Operating System

BIM IV Semester

Credits: 3

Lecture Hours:48

Er. Santosh Bhandari,
(Master Computer Science)

Unit–7

Operating System Security

Introduction

What is Operating System Security?

-The process of ensuring OS availability, confidentiality, integrity is known as operating system security.

-OS security refers to the processes or measures taken to protect the operating system from dangers, including viruses, worms, malware, and remote hacker intrusions.

-Operating system security comprises all preventive-control procedures that protect any system assets that could be stolen, modified, or deleted if OS security is breached.

Essential requirements of security

Security Principles:

1. **Privacy/Confidentiality**
2. **Integrity**
3. **Availability**
4. **Authentication/Authenticity**
5. **Non-repudiation**
6. **Encryption**
7. **Auditability**

Essential requirements E-commerce of security:

Privacy/Confidentiality – Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.

Integrity – Information should not be altered during its transmission over the network.

Availability – Information should be available wherever and whenever required within a time limit specified.

Authenticity – There should be a mechanism to authenticate a user before giving him/her an access to the required information.

Essential requirements of security:

Non-Repudiation – It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.

Encryption – Information should be encrypted and decrypted only by an authorized user.

Auditability – Data should be recorded in such a way that it can be audited for integrity requirements.

Types of violations

1. Virus
2. Worm
3. Logic Bomb
4. Trojan/Backdoor
5. Rootkit
6. Advanced Persistent Threat
7. Spyware and Adware
8. Ransomware
9. Keyloggers
10. Fileless Malware
11. Cryptojacking
12. Hybrid Malware
13. DOS Attack
14. DDoS Attack
15. SQL Injection

Types of violations

1. Program threats

Below are some program threats.

Virus: A virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system.

Trojan Horse: A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game.

Logic Bomb: A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens.

Types of violations

2. System Threats

Below are some system threats.

Worm: Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas.

Denial of Service: Denial of Service (DoS) is a cyber-attack on an individual Computer or Website with the intent to deny services to intended users. Their purpose is to disrupt an organization’s network operations by denying access to its users.

Authentication and authorization mechanism

1. Authentication

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

Authentication Factors:

- Password or PIN
- Bio-metric measurement (fingerprint & retina scan)
- Card or Key

Authentication and authorization mechanism

Authentication Mechanism:

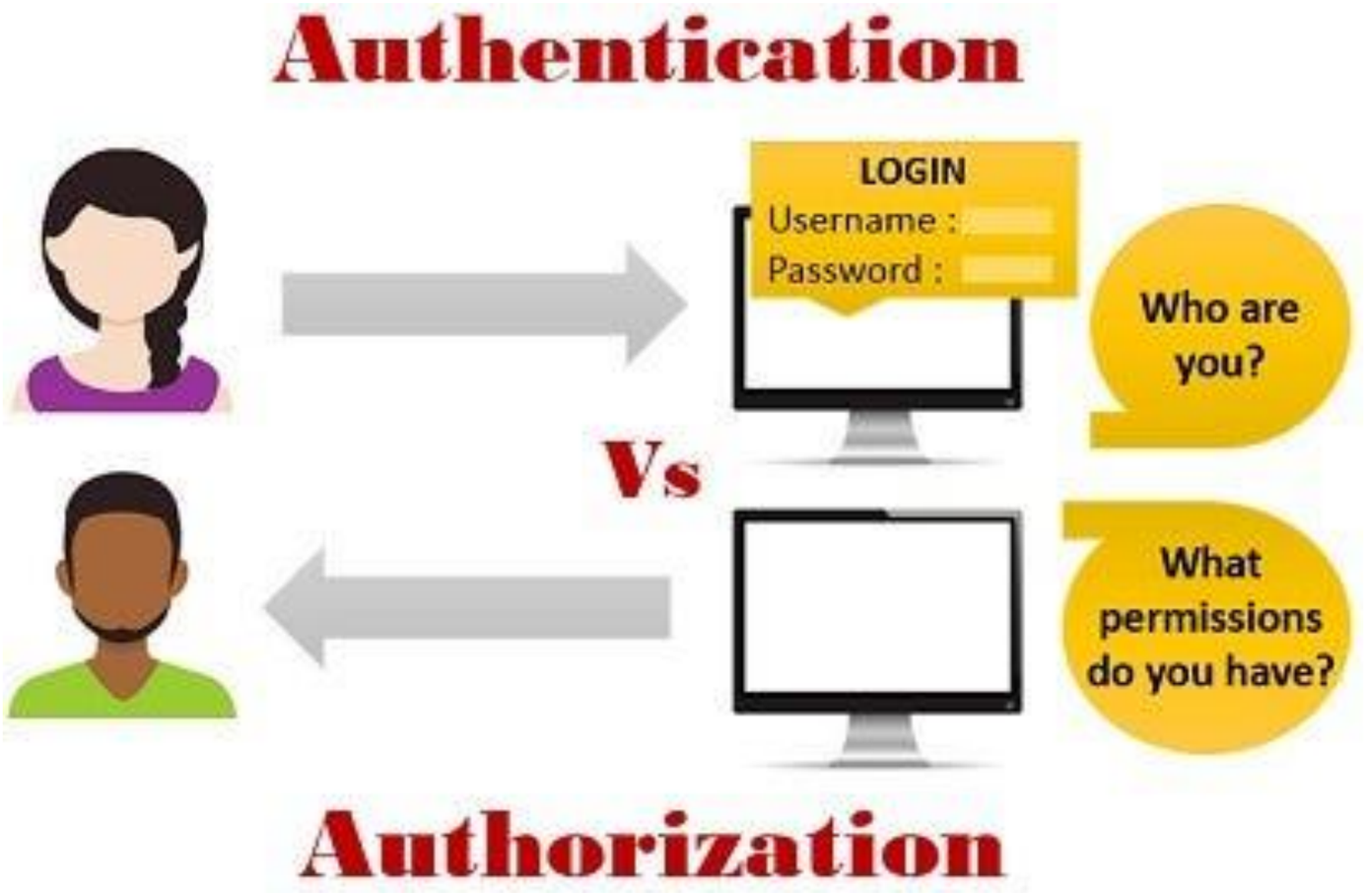
- Two-factor authentication
- Multi-factor authentication
- one-time password
- Three-factor authentication
- Bio metrics
- Hard Tokens: hardware token (OTP)
- Soft Tokens: software tokens (fingerprints to access phone)
- Contextual Authentication: (verify the context of user i.e. IP, location before providing access)
- Device identification

