

Information Security

Prepared by Dr. Ahmed Omar

IT373
Information Security

Lecture 1



Foundations of Information Security & Assurance

Lecture 1

IT373
Information Security

Prepared by
Dr. Ahmed Omar

Agenda/Outline

- Computer security concepts
 - Definition
 - Challenges
 - Model
- Threats, attacks, and assets
 - Threats and attacks
 - Threats and assets
- Security functional requirements
- Standards



Computer Security

“ Measures and controls that ensure confidentiality, integrity, and availability of information processed and stored by a computer, including hardware, software, firmware, information data, and telecommunications.”

The N I S T Internal/Interagency Report N I S T I R 7298
(*Glossary of Key Information Security Terms*, July 2019)



Essential Network and Computer Security Requirements

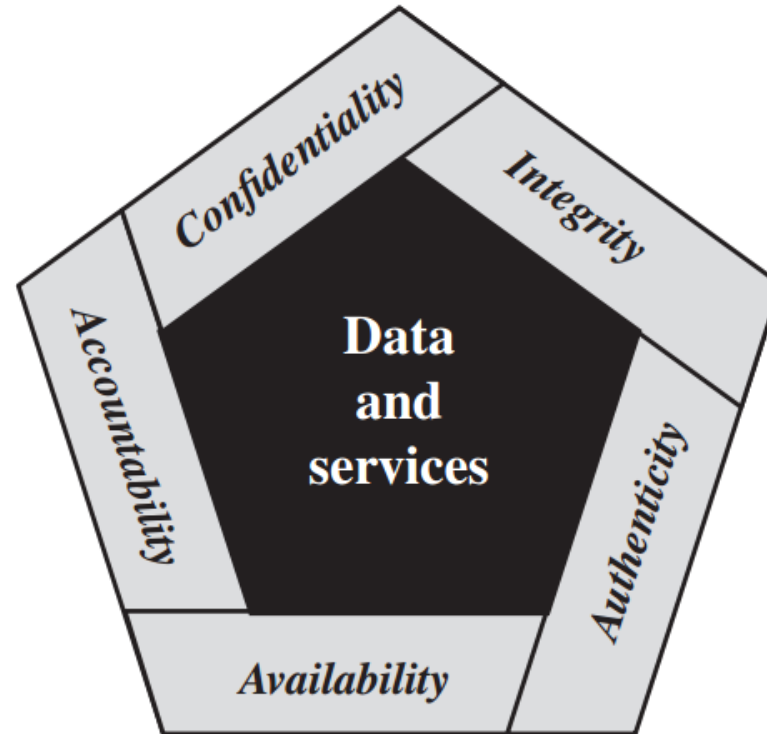


Figure 1.1 Essential Network and Computer Security Requirements

Security Objectives

- The cybersecurity definition introduces three key objectives that are at the heart of information and network security:
 - **Confidentiality:** This term covers two related concepts:
 - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals
 - **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed



Security Objectives

Integrity



Data Integrity

- Information remains unchanged
- Only authorized modifications occur
- Protects against accidental corruption

System Integrity

- System performs as intended
- Free from unauthorized manipulation
- Ensures reliable and secure operations

Security Objectives

Availability

Assures that systems work promptly and service is not denied to authorized users



The Challenges of Computer Security

1. Looks Easy, but It's Hard: Keeping computers safe seems simple, but the tools needed are actually very complicated.
2. Think Like a Hacker: To protect a system, you have to think about all the clever and surprising ways someone might try to break in.
3. Complex Fixes for Complex Problems: Security rules can seem strange or too complex, but they are needed to stop clever attacks.
4. Putting Security in the Right Place: You have to decide on the best places to put your security tools, both in the real world (like on a network) and inside the computer's software.
5. It's Not Just About a Program: Security needs more than just a tool. It also needs secrets (like passwords or keys), and we have to worry about how to create, share, and protect those secrets.

The Challenges of Computer Security

6. An Unfair Fight: The person attacking only needs to find one mistake to win. The person defending has to find and fix every single mistake to be safe.
7. People Don't Care Until It's Too Late: Most people don't see the need for security until after they get hacked.
8. You Must Always Be Watching: Security needs to be checked all the time, which is hard when everyone is busy.
9. Added Late, Not Built-In: Often, security is added to a system at the end, instead of being a part of the original plan.
10. Security vs. Ease of Use: Many people feel that strong security makes computers harder and slower to use.

Computer Security Terminology

- **Adversary (Threat Agent)**

An individual, group, organization, or government that carries out or intends to carry out harmful activities.

