Definition of Security/Privacy

EJ Jung
ejung@cs.usfca.edu

Attacks, Services and Mechanisms

- **Security Attack:** Any action that compromises the security of information.
- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.
Passive attack (1) - Eavesdrop

- Code talkers

Passive attack (2) - Analysis

- Alexa
Active attack (1) - impersonation

- Impostors on Facebook

Active (2) - replay

(b) Replay
Active (3) – intercept & modify

(c) Modification of messages

Active (4) - DoS

- Distributed DoS

(d) Denial of service
Summary of attacks

<table>
<thead>
<tr>
<th>Passive Threats</th>
<th>Active Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release of message contents</td>
<td>Masquerade</td>
</tr>
<tr>
<td>Traffic analysis</td>
<td>Replay</td>
</tr>
<tr>
<td></td>
<td>Modification of message contents</td>
</tr>
<tr>
<td></td>
<td>Denial of service</td>
</tr>
</tbody>
</table>

Figure 1.2 Active and Passive Security Threats

Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files
**Attack on Authenticity**

- Authenticity is **identification and assurance of origin of information**

  Unauthorized assumption of another’s identity

**Attack on Confidentiality**

- Confidentiality is **concealment of information**

  Eavesdropping, packet sniffing, illegal copying
Attack on Integrity

- Integrity is prevention of unauthorized changes

![Diagram showing network with an attacker intercepting messages, tampering, and releasing them again.]

Attack on Availability

- Availability is ability to use information or resources desired

![Diagram showing network with an attacker overwheleming or crashing servers, disrupting infrastructure.]

9/13/2010
CS 686
Famous words

- Encrypt and decrypt
- Plaintext and ciphertext
  - encrypt plaintext \(\rightarrow\) ciphertext
  - decrypt ciphertext \(\rightarrow\) plaintext
  - easy example: XOR

- Digital signature
  - as you sign on paper
  - for non-repudiation and accountability

- Session
  - one conversation/communication unit

Model for Network Security

Figure 1.5 Model for Network Security
Access Control Model

Figure 1.6 Network Access Security Model

Information System
- Computing resources (processor, memory, I/O)
- Data
- Processes
- Software
- Internal security controls

Opponent
- human (e.g., hacker)
- software (e.g., virus, worm)

Access Channel

Gatekeeper function

9/13/2010

CS 686