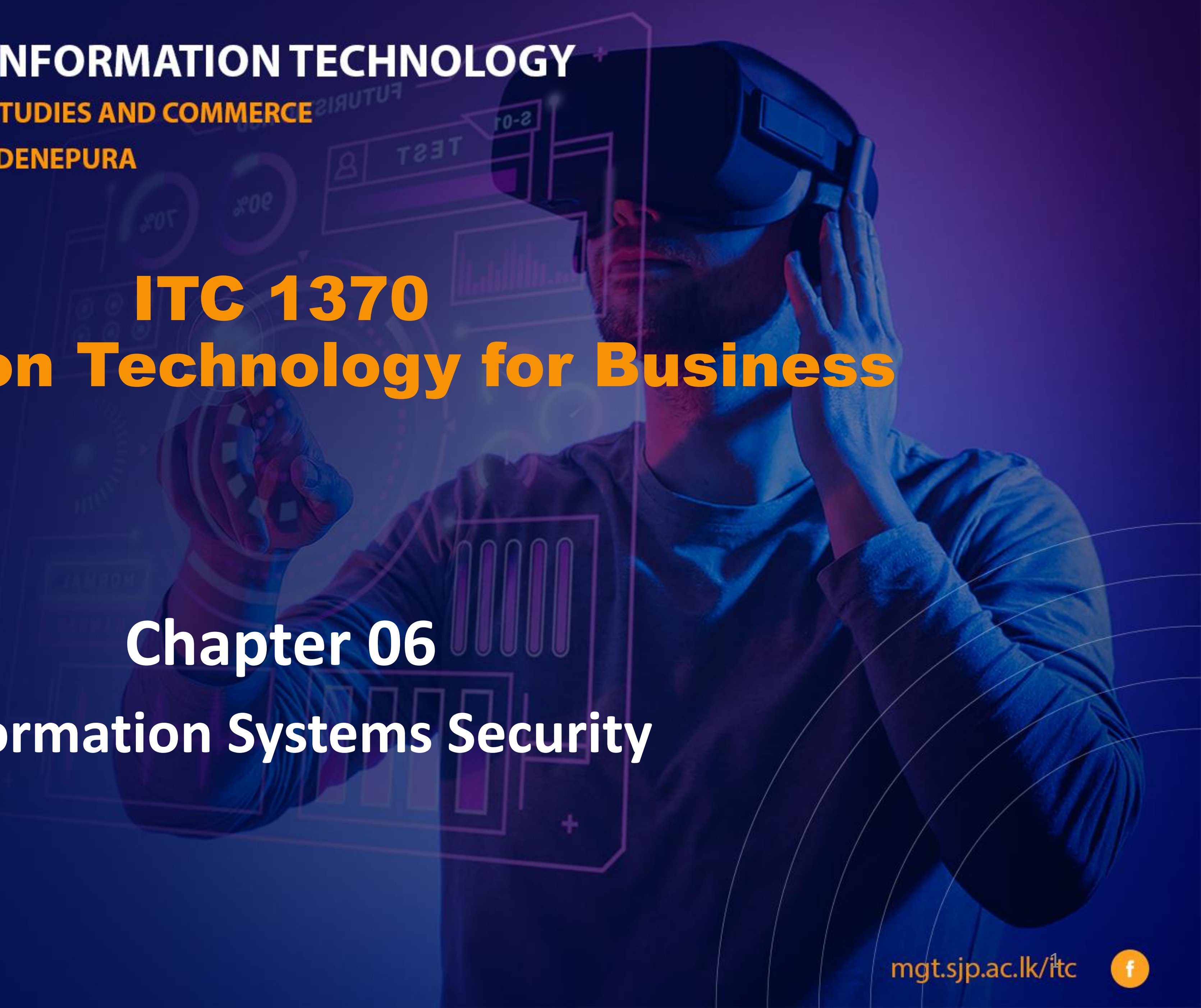
DEPARTMENT OF INFORMATION TECHNOLOGY

FACULTY OF MANAGEMENT STUDIES AND COMMERCE

UNIVERSITY OF SRI JAYEWARDENEPURA



ITC 1370
Information Technology for Business

Chapter 06

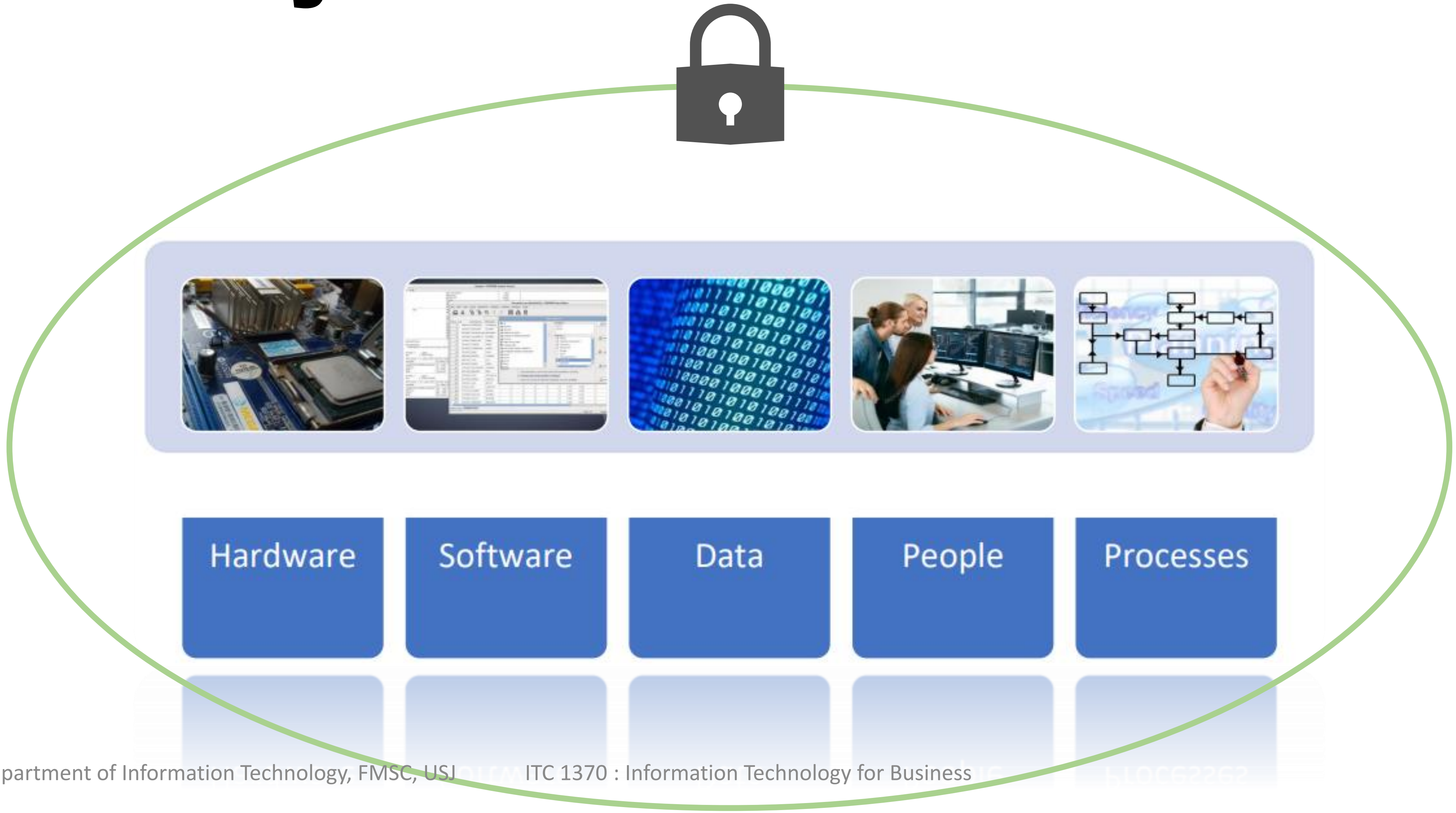
Information Systems Security

Learning Objectives

Upon successful completion of this chapter, you will be able to:

- Understand what Information Systems Security is.
- Identify the information security triad.
- Identify internal and external threats of information systems.
- Identify strategies for securing Information Systems.

What is Information Systems Security?



Hardware

Software

Data

People

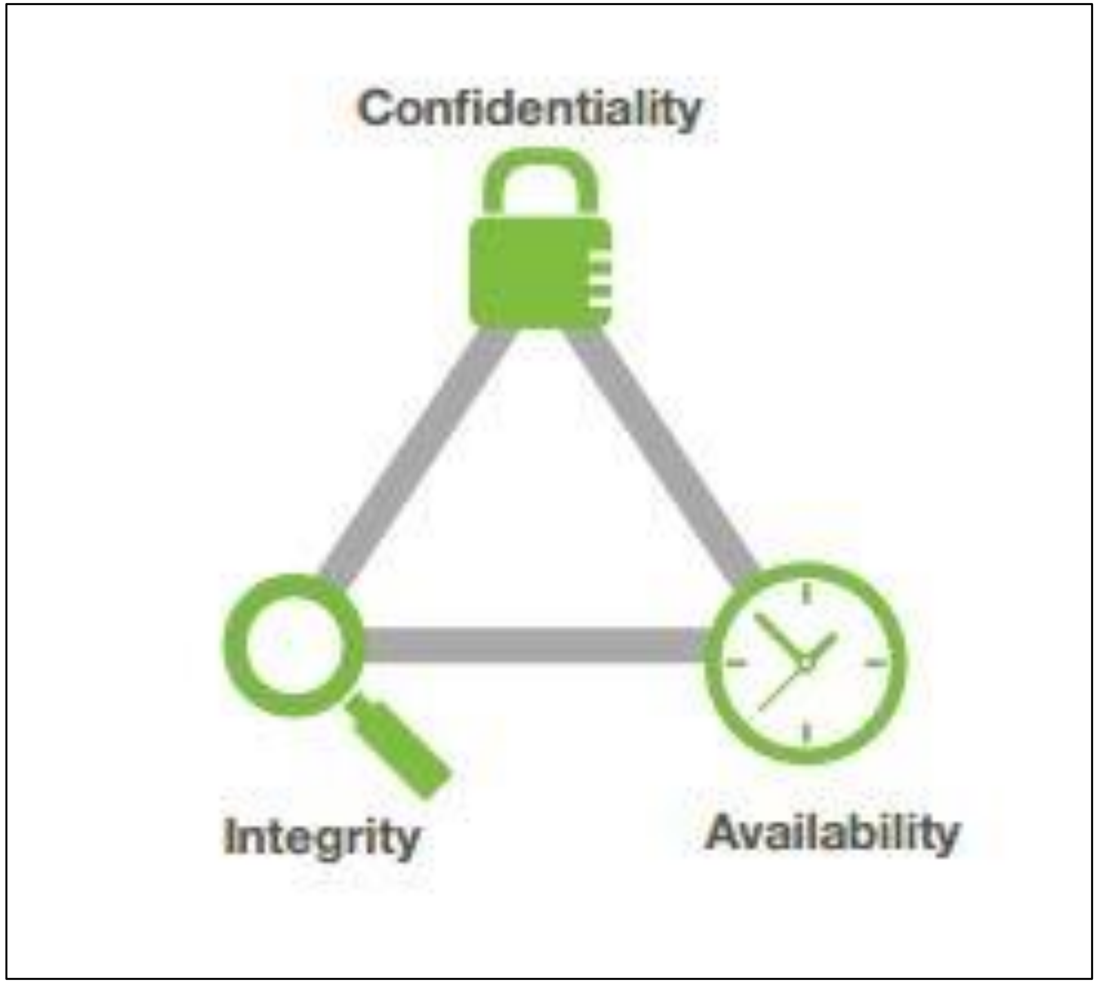
Processes

What is Information Systems Security?

“Information systems security is the collection of activities that protect the information system and the data stored in it.”

- Kim, D., & Solomon, M. (2018). *Fundamentals of information systems security* (Third edition). Jones & Bartlett Learning.

The Information Security Triad



The Information Security Triad: Confidentiality, Integrity, Availability (CIA Triad)

- **Confidentiality** — Only authorized users can view information.
  - Ex. - Universities restrict unauthorized parties to access to students' information. Access to grade records should be limited to those who have authorized access.
- **Integrity** — Only authorized users can change information. Assure that the information being accessed has not been altered, and truly represents what is intended.
  - Ex. - Only authorized personnel in the examination unit login to university's examination system and change a student's grade.
- **Availability** — Information is accessible by authorized users whenever they request the information.
  - Ex. - Online bankers require banks' web servers to be available twenty-four hours a day, seven days a week.