Authentication and authorization mechanism

2. Authorization:

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

Authentication vs. Authorization



Access control

Access Control:

-Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources.

-Secure access control uses policies that verify users are who they claim to be and ensures appropriate control access levels are granted to users.

-Access control is a security technique that has control over who can view different aspects, what can be viewed and who can use resources in a computing environment.

Access control

Access control is a security technique that regulates who or what can view or use resources in a computing environment.

There are two types of access control:

1. Physical access control: Physical access control limits access to campuses, buildings, rooms, and physical IT assets.

2. Logical access control: Logical access control limits connections to computer networks, system files, and data. Logical access control systems perform identification authentication and Authorization of users

Information system controls

Information Systems controls are a set of procedures and technological measures to ensure secure and efficient operation of information within an organization.

They are two types:

1. General control
2. Application controls

Both are used for safeguarding information systems.

Information system controls

1. General Controls

-These controls apply to information systems activities throughout an organization. The most important general controls are the measures that control access to computer systems and the information stored or transmitted over telecommunication networks.

Some general controls are as follows.

1. Software Controls – Monitor the use of system software and prevent unauthorized access of software programs, system failure and computer programs.

2. Hardware Controls – Ensure the computer hardware is physically secure and check for equipment malfunctions. Organizations should make provisions for backup or continued operation to maintain constant service.

Information system controls

3. Computer Operations Controls – This include controls over setup of computer processing jobs and computer operations and backup and recovery procedures for processing that ends abnormally.

4. Data Security Controls – Ensures critical business data on disk and tapes are not subject to unauthorized access, change or destruction while they are in use or in storage.

5. Implementation Controls – Audit the system development process at various points to ensure that the process is properly controlled and managed.

6. Administrative Controls – Formalize standards, rules, procedures and control discipline to ensure that the organization’s general and application controls are properly executed and enforced.

Information system controls

2. Application controls

Application controls are specific to a given application and include measures as validating input data, regular archiving copies of various databases, and ensuring that information is disseminated only to authorized users.

This can be classified as input, processing and output controls.

1. Input Controls – Input controls check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing and error handling.

2. Processing Controls – Processing controls establish that data are complete and accurate during updating. Run control totals, computer matching, and programmed edit checks are used as processing controls.

3. Output Controls –Output controls ensure that the results of computer processing are accurate, complete and properly distributed.

Security Model

A security model is a framework in which a security policy is developed. The development of this security policy is geared to a particular setting or instance of a policy, for example, a security policy based upon authentication, but built within the confines of a security model.

CIA

CIA security triad

-The CIA Triad is a model for the development of security policies.
-CIA is three foundational **information security principles**.

