ITMC411

Security in mobile computing

LECTURE 1

Information Security Overview

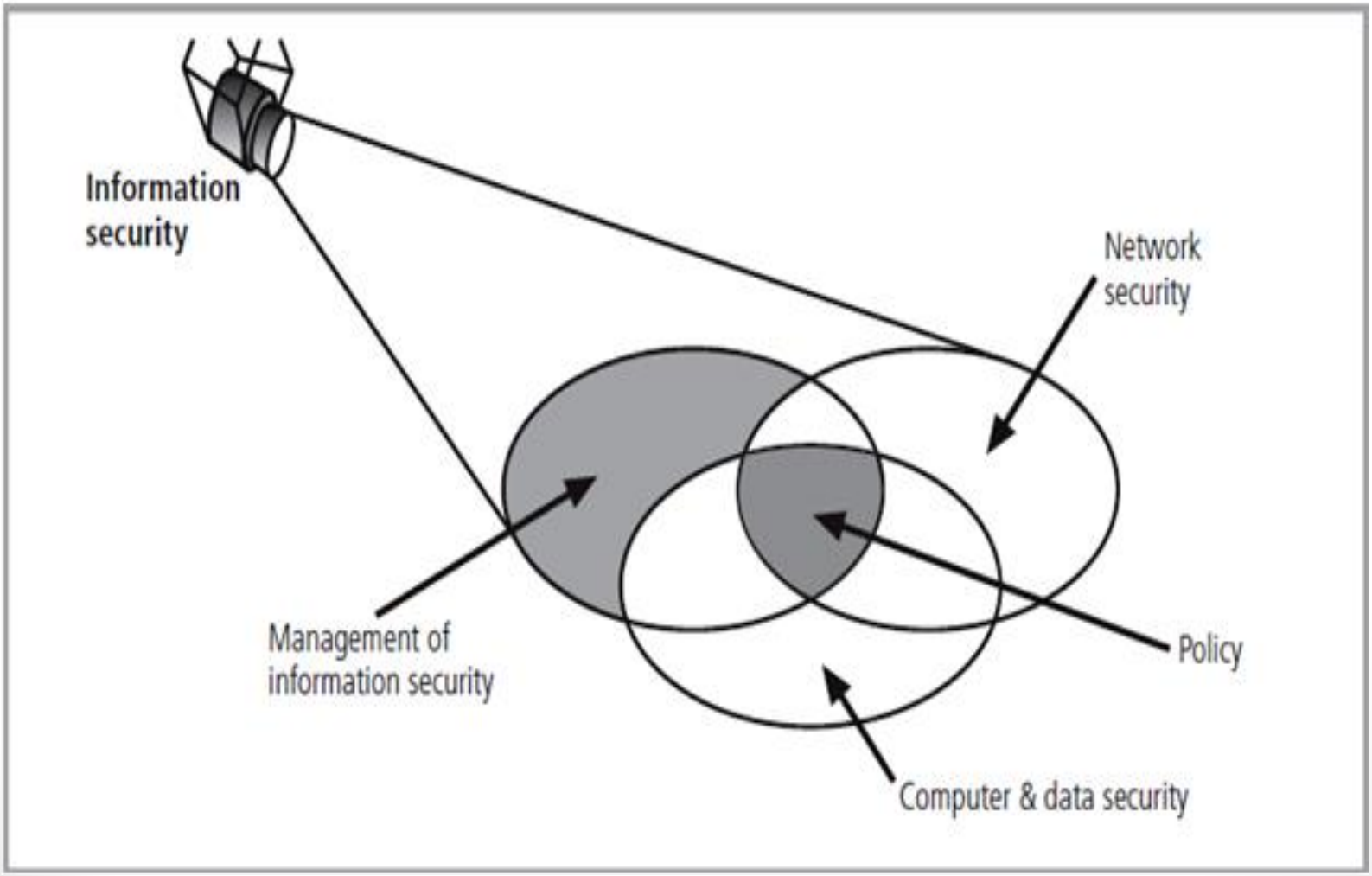
What Is Security

- In general, **security** is "the **quality** or **state** of being secure—to be free from **danger**." In other words, protection against adversaries—from those who would do harm.

