Information Security

Lecture 01: Basics of Information Security

4th Grade - Spring Semester

Instructor: Alaa Ghazi
Course Resources

• Textbook
  – Cryptography and Network Security, Fourth Edition,
  – By William Stallings

2nd Resource

  – By Wenliang (Kevin) Du
Course Topics

- Lecture 01 Basics of Information Security
- Lecture 02 Types of Attacks
- Lecture 03 Firewalls
- Lecture 04 VPN (Virtual Private Networks)
- Lecture 05 PKI (Public Key Infrastructure)
- Lecture 06 IPS/IDS (Intrusion Prevention/Detection Systems)
- Lecture 07 AntiMalware
LAB Sessions

- LAB 01 Information Security LAB Setup
- LAB 02 TCP Attacks
- LAB 03 Firewall Policy
- LAB 04 Site-to-Site VPN Setup
- LAB 05 PKI (Public Key Infrastructure)
- LAB 06 IDS Example
- LAB 07 AntiMalware
Lecture 1
Basics of Information Security
Lecture Topics

1.1 Definition
1.2 Information Security Architecture
1.3 Security Services Categories
1.4 Passive Vs. Active Security Attacks
1.5 Security Attack By Effect
1.6 Security Attack Diagrams
1.7 Attack vs. Service Matrix
1.8 Main Security Mechanisms
1.9 Steps to Handle Security Risks
1.10 Cybersecurity Framework Diagram
1.1 Definition

- **Information Security** is the protection of information and its critical elements, including systems and hardware that use, store, and transmit that information.
- **Vulnerability**: a weakness that makes targets susceptible to an attack.
- **Threat**: is a possible danger that might exploit a vulnerability.
1.2 Information Security Architecture

- **Security Service**
  - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization

- **Security Attack**
  - Any action that compromises the security of information owned by an organization

- **Security Mechanism**
  - A process or a device that is designed to detect, prevent, or recover from a security attack.

Information Security is about how to make use of the security **mechanisms** to implement security **services**, resisting **attacks** on information systems.
1.3 Security Services Categories

- Confidentiality
- Authentication
- Access control
- Integrity
- Non-repudiation
- Availability
Confidentiality

• Confidentiality is the protection of transmitted data from passive attacks. It is used to prevent the disclosure of information to unauthorized individuals or systems.
• The main purpose “ensuring that information is accessible only to those authorized to have access”.
• The other aspect of confidentiality is the protection of traffic flow from analysis.
• Ex: A credit card number has to be secured during online transaction.
Authentication

• Concerned with assuring that a communication is authentic
  – In the case of a single message, assures the recipient that the message is from the source that it claims to be from
  – In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties
Access Control

• The ability to limit and control the access to host systems and applications via communications links

• To achieve this, each entity trying to gain access must first be indentified, or authenticated, so that access rights can be tailored to the individual
Integrity

• It can apply to a stream of messages, a single message, or selected fields within a message.

• Connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.

• A connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only
Nonrepudiation

• Prevents either sender or receiver from denying a transmitted message
• When a message is sent, the receiver can prove that the alleged sender in fact sent the message
• When a message is received, the sender can prove that the alleged receiver in fact received the message
Availability

• It is defined to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity.
• The availability can significantly be affected by a variety of attacks.
• The main goal is to assure that systems work promptly and service is not denied to authorized users.
1.4 Passive Vs. Active Security Attacks

- **Passive Attack**: is an attempt to learn or make use of information from the system but does not affect system resources.

- **Active Attack**: is an attempt to alter system resources or affect their operation.
1.5 Security Attack By Effect

1. INTERRUPTION

• An asset of the system is destroyed or becomes unavailable or unusable. It is an attack on availability.

• **Examples:**
  • Destruction of some hardware
  • Jamming wireless signals
  • Disabling file management systems

2. INTERCEPTION

• An unauthorized party gains access to an asset. Attack on confidentiality.

• **Examples:**
  • Wire tapping to capture data in a network.
  • Illicitly copying data or programs
  • Eavesdropping
3. MODIFICATION
• When an unauthorized party gains access and tampers an asset. Attack is on Integrity.

• Examples:
  • Changing data file
  • Altering a program and the contents of a message

4. FABRICATION
   An unauthorized party inserts a fake object into the system. Attack on Authenticity.

• Examples:
  • Hackers gaining access to a personal email and sending message
  • Insertion of records in data files
  • Insertion of spurious messages in a network
5. Repudiation

- It occurs when the user denies that he or she has performed a certain action or has initiated a transaction. It is an attack on Non-Repudiation.

- **Examples:**
  - A bank user denies an online purchase

6. Unauthorized Access

- It is an act of illegally gaining access into any computer, network, or application. It is an attack on Access Control.

- **Examples:**
  - Compromising a computer by using a vulnerability in the OS, or applications running on it.
  - Illegally using services available only to legitimate users, by using their user IDs and passwords.
1.6 Security Attack Diagrams

(a) Normal flow

(b) Interruption

(c) Interception

(d) Modification

(e) Fabrication
## 1.7 Attack vs. Service Matrix

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Confidentiality</th>
<th>Authentication</th>
<th>Integrity</th>
<th>Non-repudiation</th>
<th>Access Control</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interruption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Interception</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modification</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fabrication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repudiation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
</tbody>
</table>
1.8 Main Security Mechanisms

1. **Information flow control**: controls the flow of information between network segments.

2. **Access Control Matrix (ACM)**: The access control matrix exists both in operating systems and in database and it describes allowed accesses.

3. **Firewalls**: control traffic between the Internet and the local system or intranet

4. **Cryptography**: is the process of converting between readable text, called plaintext, and an unreadable form, called ciphertext. The sender converts the plaintext message to ciphertext, and the receiver converts the ciphertext message back to its plaintext form.

5. **Digital signature**: ensures the authenticity of documents, programs, and messages.

6. **Intrusion detection**: detects attempted or successful attacks on a system

7. **Auditing**: bookkeeping on all security-related events in a system
1.9 Steps to Handle Security Risks

1. **Identify**: The first step in cybersecurity strategy is to understand your resources and risks.

2. **Protect**: Deploy security protection mechanisms.

3. **Detect**: If an attack occurs, you’ll want mechanisms in place that will alert you as quickly as possible.

4. **Respond**: If a cybersecurity breach happens, you’ll want to contain and reduce any damage.

5. **Recover**: After a cybersecurity breach, you’ll need mechanisms in place to help resume normal operations.
1.10 Cybersecurity Framework Diagram