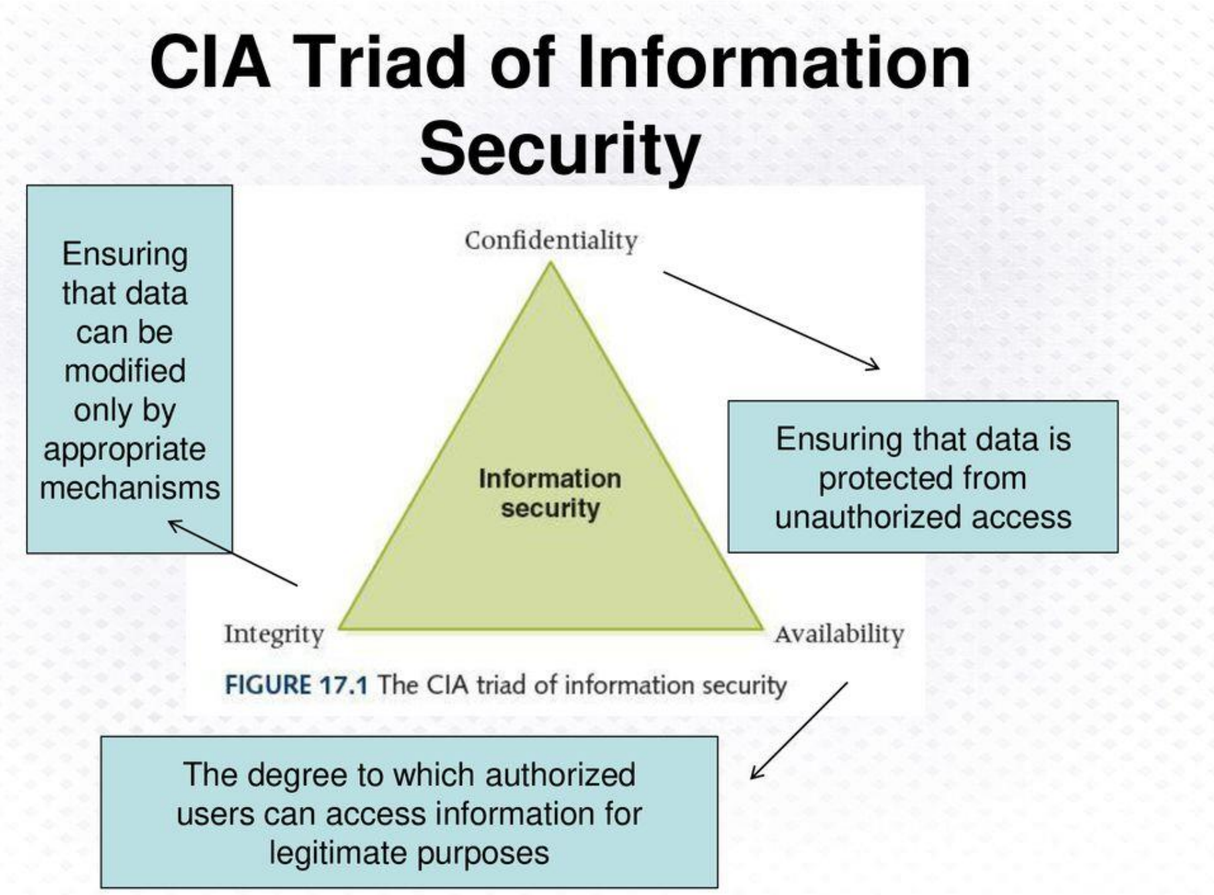


FIGURE 17.1 The CIA triad of information security

CIA security triad

Confidentiality: -Confidentiality refers to an organization's efforts to keep their data private or secret.
-Ensuring that *only those who are authorized have access to specific assets* and that *those who are unauthorized are actively prevented from obtaining access*.

Example: only authorized Payroll employees should have access to the employee payroll database.

Confidentiality

Confidentiality violation countermeasures:

-Uses encryption to encrypt and hide data.