- **Attack**

A malicious action aimed at gathering, disrupting, denying, degrading, or destroying information system resources or the data itself.

- **Countermeasure**

A device or technique designed to reduce the effectiveness of harmful or adversarial activities, or to prevent surveillance, sabotage, theft, or unauthorized access to sensitive information or systems.

Computer Security Terminology

- **Risk**

A measure of the degree to which an entity faces potential harm from a specific situation or event, typically determined by

- 1) the negative impacts that would result if the event occurs.
- 2) the probability of its occurrence.

- **Security Policy**

A collection of guidelines for delivering security services. It outlines and limits the activities of a data processing facility to ensure the security of systems and data.

- **System Resource (Asset)**

A significant application, general support system, high-impact program, physical infrastructure, mission-critical system, personnel, equipment, or a group of related systems.

Computer Security Terminology

- **Threat**

Any situation or event that could negatively affect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system by means of unauthorized access, destruction, disclosure, modification of information, or denial of service.

- **Vulnerability**

A flaw in an information system, security procedures, internal controls, or implementation that could be exploited or activated by a threat source.

Assets of a Computer System

- **Hardware:** Including computer systems and other data processing, data storage, and data communications devices.
- **Software:** Including the operating system, system utilities, and applications.
- **Data:** Including files and databases, as well as security-related data, such as password files.
- **Communication facilities and networks:** Local and wide area network communication links, bridges, routers, and so on.



- Categories of Vulnerabilities
 - **Corrupted:** Loss of integrity.
 - **Leaky:** Loss of confidentiality.
 - **Unavailable or Very Slow:** Loss of availability.
- Threats
 - Capable of exploiting vulnerabilities.
 - Pose potential security risks to an asset.



- Attacks (Threats Carried Out)
 - **Active:** Attempts to modify system resources or affect their operation.
 - **Passive:** Attempts to gather or use system information without altering system resources.

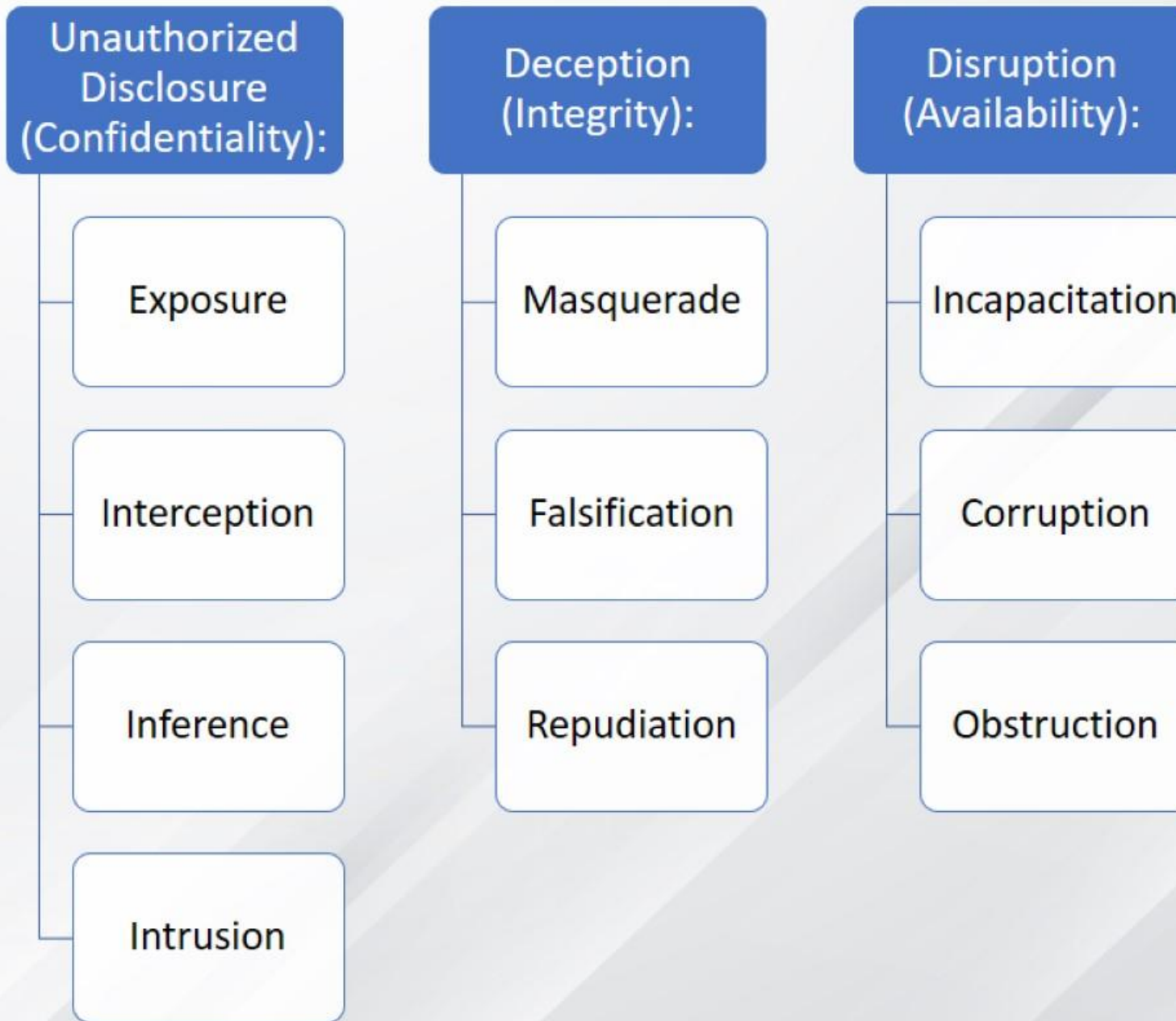
Classify attacks based on the origin of the attack:

- **Insider:** Initiated by an entity within the security perimeter.
- **Outsider:** Initiated from outside the perimeter.



- Means Used to Address Security Attacks
 - **Prevent:** Take actions to stop attacks before they occur.
 - **Detect:** Identify and report attacks when they happen.
 - **Recover:** Restore normal operations after an attack.





- Unauthorized Disclosure:
 - **Exposure:** Sensitive information deliberately or accidentally released (e.g., credit card leaks, accidental data exposure on the web).
 - **Interception:** Unauthorized access to communication on networks (e.g., LAN, Internet).
 - **Inference:** Gaining information through traffic analysis or repeated database queries.
 - **Intrusion:** Bypassing access controls to obtain sensitive data.

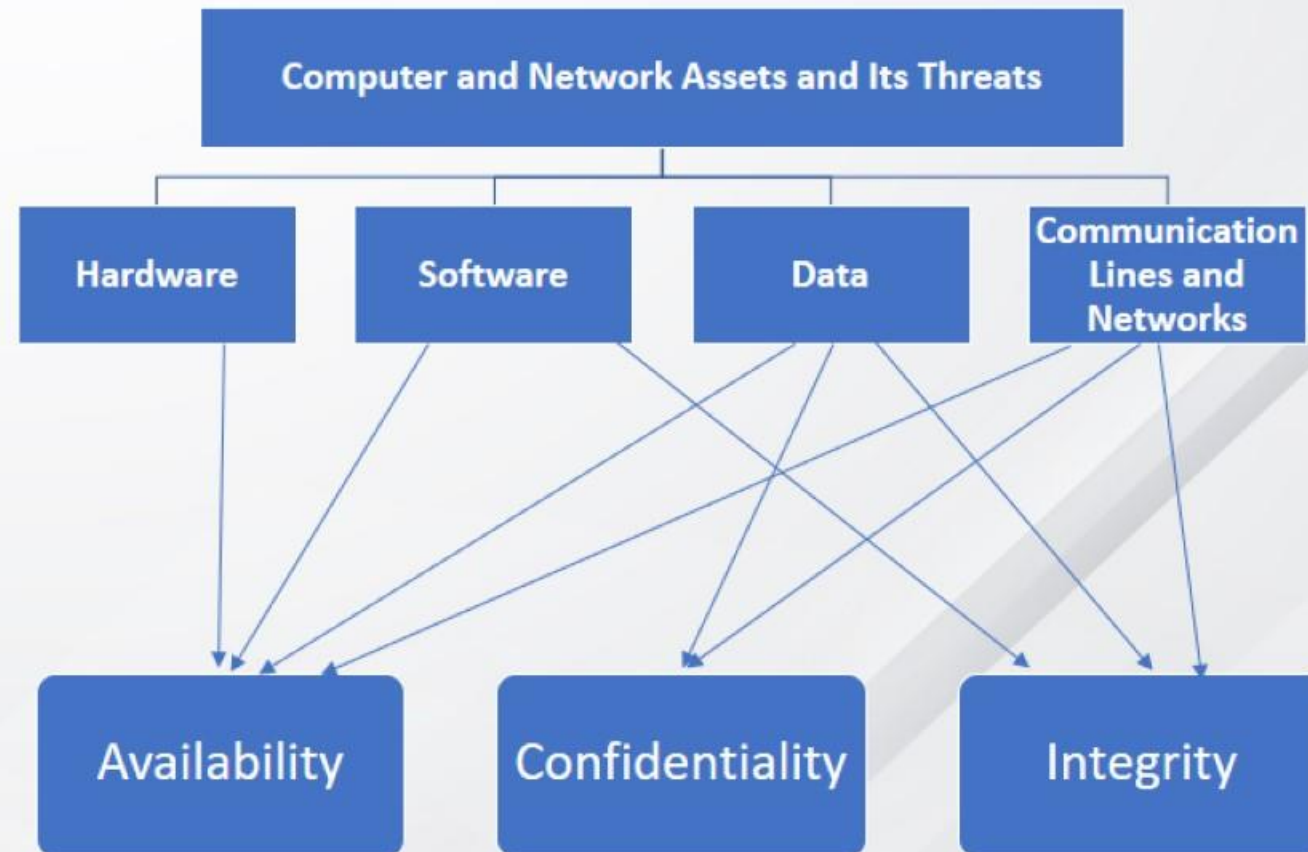


- Deception:
 - **Masquerade:** Posing as an authorized user or using malicious software (e.g., Trojan horses).
 - **Falsification:** Altering or replacing valid data (e.g., changing grades in a database).
 - **Repudiation:** Denying sending, receiving, or possessing data.



- Disruption:
 - **Incapacitation:** System availability attack (e.g., hardware damage, malware disabling services).
 - **Corruption:** Altering system resources or services (e.g., installing backdoors).
 - **Obstruction:** Disabling or overloading communication links or resources.





Threats and Assets (Hardware Threats)

- **Primary Threat:** Availability
- Vulnerabilities:
 - Accidental or deliberate damage and theft
 - USB drive theft leads to confidentiality loss
- **Countermeasures:**
 - Physical and administrative security



Threats and Assets (Software Threats)

- **Primary Threat:** Availability and Integrity
- Vulnerabilities:
 - Deletion or alteration of software (viruses, modification)
 - Unauthorized copying (software piracy)
- **Countermeasures:**
 - Configuration management (backups)
 - Monitoring for software integrity



Threats and Assets (Data Threats)

- **Primary Threats:** Availability, Secrecy, Integrity
- Vulnerabilities:
 - Destruction of data (accidental or malicious)
 - Unauthorized access through analysis (statistical databases)
 - Modifications can range from minor to disastrous
- **Countermeasures:**
 - Encryption, controlled access, data consistency checks



Threats and Assets (Network Threats)

- **Types of Attacks:**
 - **Passive:** Eavesdropping, Traffic Analysis
 - **Active:** Replay, Masquerade, Message Modification, Denial of Service
- **Countermeasures:**
 - **Passive:** Encryption for prevention