Internal and external threats of information systems

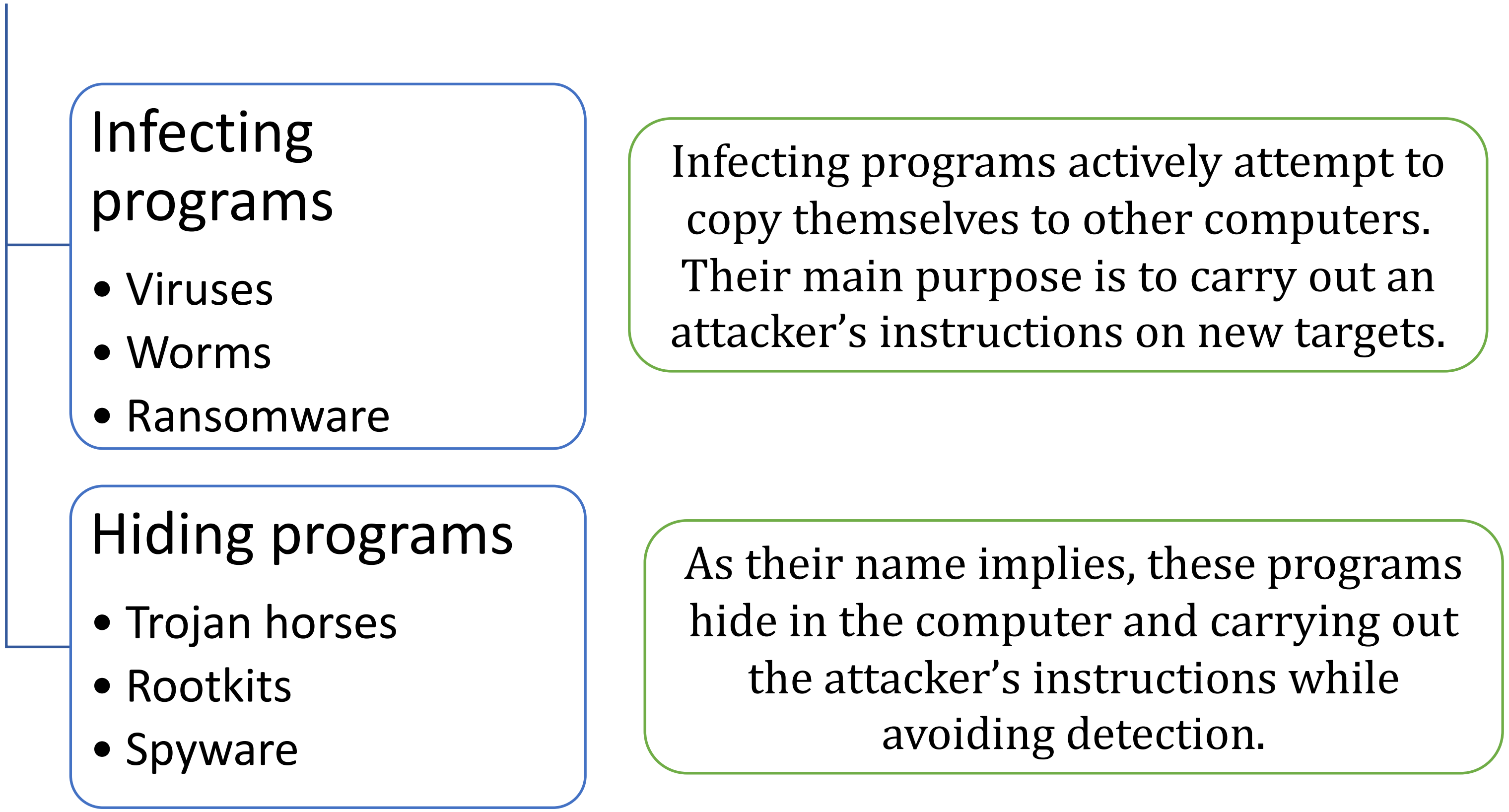
1. Malicious software
2. Hardware or software failure
3. Human error/mistakes
4. Internal attacker
5. Equipment theft
6. External attacker
7. Natural disaster
8. Terrorism

Malicious software

- Some software infiltrates one or more target computers and follows an attacker's instructions.
- These instructions can include causing damage, escalating security privileges, revealing private data, or even modifying or deleting data.
- This type of software called **Malicious software**, or **Malware** for short.
- The purpose of malware is to damage or disrupt a system.

Malicious software

Exists in two main categories.



Infecting programs

- Viruses
- Worms
- Ransomware

Infecting programs actively attempt to copy themselves to other computers. Their main purpose is to carry out an attacker’s instructions on new targets.

Hiding programs

- Trojan horses
- Rootkits
- Spyware

As their name implies, these programs hide in the computer and carrying out the attacker’s instructions while avoiding detection.

Malicious software

- **Viruses** - A computer virus is a software program that attaches itself to or copies itself into another program on a computer. The purpose of the virus is to trick the computer into following instructions that were not intended by the original program developer.

- **Worms** - A worm is a self-contained program that replicates and sends copies of itself to other computers, generally across a network, without any user input or action. The main difference between a virus and a worm is that a worm does not need a host program to infect. The worm is a standalone program.

Malicious software

- **Trojan Horses** - A Trojan horse, also called a Trojan, is malware that masquerades as a useful program and trick users into running them. Today's Trojans do far more than just save copies of themselves. Trojans can hide programs that collect sensitive information, open backdoors into computers, or actively upload and download files.

- **Rootkits** - A rootkit modifies or replaces one or more existing programs to hide traces of attacks. Although rootkits commonly modify parts of the operating system to conceal traces of their presence, they can exist at any level—from a computer's boot instructions up to the applications that run in the operating system. Rootkits provide attackers with easy access to compromised computers to launch additional attacks.

Malicious software

- **Spyware** - Spyware is a type of malware that gathers information about a user through an Internet connection, without his or her knowledge.

- **Ransomware** - Ransomware attacks a computer and limits the user’s ability to access the computer’s data. Then the attacker demands a payment to restore full access. The demand for a payment, or *ransom*, gives this type of malware its name. Many current ransomware programs operate by encrypting important files or even the entire disk and making them inaccessible.

Watch - https://www.youtube.com/watch?v=n8mbzU0X2nQ

Hardware or software failure

- Hardware failure - A malfunction within the electronic circuits or electromechanical components (disks, tapes) of a computer system.

  Possible reasons for failure -

  - Electricity interruptions
  - Overheating
  - Improper grounding of equipment etc.

- Software failure - The inability of a program to continue processing due to erroneous logic.

  Possible reasons for failure -

  - Bad logic in code
  - Incorrect formula
  - Data type mismatch
  - Inadequate computer resources etc.

Human errors or mistakes

The user is the weakest link in security. Even information systems security practitioners can make mistakes. Human error is a major risk and threat to any organization. No group can completely control any person's behavior.

E.g. –

- The use of weak passwords
- Sending sensitive information to the wrong recipients
- Sharing password/account information with unauthorized parties
- Installation of unauthorized, unregistered software (application and OS)
- The unmonitored download of files from the Internet
- Falling for phishing scams
- Coding mistakes
- Email misdelivery

A **phishing** email is a fake or bogus email to trick the recipient into clicking on an embedded URL link or opening an email attachment.

Internal Attacker

An internal attacker is an individual or a group within an organization seeks to ruin operations or misuse organizational assets through its computer systems.