A successful organization should have the following multiple layers of security in place to protect its operations:

- **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse.
- **Personnel security**, to protect the individual or group of individuals who are authorized to access the organization and its operations.
- **Operations security**, to protect the details of a particular operation or series of activities.
- **Communications security**, to protect communications media, technology, and content.
- **Network security**, to protect networking components, connections, and contents
- **Information security**, to protect the **confidentiality**, **integrity** and **availability** of information assets, whether in storage, processing, or transmission.

Components of Information Security



Key Information Security Concepts

- **Access**: A subject or object's ability to **use**, **manipulate**, **modify**, or **affect** another subject or object.
- **Asset**: The resource that is being protected. **An asset can be :**
  - **logical**, such as a Web site, information, or data;
  - **physical**, such as a person, computer system, or other tangible object.
- **Attack**: Attacks can be **active** or **passive**, **intentional** or **unintentional**, and **direct** or **indirect**.
- **Control, safeguard, or countermeasure**: Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities.
- **Exploit**: A technique used to compromise a system.
- **Exposure**: A condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.

Key Information Security Concepts

- **Loss**: A single instance of an information asset suffering damage when an organization's information is stolen.
- **Protection profile or security posture**: The entire set of controls and safeguards, including **policy**, **education**, **training** and **awareness**, and **technology**, that then organization implements (or fails to implement) to protect the asset.
- **Risk**: The probability that something unwanted will happen.
- **Threat**: A category of objects, persons, or other entities that presents a danger to an asset.
- **Threat agent**: The specific instance or a component of a threat.
- **Vulnerability**: A weaknesses or fault in a system or protection mechanism that opens it to attack or damage.

The Security Systems Development Life Cycle

Phases	Steps common to both the systems development life cycle and the security systems development life cycle	Steps unique to the security systems development life cycle
Investigation	● Outline project scope and goals ● Estimate costs ● Evaluate existing resources ● Analyze feasibility	● Management defines project processes and goals and documents these in the program security policy
Analysis	●Assess current system against plan developed in Phase 1 ● Develop preliminary system requirements ● Study integration of new system with existing system ● Document findings and update feasibility analysis	● Analyze existing security policies and programs ● Analyze current threats and controls ● Examine legal issues ● Perform risk analysis
Logical Design	● Assess current business needs against plan developed in Phase 2 ● Select applications, data support, and structures ● Generate multiple solutions for consideration ● Document findings and update feasibility analysis	● Develop security blueprint ● Plan incident response actions ● Plan business response to disaster ● Determine feasibility of continuing and/or outsourcing the project
Physical Design	● Select technologies to support solutions developed in Phase 3 ● Select the best solution ● Decide to make or buy components ● Document findings and update feasibility analysis	● Select technologies needed to support security blueprint ● Develop definition of successful solution ● Design physical security measures to support techno logical solutions ● Review and approve project
Implementation	● Develop or buy software ● Order components ● Document the system ● Train users ● Update feasibility analysis ● Present system to users ● Test system and review performance	● Buy or develop security solutions ● At end of phase, present tested package to management for approval
Maintenance and Change	● Support and modify system during its useful life ● Test periodically for compliance with business needs ● Upgrade and patch as necessary	●Constantly monitor, test, modify, update, and repair to meet changing threats

What Is information security?

- **InfoSec**, or **information security** :is a set of **tools** and **practices** that you can use to protect your digital and analog information.
- **InfoSec** covers a range of IT domains, including infrastructure and network security, auditing, and testing.

Information Security VS Cybersecurity

- **Information security** : is a broader category of protections, covering cryptography, mobile computing, and social media.
  It is related to **information assurance**, used to protect information from **non-person-based** threats, such as server failures or natural disasters.
- **cybersecurity** only covers Internet-based threats and digital data.

Information security principles (**CIA**)

- **Confidentiality**: prevents **unauthorized users** from accessing information to protect the privacy of information content. **Confidentiality** is maintained through access restrictions.
- **Integrity**: ensures the **authenticity** and **accuracy** of information. **Integrity** is maintained by restricting permissions for editing or the ability to modify information.
- **Availability**: ensures that **authorized users** can reliably access information. **Availability** is maintained through continuity of access procedures, backup or duplication of information, and maintenance of hardware and network connections.