 - **Active:** Detection and recovery from disruption



Security Functional Requirements

Countermeasures can be classified as technical or managerial.

FIPS 200 defines **17 security-related areas** for protecting information system confidentiality, integrity, and availability.

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Certification, Accreditation, and Security Assessments
5. Configuration Management
6. Contingency Planning
7. Identification and Authentication
8. Incident Response
9. Maintenance
10. Media Protection
11. Physical and Environmental Protection
12. Planning
13. Personnel Security
14. Risk Assessment
15. Systems and Services Acquisition
16. System and Communications Protection
17. System and Information Integrity



Security Requirements

1. **Access Control:** Restrict access to information systems to authorized users, processes on behalf of authorized users, or devices (including other systems). Limit access to the types of transactions and functions that authorized users are permitted to perform.
2. **Awareness and Training:**
 - (i) Ensure managers and users are aware of security risks associated with their activities and understand relevant laws, regulations, and policies related to information system security.
 - (ii) Provide adequate training for personnel to perform their information security-related duties and responsibilities effectively.
3. **Audit and Accountability:**
 - (i) Generate, safeguard, and retain audit records to monitor, analyze, investigate, and report on unlawful, unauthorized, or inappropriate information system activities.
 - (ii) Ensure that the actions of individual users can be uniquely traced to hold them accountable for their activities.



Security Requirements

4. Certification, Accreditation, and Security Assessments:

- (i) Regularly evaluate the effectiveness of security controls in organizational information systems.
- (ii) Develop and implement action plans to address deficiencies and reduce or eliminate vulnerabilities in these systems.
- (iii) Authorize the operation of information systems and any associated connections.
- (iv) Continuously monitor security controls to ensure their ongoing effectiveness



Security Requirements

5. Configuration Management:

- (i) Establish and maintain baseline configurations and inventories of organizational information systems, including hardware, software, firmware, and documentation, throughout their development life cycles.
- (ii) Set and enforce security configuration settings for information technology products used in organizational information systems.



