Lecture 1- Notes

Key Concepts in Computer Security

CIA Triad

- Confidentiality: Prevent unauthorized access.
- Integrity: Ensure data accuracy and trustworthiness.
- Availability: Ensure reliable access to systems and data.

Additional Concepts

- Authenticity: Verify identity and source.
- Accountability: Trace actions to responsible entities.

Security Requirements Examples

- High Integrity: Patient medical data.
- Moderate Availability: University website.
- High Confidentiality: Student grades (FERPA).

Malicious Behaviors

- Fraud, vandalism, terrorism, warfare, espionage, sabotage, spam, illegal content.
- Security Attacks
- Passive Attacks
- Eavesdropping, traffic analysis.

Active Attacks

Masquerade, replay, message modification, denial of service.

OSI Security Architecture

- Security Attack: Compromises system security.
- Security Mechanism: Detects/prevents attacks.
- Security Service: Enhances system/data security.

Security Services (X.800)

- Authentication: Peer entity & data origin.
- Access Control: Restrict resource access.
- Data Confidentiality: Protect data and traffic flow.
- Data Integrity: Ensure message accuracy.
- Nonrepudiation: Prevent denial of message origin or receipt.
- Availability: Ensure system accessibility.

Security Mechanisms

- Specific: Encryption, digital signatures, access control, traffic padding.
- Pervasive: Trusted functionality, security labels, audit trails, recovery.

Attack Surface

- Network: Open ports, services.
- Software: Vulnerable code.
- Human: Social engineering, insider threats.

Defence in Depth

Layered security approach to reduce risk and attack surface.

Attack Trees

- Hierarchical models showing paths to exploit vulnerabilities.
- Example: Internet banking authentication attack tree.

Security Models

- Network Security Model: Secure message transmission using transformations and shared secrets.
- Access Security Model: Prevent unauthorized access via gatekeepers and internal controls.

Cybersecurity Standards

- NIST: U.S. standards and guidelines.
- ISOC/IETF/IAB: Internet infrastructure standards.
- NCSC: UK's national cybersecurity guidance and incident response.