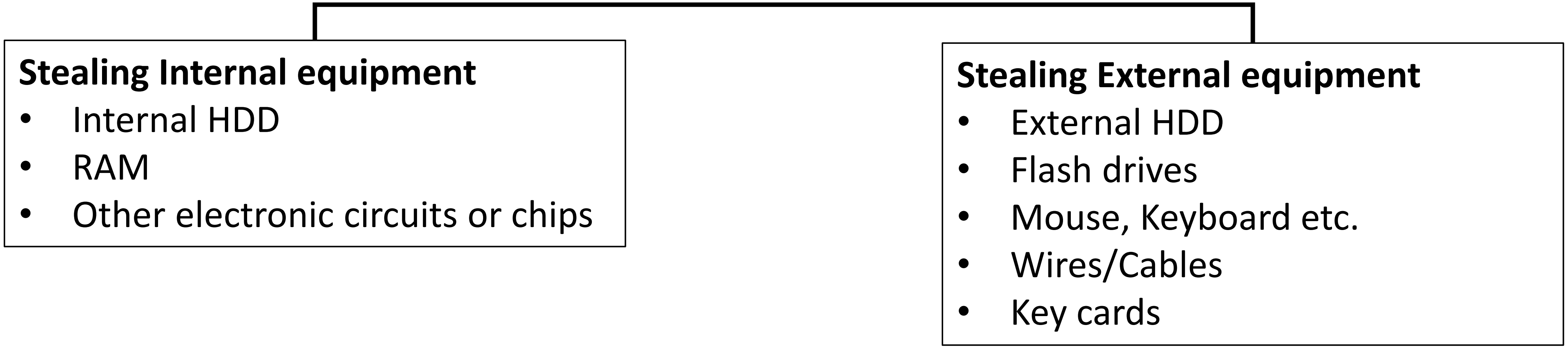
Typically involves a current or former employee, or business associate who has access to sensitive information within the network of an organization.

An internal attacker would perform following activities such as,

- Downloading or accessing substantial amounts of data
- Sharing sensitive data outside the organization
- Attempts to bypass security
- Accessing sensitive data not associated with their job function
- Run personal applications on organization's systems/computers

Equipment theft

Act of stealing computer(hardware) equipment.



Stealing Internal equipment

- Internal HDD
- RAM
- Other electronic circuits or chips

Stealing External equipment

- External HDD
- Flash drives
- Mouse, Keyboard etc.
- Wires/Cables
- Key cards

Equipment theft can occur with the intention of selling stolen equipment or selling sensitive data outside the organization.

External Attacker

An external attacker is an individual or a group from outside an organization seeks to ruin operations or misuse organizational assets through its computer systems.

Following type of methods use by an external attacker to hack, damage or disrupt a system.

- Phishing
- Keystroke loggers
- Botnets
- DOS (Denial of Service) attacks
- Man-in-the-middle attacks
- Social Engineering

External Attacker

Phishing - Phishing is an attempt to commit identity theft via email or instant message. The message appears to come from a legitimate source, such as a trusted business or financial institution, and includes an urgent request for personal information. Phishing messages usually indicate a critical need to update an account (banking, credit card, etc.) immediately. The message instructs the victim to either provide the requested information or click on a link provided in the message.

Watch - https://www.youtube.com/watch?v=BnmneAjVrM4&list=PLPmbqO785Hlu-lW7655fc7XxzjGBSdiut&index=25

Keystroke loggers - a keystroke logger captures keystrokes, or user entries. The keystroke logger then forwards that information to the attacker. This enables the attacker to capture logon information, banking information, and other sensitive data.

External Attacker

DoS (Denial of Service) attacks - purpose of a denial of service (DoS) attack is to overwhelm a server or network segment to the point that the server or network becomes unusable. A successful DoS attack crashes a server or network device or creates so much network congestion that authorized users cannot access network resources.

Watch - https://www.youtube.com/watch?v=yLbC7G71IyE&list=PLPmbqO785Hlu-lW7655fc7XxzjGBSdiut&index=24

Botnets – (short for ‘robotically controlled networks’). A botnet consists of a network of compromised computers that attackers use to launch attacks and spread malware. Attackers can use botnets to distribute malware and spam and to launch DoS attacks against organizations or even countries.

Watch - https://www.youtube.com/watch?v=3BbxUCOFX8g&list=PLPmbqO785Hlu-lW7655fc7XxzjGBSdiut&index=22

External Attacker

Man-in-the-middle attacks - In this type of attack, an attacker intercepts messages between two parties before transferring them on to their intended destination. Attackers use man-in-the-middle attacks to steal information, to corrupt transmitted data, to gain access to an organization’s internal computer and network resources, and to introduce new information into network sessions.

Social Engineering - Social engineering is the art of one human attempting to deceive another human into doing something or exposing information. This involves tricking authorized users into carrying out actions for unauthorized users.

Watch - https://www.youtube.com/watch?v=lc7scxvKQOo

Who is a Hacker?

Hacker is a person who enjoys exploring and learning how to modify something, particularly related to computer systems.

Types of Hackers

- **Black-hat hackers** - A black-hat hacker tries to break IT security and gain access to systems with no authorization in order to gain financial benefits, revenge or simply prove technical ability.

- **White-hat hackers** - A white-hat hacker, or ethical hacker, is an information systems security professional who has authorization to identify vulnerabilities and perform penetration testing.

- **Gray-hat hackers** - may set out to find vulnerabilities in a system but they will only report their findings to the owners of a system if doing so coincides with their agenda. Or they might even publish details about the vulnerability on the internet so that other attackers can exploit it.

Watch Later

https://www.youtube.com/watch?v=opRMrEfAIiI&t=3s

https://www.youtube.com/watch?v=j0EZpH_eIsY

Strategies for securing Information Systems

1. Authentication
2. Access Control
3. Encryption
4. Backups
5. Firewalls
6. Intrusion Detection Systems
7. Physical Security
8. Security Policies
9. Anti-malware programs
10. Security Awareness Training

Authentication

is the process or action of verifying the identity of a user.

Authentication can be accomplished by identifying someone through one or more of three factors:

1. Something they know (Ex – Username, Password, Pin number etc.)
2. Something they have (Ex- Key cards, Secure Tokens, Phone APPs etc.)
3. Something they are (Ex- Fingerprint, Facial geometry, Eye scan etc. - **Biometrics**)

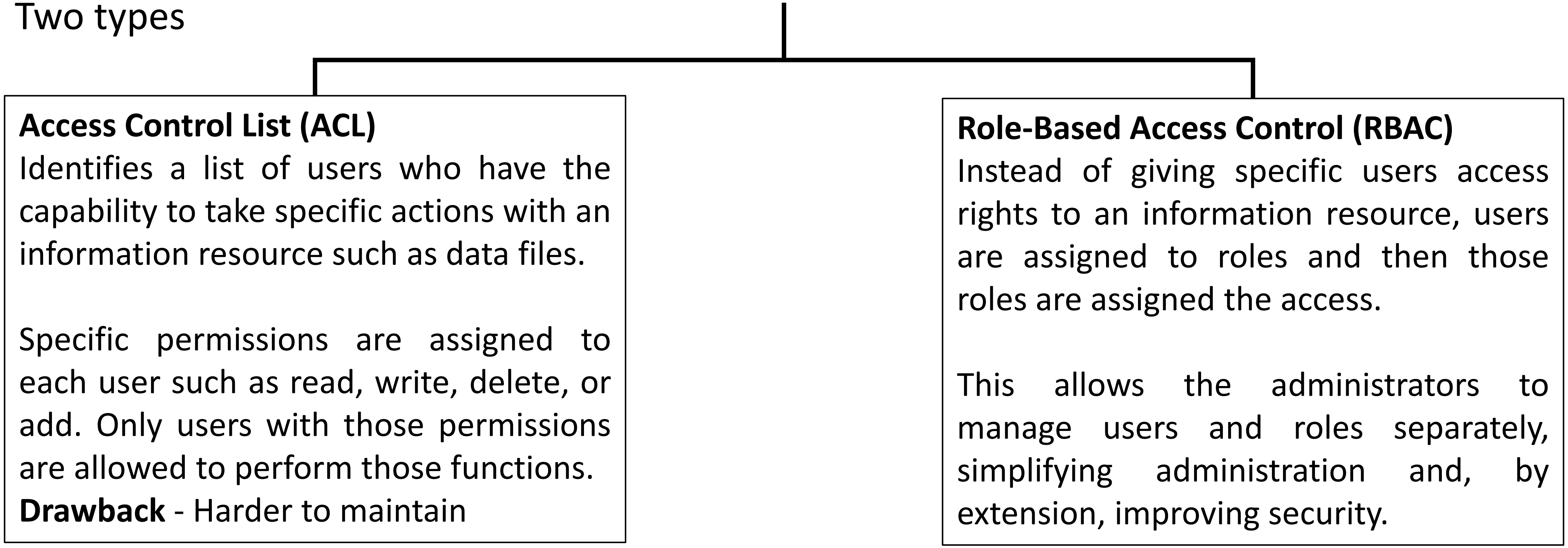
A more secure way to authenticate a user is through *multi-factor authentication*. By combining two or more of the factors listed above, it becomes much more difficult for someone to misrepresent themselves.