Security Requirements

6. **Contingency Planning:** Develop, maintain, and implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems. This ensures the availability of critical information resources and continuity of operations during emergencies.
7. **Identification and Authentication:** Identify users, processes acting on behalf of users, or devices and verify their identities as a prerequisite for granting access to organizational information systems.
8. **Incident Response:**
 - (i) Establish a comprehensive incident-handling capability that includes preparation, detection, analysis, containment, recovery, and user-response activities for organizational information systems.
 - (ii) Track, document, and report incidents to relevant organizational officials and/or authorities.



Security Requirements

9. Maintenance:

- (i) Conduct regular and timely maintenance on organizational information systems.
- (ii) Implement effective controls over the tools, techniques, mechanisms, and personnel involved in system maintenance.

10. Media Protection:

- (i) Safeguard both paper and digital information system media.
- (ii) Restrict access to information on media to authorized users.
- (iii) Properly sanitize or destroy media before disposal or reuse.



Security Requirements

11. Physical and Environmental Protection:

- (i) Restrict physical access to information systems, equipment, and their operating environments to authorized individuals.
- (ii) Secure the physical plant and support infrastructure for information systems.
- (iii) Ensure supporting utilities are available for information systems.
- (iv) Protect information systems from environmental hazards.
- (v) Implement appropriate environmental controls in facilities housing information systems.



Security Requirements

12. Planning: Develop, document, periodically update, and implement security plans for organizational information systems. These plans should outline the security controls in place or planned and specify the rules of behavior for individuals accessing the systems.



Security Requirements

13. Personnel Security:

- (i) Ensure that individuals in key positions, including third-party service providers, are trustworthy and meet established security criteria.
- (ii) Protect organizational information and systems during and after personnel actions, such as terminations and transfers.
- (iii) Implement formal sanctions for individuals who fail to comply with organizational security policies and procedures.



Security Requirements

14. Risk Assessment: Regularly evaluate the risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals that arise from the operation of information systems and the processing, storage, or transmission of organizational information.



Security Requirements

15. Systems and Services Acquisition:

- (i) Allocate sufficient resources to ensure adequate protection of organizational information systems.
- (ii) Integrate information security considerations into system development life cycle processes.
- (iii) Implement restrictions on software usage and installation.
- (iv) Ensure that third-party providers maintain adequate security measures to protect outsourced information, applications, and services.



Security Requirements

16. System and Communications Protection:

- (i) Monitor, control, and secure organizational communications at external and key internal boundaries of information systems.
- (ii) Apply architectural designs, software development techniques, and systems engineering principles that enhance information security within organizational information systems.



Security Requirements

17. System and Information Integrity:

- (i) Identify, report, and rectify flaws in information and information systems promptly.
- (ii) Implement protections against malicious code at suitable locations within organizational information systems.
- (iii) Monitor security alerts and advisories for information systems and take appropriate actions in response.

Source: Based on FIPS 200



- **Security Policy**

A formal statement of rules and practices that define or regulate how a system or organization provides security services to safeguard sensitive and critical system resources.

- **Security Implementation**

Involves four complementary actions:

- **Prevention:** Measures taken to avoid security incidents.
- **Detection:** Identifying and recognizing security breaches or vulnerabilities.
- **Response:** Actions taken to address and manage security incidents.
- **Recovery:** Restoring systems and operations to normal after a security incident.



- Assurance
 - Encompassing both system design and system implementation, assurance is an attribute of an information system that provides grounds for having confidence that the system operates such that the system's security policy is enforced
- Evaluation
 - Process of examining a computer product or system with respect to certain criteria
 - Involves testing and may also involve formal analytic or mathematical techniques



Standards (1 of 2)

- Standards have been developed to cover management practices and the overall architecture of security mechanisms and services
- The most important of these organizations are:
 - National Institute of Standards and Technology (NIST)
 - NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation
 - Internet Society (ISOC)
 - ISOC is a professional membership society that provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards



- **International Telecommunication Union (ITU-T)**
ITU is a United Nations agency where governments and the private sector collaborate to coordinate global telecommunications networks and services.
- **International Organization for Standardization (ISO)**
ISO is a nongovernmental organization that creates international agreements published as International Standards.



Summary

- Computer security concepts
 - Definition
 - Challenges
 - Model
- Threats, attacks, and assets
 - Threats and attacks
 - Threats and assets
- Security functional requirements
- Computer security strategy
 - Security policy
 - Security implementation
 - Assurance and evaluation
- Standards





Thank You

