WEEK-8

COMPUTER NETWORKS AND SECURITY ETHICS

(Threats, Mitigation)

Dr Eric Opoku Osei

NETWORK SECURITY & ETHICS

FACTORS OF A TRUSTED COMPUTER NETWORK

A dependable and trusted system should include:

Confidentiality: No unauthorized disclosure of information

Integrity: No accidental or malicious alterations of information have been performed (even by authorized entities)

Availability: Accessible and usable upon demand for authorized entities

Reliability: Continuity of service delivery (Cloud servers

Safety: Very low probability of catastrophes

NETWORK SECURITY THREATS & ETHICS ISSUES

Four (4) types of security threats:

1. Interception: Refers to the situation that an unauthorized party has gained access to a service or data.

2. Interruption: Refers to the situation in which services or data become unavailable, unusable, or destroyed.

3. Modification: Involves unauthorized changing of existing data or tampering with a service.

4. Fabrication: Refers to the situation in which additional data or activity are generated that originally did not exist.

EXAMPLES OF SECURITY THREATS

Interception

- Transmission Channel: Reading the content of transferred messages
- Database Object: Reading the data contained in an object

Interruption

- Transmission Channel: Preventing message transfer
- Database Object: Denial of service

Modification

- Transmission Channel: Changing message content
- Database Object: Changing an object's encapsulated data

Fabrication

- Transmission Channel: Inserting messages
- Database Object: Spoofing an object . Spoof is to imitate or exaggerate.

SECURITY MECHANISM TO REDUCE VIOLATION

A **security policy** describes which actions are allowed and which are prohibited. To protect against security threats, we have a number of **security mechanisms** at our disposal:

- **Encryption**: Transform data into something that an attacker cannot understand (confidentiality). It is also used to check whether something has been modified (integrity).
- **Authentication**: Verify the claim that a subject says it is : verifying the identity of a subject.

  (username & password, cards, eye/retina scans, voice recognition, and fingerprints)
- **Authorization**: After Authentication; Determining whether a subject is permitted to make use of certain data in the system or services. *(File access hierarchy)*
- **Auditing**: Trace which subjects accessed what file, and in which way. Useful only if it can help catch an attacker. (Log tray auditing)

- NB: Authorization makes sense only if the requesting subject has been authenticated.

THANK YOU