Example – Log in to your Gmail account using both Password and OTP received to your phone.

Access Control

Once a user has been authenticated, the next step is to ensure that they can only access the information resources that are appropriate. This is done through the use of *access control*. Access control determines which users are authorized to read, modify, add, and/or delete information.

- Two types



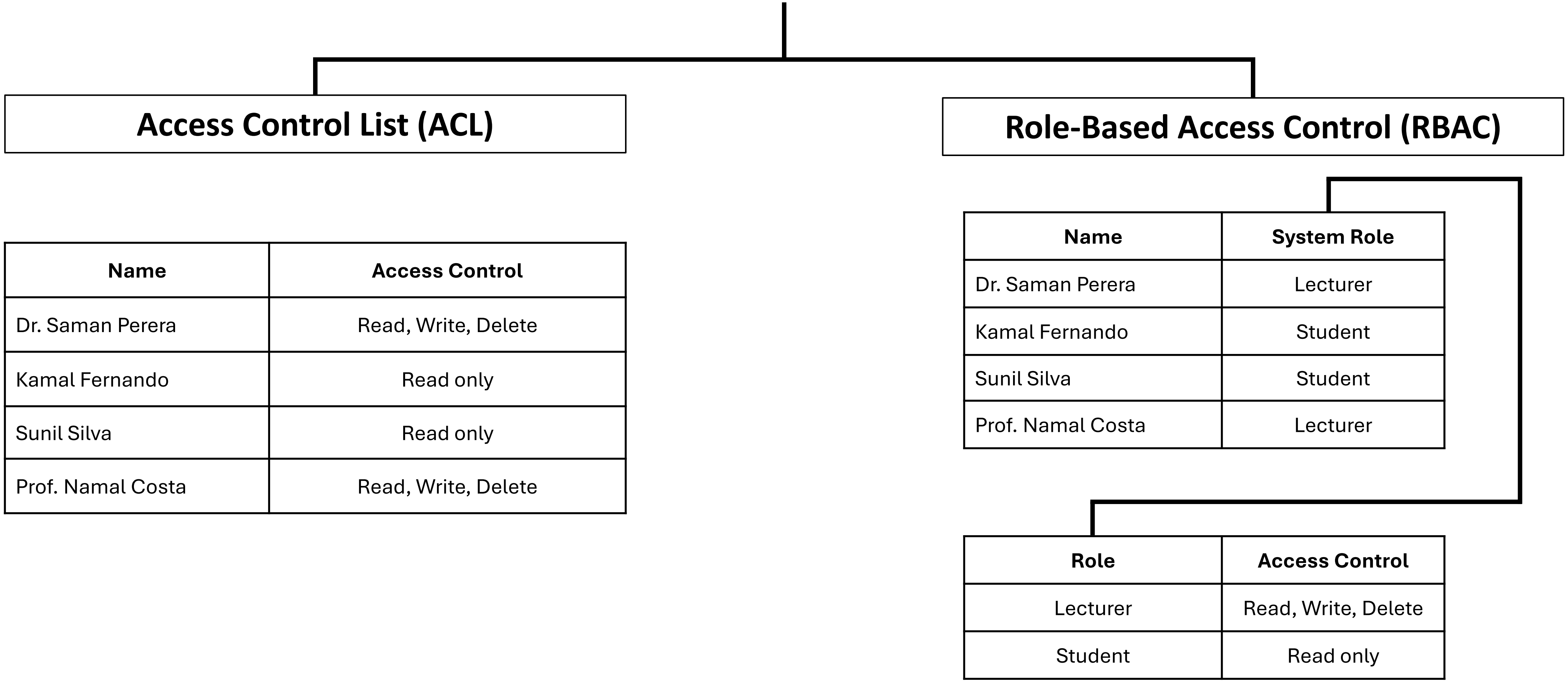
Access Control List (ACL)
Identifies a list of users who have the capability to take specific actions with an information resource such as data files.

Specific permissions are assigned to each user such as read, write, delete, or add. Only users with those permissions are allowed to perform those functions.
Drawback - Harder to maintain

Role-Based Access Control (RBAC)
Instead of giving specific users access rights to an information resource, users are assigned to roles and then those roles are assigned the access.

This allows the administrators to manage users and roles separately, simplifying administration and, by extension, improving security.

Access Control (Cntd.)



Access Control List (ACL)

Name	Access Control
Dr. Saman Perera	Read, Write, Delete
Kamal Fernando	Read only
Sunil Silva	Read only
Prof. Namal Costa	Read, Write, Delete

Role-Based Access Control (RBAC)