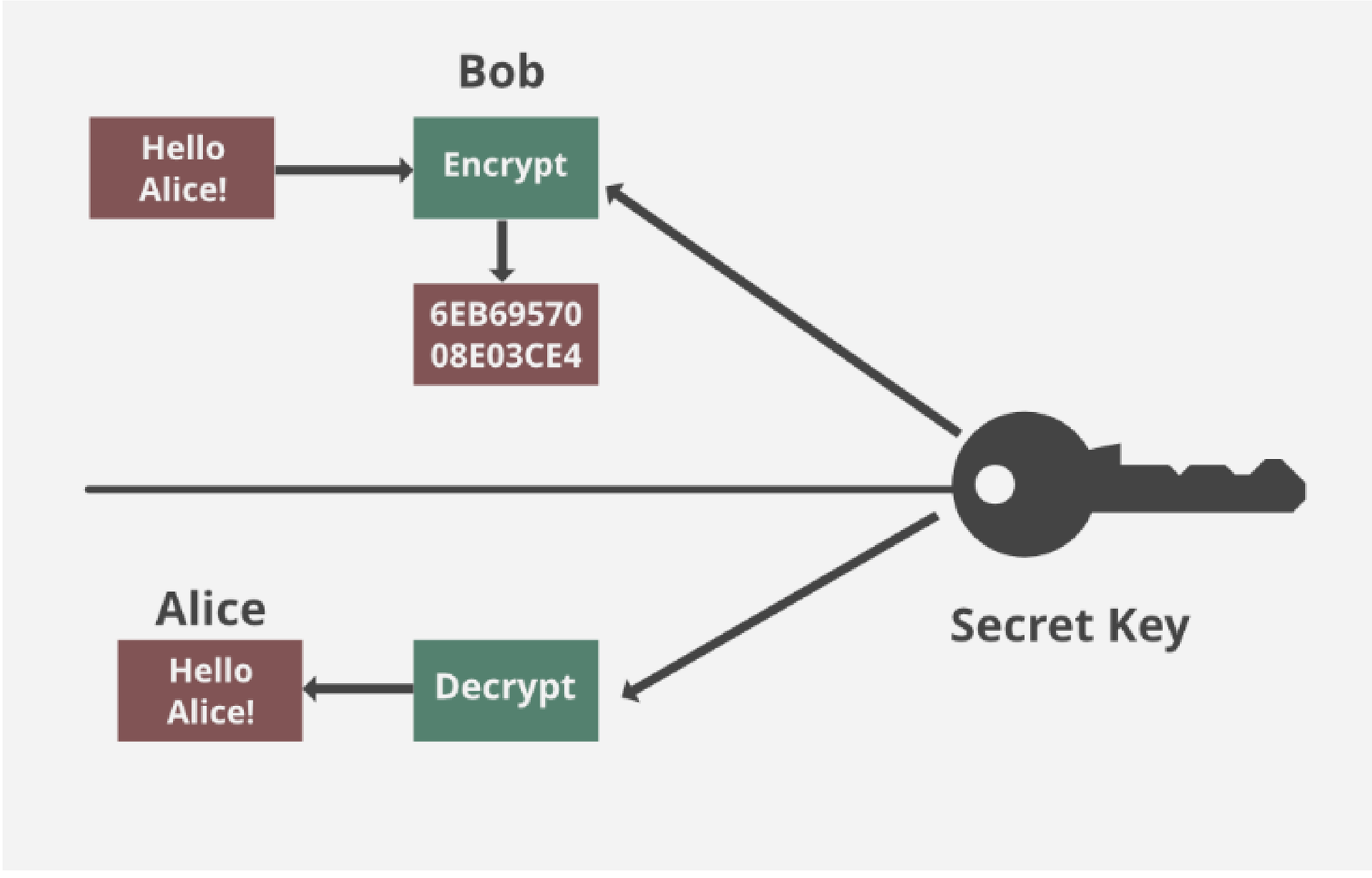
-Data classification and labeling

-strong access controls and authentication mechanisms

-Encryption of data in process, in transit, and in storage;

-Adequate education and training for all individuals

Confidentiality



Integrity

-Integrity involves making sure your data is **trustworthy** and free from tampering.

- Ensuring integrity involves protecting data in use, in transit (such as when sending an email or uploading or downloading a file), whether on a laptop, a portable storage device, in the data center, or in the cloud.
-Integrity is about *ensuring that data* ***has not been tampered with and, therefore, can be trusted.*** *It is correct, authentic, and reliable*.

Example, ecommerce buyer expect product and pricing information to be accurate, and that pricing, availability, and other information will not be altered after they place an order.

Integrity

Integrity Violation Countermeasure:

-Use hashing, encryption, digital certificates, or digital signatures.

-Intrusion detection systems, auditing, version control

-Use strong authentication mechanisms and access controls.

Availability

-Availability means that *networks, systems, and applications are up and running*.

-It ensures that *authorized users have timely, reliable access to resources when they are needed*.

Availability : Violations

-Availability can also be compromised through use of denial-of-service (DoS) attacks or ransomware.

-Hardware or software failure, power failure, natural disasters, and human error.

Availability

Availability violation countermeasure

-Providing multiple paths for traffic, so that data can keep flowing even in the event of a failure.

-Backups and full disaster recovery plans also help a company regain availability soon after a negative event.

-Regular software patching and system upgrades

Find me

9851083215

Santosh.it288@mail.com

www.phtechno.com

Kathmandu