Lecture 1
Introduction to data security
What Is Security?

- **Computer Security**
  The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources.

- **Network and Internet Security**
  Measures to deter, prevent, detect, and correct security violations that involve transmission of information.
Key Security Concepts
Key Security Concepts

- **Confidentiality**
  Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

- **Integrity**
  Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

- **Availability:**
  Ensuring timely and reliable access to and use of information.
Impact of Security Breaches

How do security breaches impact organizations?

- Effectiveness of primary operations are reduced
- Financial loss
- Damage to assets
- Harm to individuals
OSI Security Architecture

- ITU-T (International Telecommunication Union, Telecommunication Standardization Sector) X.800 Security Architecture for OSI.
- It provides a systematic way of defining and providing security requirement.
Aspects of Security

- **Security Attack**
  Any action that attempts to compromise the security of information or facilities.
  - Threat: potential for violation of security of information or facilities.
  - Attack: is he actual violation of security

- **Security Mechanism**
  method for preventing, detecting or recovering from an attack.

- **Security Service**
  Uses security mechanisms to enhance the security of information or facilities in order to stop attacks.
Types of Attacks

- **Passive Attack**
  Make use of information, but not affect system resources, e.g.
  1. Release message contents
  2. Traffic analysis
  Relatively hard to detect, but easier to prevent

- **Active Attack**
  Alter system resources or operation, e.g.
  1. Masquerade
  2. Replay
  3. Modification
  4. Denial of service
  Relatively hard to prevent, but easier to detect
Release Message Contents

Bob

Darth
read contents of message from Bob to Alice

Internet or other comms facility

Alice
Traffic Analysis
Masquerade Attack
Replay Attack
Modification Attack
Denial of Service Attack
Defining a Security Service

- ITU-T X.800: service that is provided by a protocol layer of communicating systems and that ensures adequate security of the systems or of data transfers
- IETF RFC 2828: a processing or communication service that is provided by a system to give a specific kind of protection to system resources
- Security services implement security policies and are implemented by security mechanisms
Security Services

- **Authentication:** Assure that the communicating entity is the one that it claims to be. (Peer entity and data origin authentication)
- **Access Control:** Prevent unauthorized use of a resource.
- **Data Confidentiality:** Protect data from unauthorized disclosure.
- **Data Integrity:** Assure data received are exactly as sent by authorized entity
- **Non-repudiation:** Protect against denial of one entity involved in communications of having participated in communications
- **Availability:** System is accessible and usable on demand by authorized users according to intended goal
Security Mechanisms

- Techniques designed to prevent, detect or recover from attacks
- No single mechanism can provide all services
- Common in most mechanisms: cryptographic techniques
Security Mechanisms

- Specific security mechanisms from ITU-T X.800: Encipherment, digital signature, access control, data integrity, authentication exchange, traffic padding, routing control, notarisation
- Pervasive security mechanisms from ITU-T X.800: Trusted functionality, security label, event detection, security audit trail, security recovery
Security Services and Mechanisms

<table>
<thead>
<tr>
<th>Service</th>
<th>Encipherment</th>
<th>Digital signature</th>
<th>Access control</th>
<th>Data integrity</th>
<th>Authentication exchange</th>
<th>Traffic padding</th>
<th>Routing control</th>
<th>Notarization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer entity authentication</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data origin authentication</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access control</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Traffic flow confidentiality</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Data integrity</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Availability</td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>