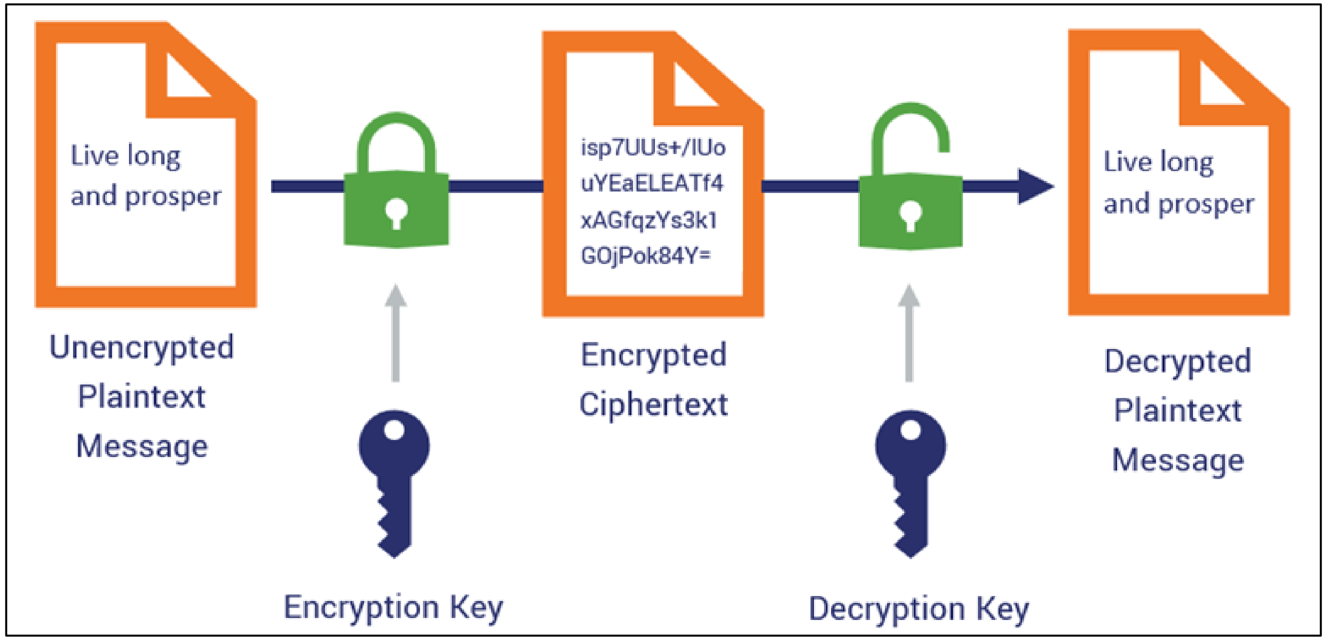
Name	System Role
Dr. Saman Perera	Lecturer
Kamal Fernando	Student
Sunil Silva	Student
Prof. Namal Costa	Lecturer

Role	Access Control
Lecturer	Read, Write, Delete
Student	Read only

Encryption

Encryption is a process of encoding data upon its transmission or storage so that only authorized individuals can read it.

This encoding is accomplished by software which encodes the plain text that needs to be transmitted (encryption). Then the recipient receives the cipher text and decodes it (decryption).

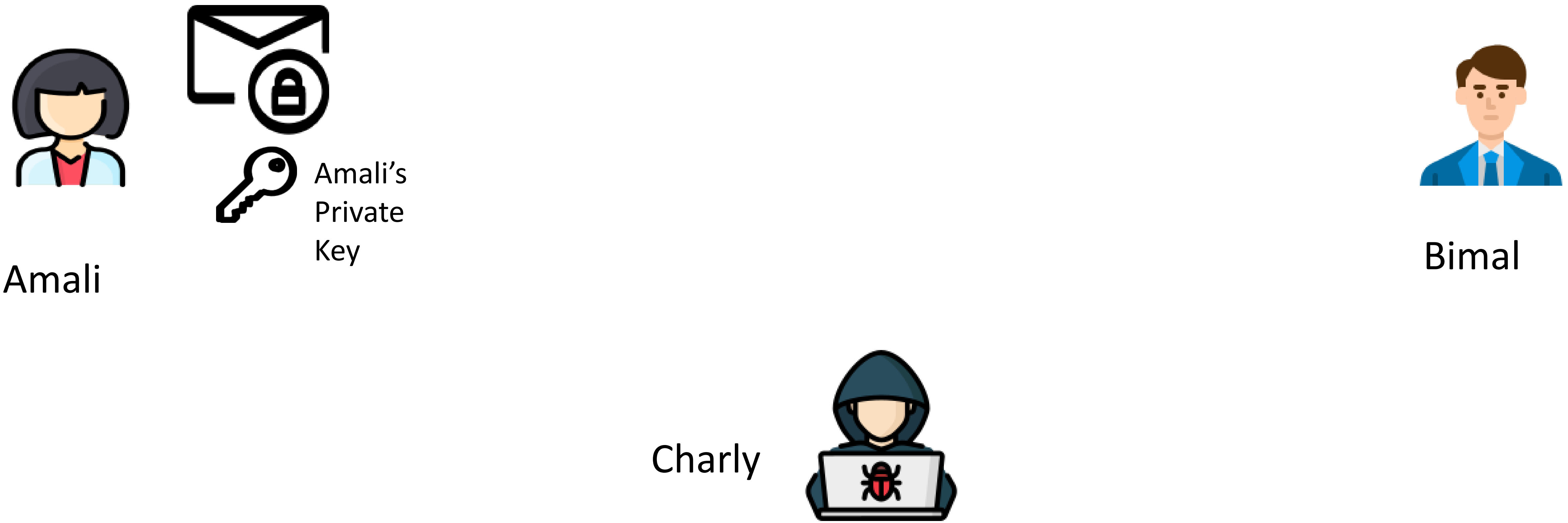


Watch - https://www.youtube.com/watch?v=6-JjHa-qLPk

Types of Encryption

Watch - https://www.youtube.com/watch?v=AQDCe585Lnc
Refer - Thunderbird help: https://www.howtogeek.com/706402/how-to-use-openpgp-encryption-for-emails-in-thunderbird/

1. **Symmetric** vs Asymmetric (Encryption) – (Private Key Encryption)