Types of Information Security

- **Application Security** : **strategies** protect **applications** and **application programming interfaces (APIs)**. You can use these strategies to prevent, detect and correct **bugs** or other vulnerabilities in your applications.
- **Infrastructure security**: **strategies** protect infrastructure components, including **networks**, **servers**, **client devices**, **mobile devices**, and **data centers**.
- **Cloud security** : focused on **cloud or cloud-connected components** and **information**.
- **Cryptography**: uses a practice called **encryption** to secure information by **obscuring** the contents.
- **Incident response**: is a set of **procedures** and **tools** that you can use to **identify**, **investigate**, and **respond** to threats or damaging events.
- **Vulnerability Management**: is a **practice** meant to reduce **inherent risks** in an application or system.
- **Disaster recovery**: **strategies** protect your organization from loss or damage due to unforeseen events. For example, **ransomware**, **natural disasters**, or **single points of failure**.

Common Information Security Risks

- **Social engineering attacks**

  Social engineering involves using **psychology** to trick users into providing information or access to attackers.

- **Advanced persistent threats (APT)**

  APTs are threats in which individuals or groups gain access to your systems and remain for an extended period.

- **Insider threats**

  are vulnerabilities created by individuals within your organization. These threats may be accidental or intentional.

Common Information Security Risks

- **Cryptojacking**
  also called **crypto mining**, is when attackers abuse your system resources to mine cryptocurrency. Attackers typically accomplish this by tricking users into downloading malware or when users open files with malicious scripts included.
- **Distributed denial of service (DDoS)**
  DDoS attacks occur when attackers overload servers or resources with requests.
- **Ransomware**: attacks use **malware** to encrypt your data and hold it for ransom.

Common Information Security Risks

- **Man-in-the-middle (MitM) attack**
  MitM attacks occur when communications are sent over insecure channels. attackers intercept requests and responses to read the contents, manipulate the data, or redirect users.

- **There are multiple types of MitM attacks, including:**
  - **Session hijacking**—in which attackers substitute their own IP for legitimate users to use their session and credentials to gain system access.
  - **IP spoofing**—in which attackers imitate trusted sources to send malicious information to a system or request information back.
  - **Eavesdropping attacks**—in which attackers collect information passed in communications between legitimate users and your systems.

Information Security Technologies

- **Firewalls**
  a layer of protection that you can apply to networks or applications. These tools enable you to filter traffic and report traffic data to monitoring and detection systems.
- **Security incident and event management (SIEM)**
  SIEM solutions enable you to ingest and correlate information from across your systems. This aggregation of data enables teams to detect threats more effectively, more effectively manage alerts, and provide better context for investigations

Information Security Technologies

- **Data loss prevention (DLP)**

  DLP strategies incorporate tools and practices that protect data from loss or modification. This includes categorizing data, backing up data, and monitoring how data is shared across and outside an organization.

- **Intrusion detection system (IDS)**

  IDS solutions are tools for monitoring incoming traffic and detecting threats.

Information Security Technologies

- **Intrusion prevention system (IPS)**
  IPS security solutions **respond** to traffic that is identified as suspicious or malicious, blocking requests or ending user sessions.

- **User behavioral analytics (UBA)**
  UBA solutions gather information on user activities and correlate those behaviors into a baseline. Solutions then use this baseline as a comparison against new behaviors to identify inconsistencies.

Information Security Technologies

- **Blockchain cybersecurity**: is a technology that relies on immutable transactional events. In **blockchain** technologies, distributed networks of users verify the authenticity of transactions and ensure that integrity is maintained.
- **Endpoint detection and response (EDR)**
  EDR cybersecurity solutions enable you to monitor endpoint activity, identify suspicious activity, and automatically respond to threats.
- **Cloud security posture management (CSPM)**
  CSPM is a set of practices and technologies you can use to evaluate your cloud resources' security. These technologies enable you to scan configurations, compare protections to benchmarks, and ensure that security policies are applied uniformly.