# Introduction on Information security


## Chapter 1 – Overview

**Riccardo Spolaor, Ph.D** rspolaor@sdu.edu.cn

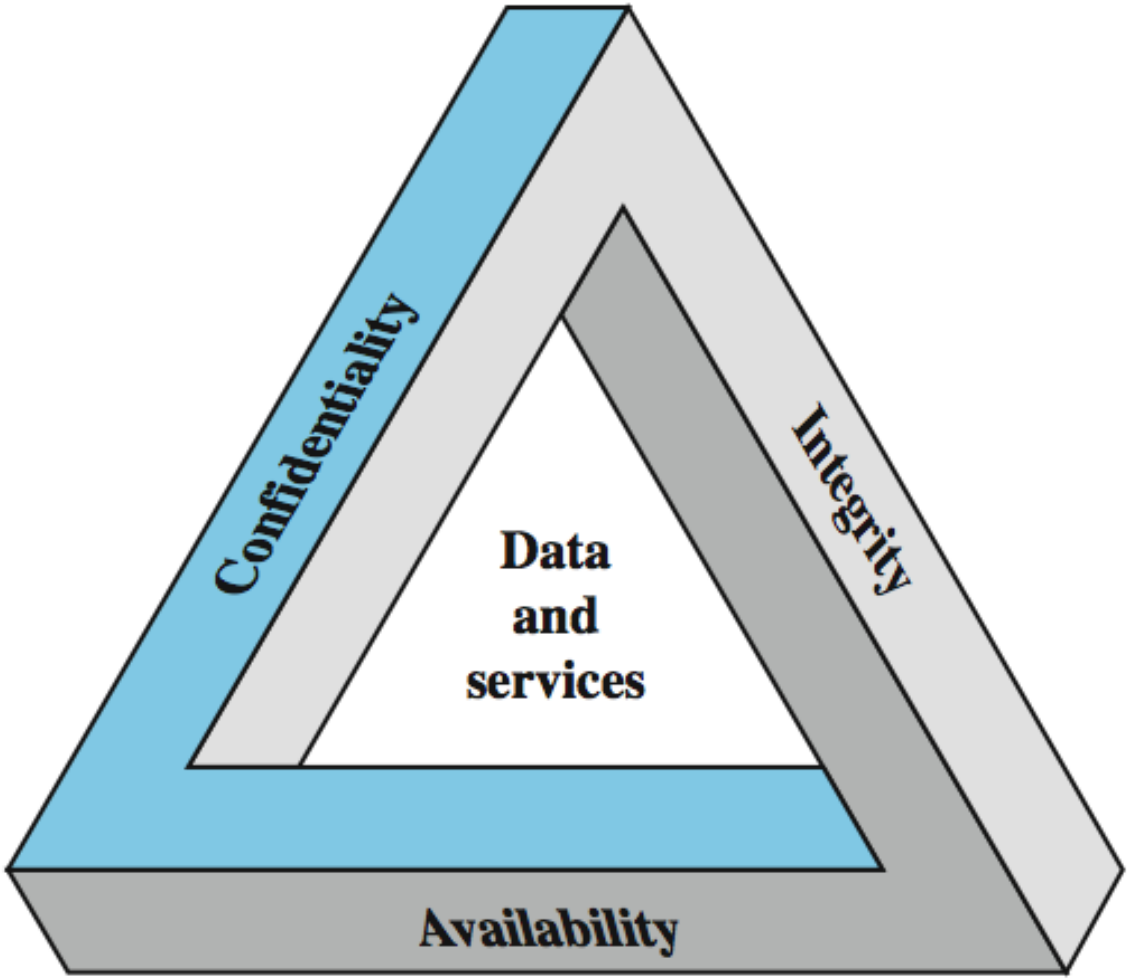
Shandong University, School of Computer Science and Technology

# Overview

**Computer Security:**

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 (includes hardware, software, firmware, information/data, and telecommunications).