Amali

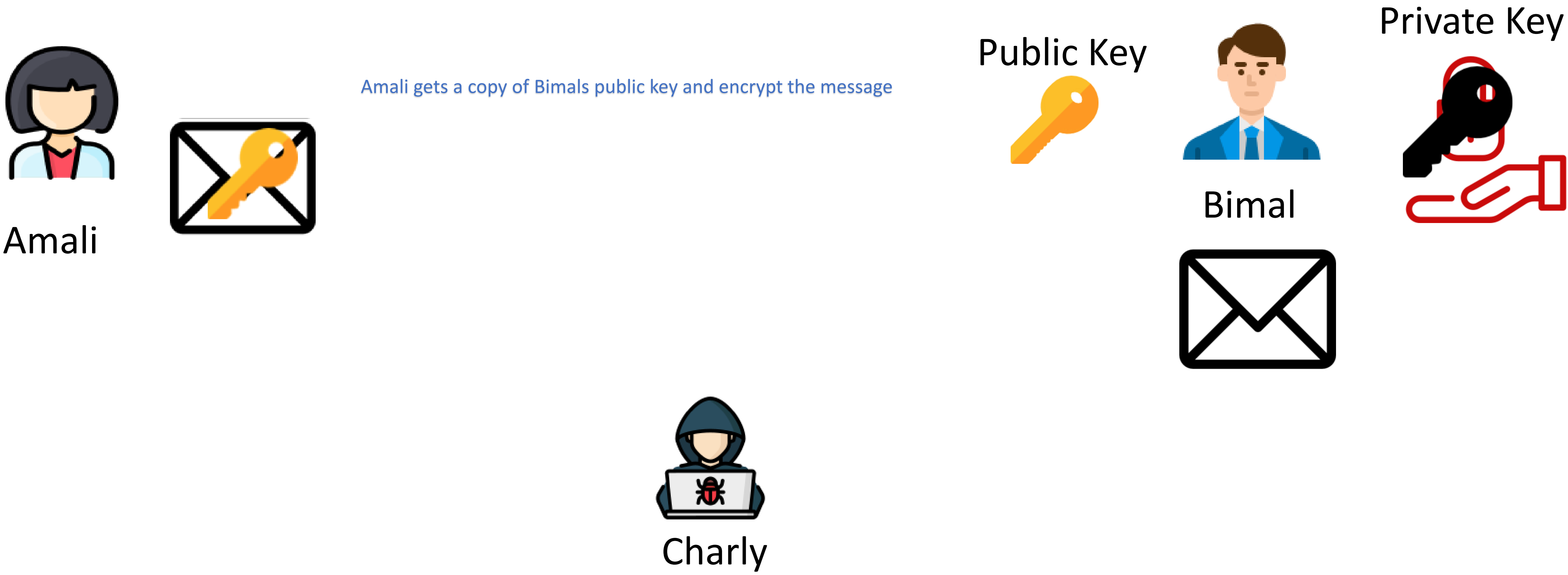
Amali's Private Key

Bimal

Charly

Types of Encryption

2. Symmetric vs **Asymmetric (Encryption) –** (Public Key Encryption)



Amali gets a copy of Bimals public key and encrypt the message

Amali

Public Key

Bimal

Private Key

Charly

Digital certificate

- Digital certificates are electronic credentials that bind the identity of the certificate owner to a pair of electronic encryption keys, (one public and one private), that can be used to encrypt and sign information digitally.

- A digital certificate is a pair of Keys (= Passwords) issued by a trusted certificate authority (CA).

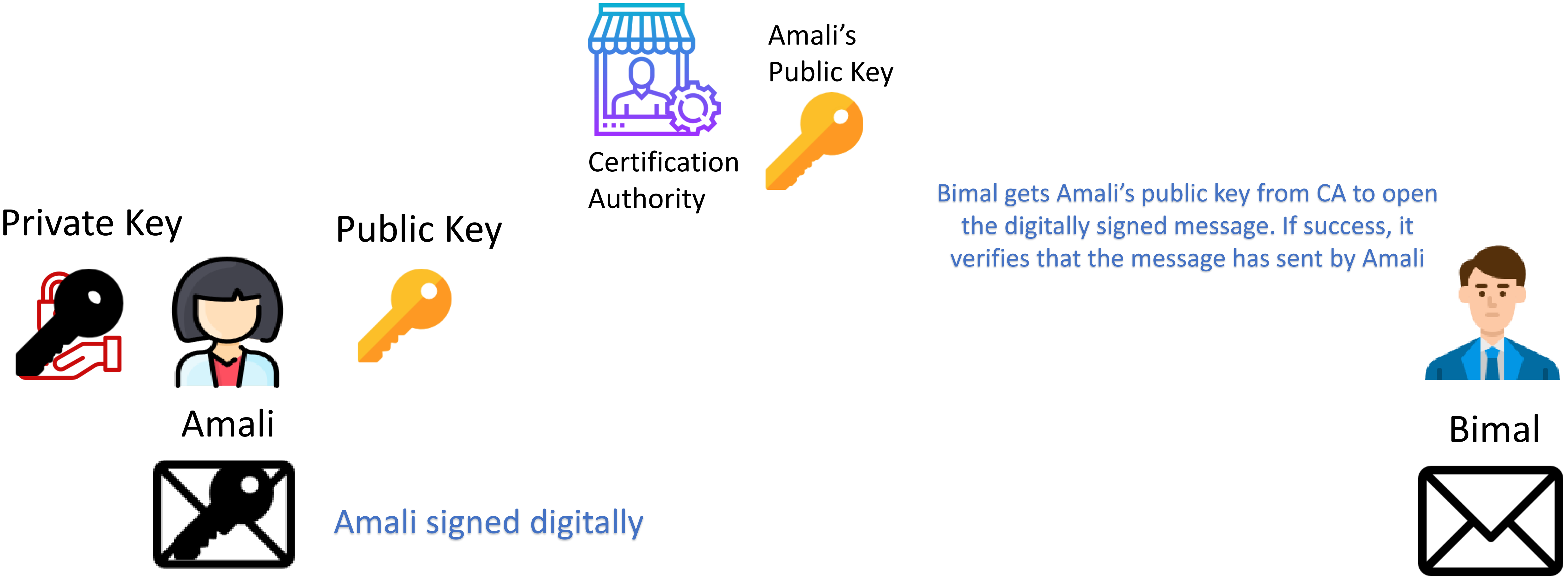
Private Key

Amali

Public Key

Certification Authority / Software

Asymmetric Encryption (use as a Digital Signature)



Certification Authority

Amali's Public Key

Private Key

Public Key

Amali

Bimal gets Amali's public key from CA to open the digitally signed message. If success, it verifies that the message has sent by Amali

Bimal

Amali signed digitally

Backups

Process of keeping a copy of a file or other item of data made, on an alternative location, in case the original is lost or damaged.

Not only should the data on the corporate servers be backed up, but individual computers used throughout the organization should also be backed up.

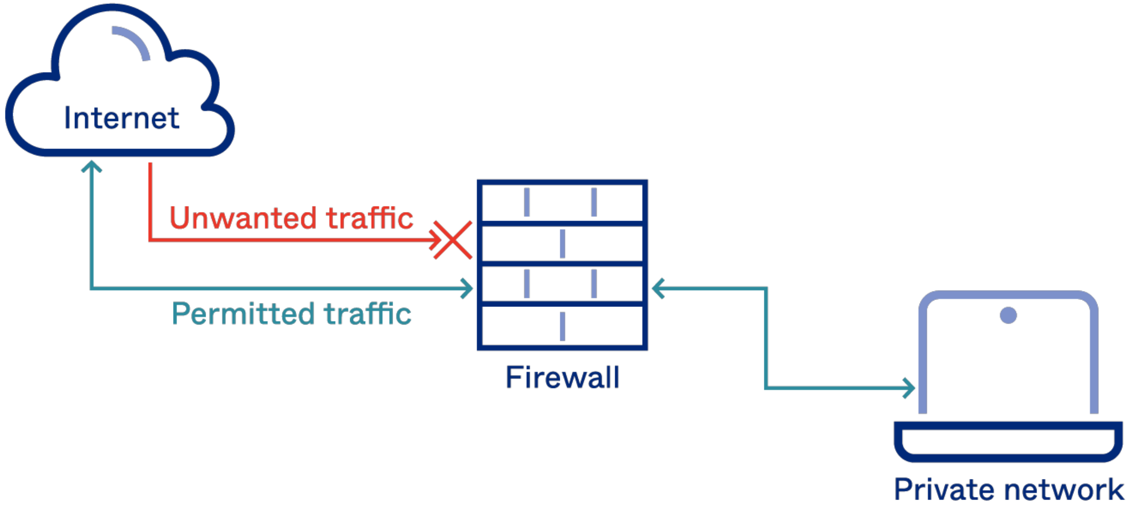
A good backup plan should consist of following components.

