LECTURE1 SUPPLEMENTARY MATERIAL

Dr. Asem Kitana

CSEC1310

Cybersecurity

- Cybersecurity is the practice of deploying people, policies, processes and technologies to ***protect*** organizations, their critical systems and sensitive information from digital attacks.
- To achieve the cybersecurity goal, different models could be implemented, such as:
- CIA Model
- AAA Model

CIA Model

- CIA is an essential cybersecurity model that consists of three main security controls/services:
  - C: Confidentiality
  - I: Integrity
  - A: Availability

AAA Model

- AAA is a complementary cybersecurity model that supports the CIA model, where the AAA represents the following three security controls:
  - A: Authentication
  - A: Authorization
  - A: Accounting

Confidentiality

- Keeping information secret from all, but those who are authorized to see it.
- Interception (Attack on Confidentiality):

means unauthorized party has gained access to an asset (such as Passive MITM attacks).

- Countermeasures:

Cryptography techniques, such as RSA and Triple DES

Integrity

- Ensuring that information has not been altered by unauthorized entities.
- Modification (Attack on Integrity):

An unauthorized party accesses an asset, and tampers with it (such as Active MITM attacks).

- Countermeasures:

Hashing algorithms, such as MD5 and SHA-2

Availability

- □ Assuring that system assets be available to authorized parties when needed.
- □ Interruption (Attack on Availability):

  In this attack, an asset of a system becomes lost, unavailable, or unusable (such as DDoS attacks).
- ❑ Countermeasures:

  Server Clustering

Authentication

- The process of verifying/validating user’s identity for accessing an entity.
- Fabrication (Attack on Authentication):

  The mechanism of employing other people identity to gain unauthorized access (such as stolen credentials).
- Countermeasures:

  Biometric systems, such as fingerprint recognition and keystroke dynamics.

Authorization

- The mechanism of granting a user a particular set of privileges (full/partial) for accessing an entity.
- Attack on Authorization:

The process of gaining not-allowed levels of actions on a system (such as activating unauthorized security policy).

- Countermeasures:

Access control mechanisms, such as Access Control Lists (ACLs).

Accounting

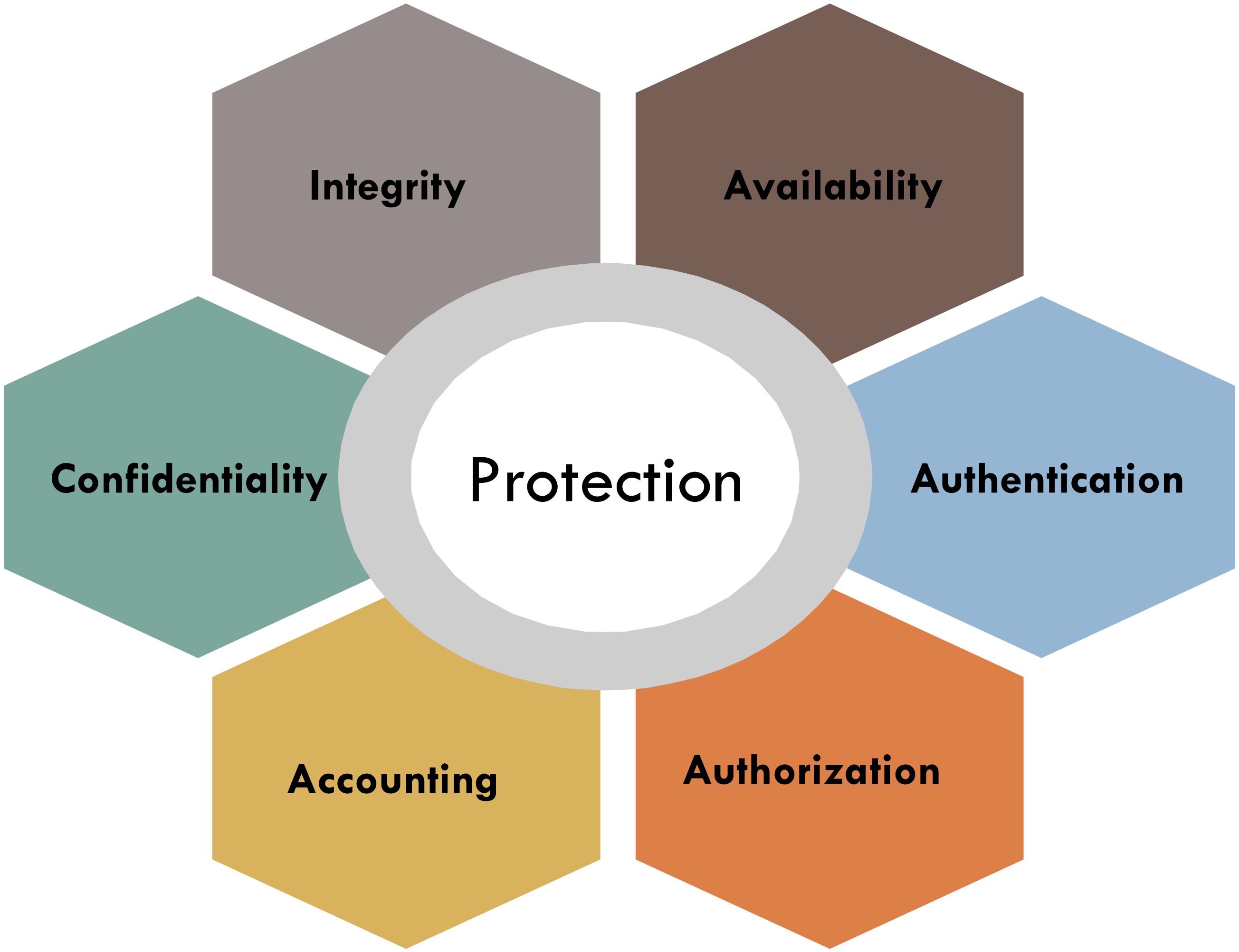
- The mechanism of making sure that an action of an entity in a system is traceable (i.e. knowing who did what action and when).
- Attack on Accounting:

Denying a specific action on a system.

- Countermeasures:

- Non-repudiation techniques, such as signing a request of an action by a digital signature.
- Auditing techniques, such as reviewing log files.

Cybersecurity



Cyber Attacks

- **Cyber Attack** is an action that exploits a vulnerability in a system.
- **Threat** is an object, person, or other entity that represents a constant danger/harm to an asset (e.g. malware, DoS, earthquake)
- **Vulnerability** is an identified weakness or flaw of an asset whose controls are not present, or are no longer effective (e.g. broken access control, misconfigurations, human weaknesses).
- A threat takes advantage of a vulnerability.

Who are the Attackers?

- Elite Hackers
  - White-hat hackers
  - Black-hat hackers
  - Gray-hat hackers
- Script Kiddies
- Insiders

Elite Hackers

- White-hat hackers

Breaking into a system for notifying firm or vendor of vulnerabilities.

- Black-hat hackers

Breaking into systems illegally, with malicious intent, and often for personal gain.

- Gray-hat hackers

Going back and forth between the two ways of hacking.

Script Kiddies

- Use prewritten attack scripts (kiddie scripts)
- Large numbers make dangerous
- Noise of kiddie script attacks masks more sophisticated attacks

Insiders

- Corporate Employees
  - Have access and knowledge
  - Financial theft
  - Theft of trade secrets (intellectual property)
  - Sabotage
  - Consultants and contractors
  - IT and security staff are biggest danger

Types of Attacks

- Passive Attacks
  - Attacks that do not require modification of the data.

- Active Attacks
  - Attacks that do require modification of the data.

Examples of Cyber Attacks

□ Brute Force Attack

The deployment of computing and network resources to try every possible combination of options of a password.

□ Dictionary Attack

The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses.

Examples of Cyber Attacks

- Denial-of-service (DoS) Attack
  - attacker sends a large number of connection or information requests to a target
  - so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
  - may result in a system crash, or merely an inability to perform ordinary functions
- Distributed Denial-of-service (DDoS) Attack

an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

Examples of Cyber Attacks

- Man-in-the-Middle (MITM) Attack

an attacker sniffs packets from the network, modifies them, and inserts them back into the network.

- MITM could be passive or active.

Social Engineering

- People are the weakest link.

- Social Engineering

The process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.

Social Engineering

- Phishing
- Voice Phishing (a.k.a. Vishing)
- SMS Phishing (a.k.a. Smishing)

Social Engineering

- This video illustrates the practice of using Vishing technique to access a cell phone account in 2 minutes.

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