- Full understanding of the organization’s information resources.
- Regular backups of all data.
- Offsite storage (Ex- Cloud storage) of backup data sets.
  - Ex- Google Drive, One Drive etc.
- Test of data restoration.

Firewalls

A **firewall** is a program or dedicated hardware device that inspects network traffic passing through it and denies or permits that traffic based on a set of rules you determine at configuration.

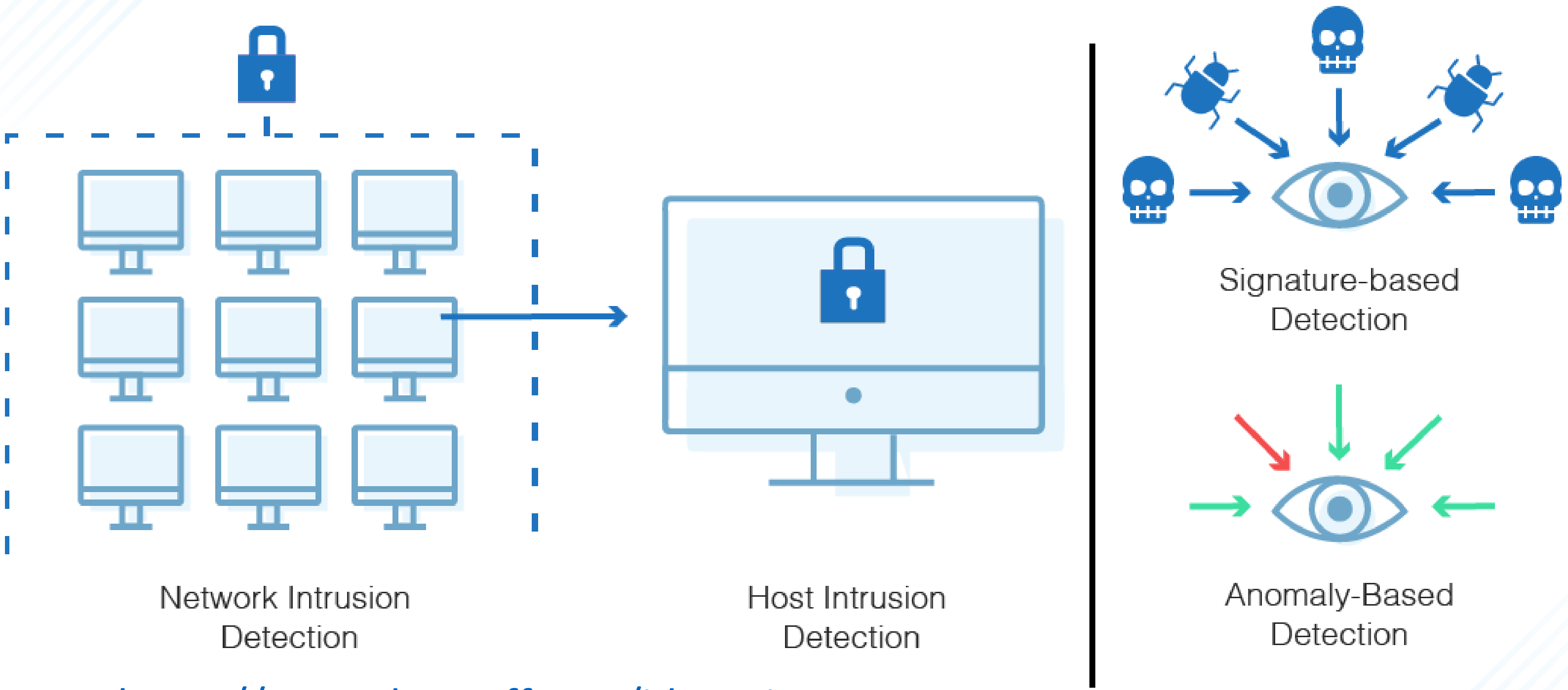
A firewall protects all company servers and computers by stopping packets from outside the organization's network that do not meet a strict set of criteria. A firewall may also be configured to restrict the flow of packets leaving the organization.



Watch - https://www.youtube.com/watch?v=kDEX1HXybrU

Intrusion Detection Systems

Intrusion Detection Systems (IDS) can be placed on the network for security purposes. An IDS does not add any additional security. Instead, it **provides the capability to identify if the network is being attacked**. An IDS can be configured to watch for specific types of activities and then alert security personnel if that activity occurs. An IDS also can log various types of traffic on the network for analysis later. It is an essential part of any good security system.



Source - https://www.dnsstuff.com/ids-vs-ips

Physical Security

Physical security is the protection of the actual hardware and networking components that store and transmit information resources. To implement physical security, an organization must identify all of the vulnerable resources and take measures to ensure that these resources cannot be physically tampered with or stolen.

These measures include the following.

- Locked doors.
- Physical intrusion detection.
- Secured equipment.
- Environmental monitoring.
- Employee training.
- Uninterruptible power supply (UPS) and/or a backup power generator to keep systems going in the event of a power failure.
- Fire prevention systems.
- Surge protectors to minimize the effect of power surges on delicate electronic equipment.

Security Policies

- Besides the technical controls listed above, organizations also need to implement security policies as a form of administrative control.
- A good information security policy lays out the guidelines for employee use of the information resources of the company and provides the company with the action to be taken in the event that an employee violates a policy.
- Policies require compliance. Failure to comply with a policy will result in disciplinary action.
- A security policy should also address any governmental or industry regulations that apply to the organization. For example, any business organization in Sri Lanka must be aware of the ‘Personal Data Protection Act, No. 9 of 2022’, which applies to any processing of personal information by organizations that takes place in Sri Lanka.

Example of a Security Policy - https://itsecurity.uiowa.edu/university-it-policy

Security Policies (Cont.)

Security policy may include the following

- Acceptable usage policy
- Email protection policies
- Mobile device policy
- Password Creation and Management Policy
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Email/communication policy
- Remote access policy etc.

Anti-malware programs

- is a computer program used to prevent, detect, and remove malware.

Many anti-malware products are available to prevent the spread of all types of malware as well remove malware from infected computers. These include the following:

- BitDefender—www.bitdefender.com
- Kaspersky Anti-Virus—www.kaspersky.com
- Norton AntiVirus—www.symantec.com/norton/antivirus
- ESET Nod32 Antivirus—www.eset.com
- AVG Antivirus—www.avg.com
- McAfee Endpoint Protection—www.mcafee.com

Security Awareness Training

Every organization, regardless of the industry vertical or regulatory compliance law requirement, must have a new-hire and ongoing or annual security awareness training program.

This security awareness training course must be part of an organization’s security awareness campaign. A security awareness campaign consists of training, periodic newsletters or memos, “lunch and learn” training sessions, and security incidents that are opened as a result of a security policy violation.

References

Kim, D., & Solomon, M. (2018). Fundamentals of information systems security (Third edition). Jones & Bartlett Learning

Thank You