# Key Security Concepts



# Key security concepts (definitions)

- **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

# Computer Security Challenges

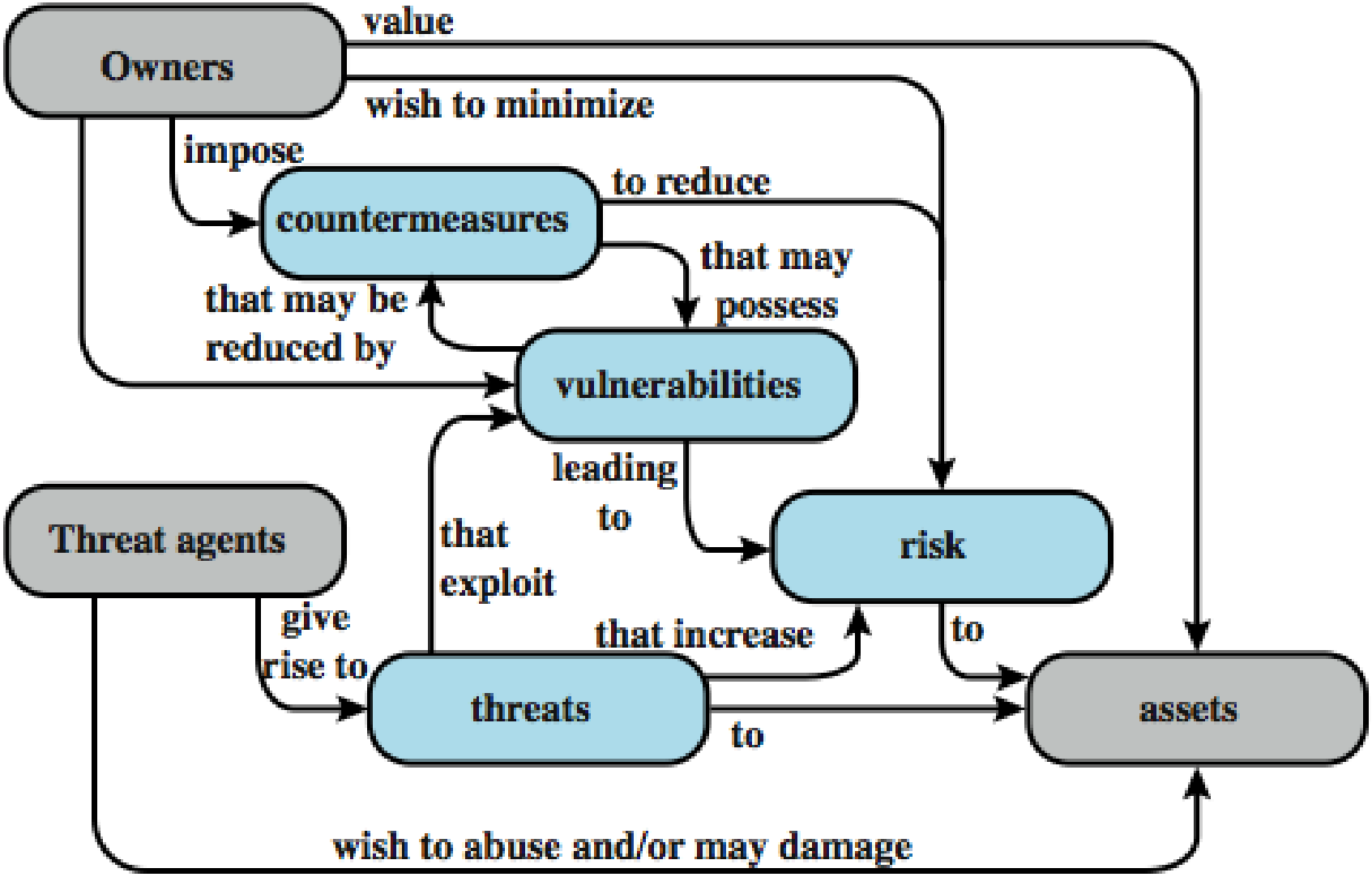
- not simple
- must consider potential attacks
- procedures used counter-intuitive
- involve algorithms and secret info
- must decide where to deploy mechanisms
- battle of wits between attacker / admin
- not perceived on benefit until fails
- requires regular/constant monitoring
- too often an after-thought
- regarded as impediment to using system

# Levels of Impact

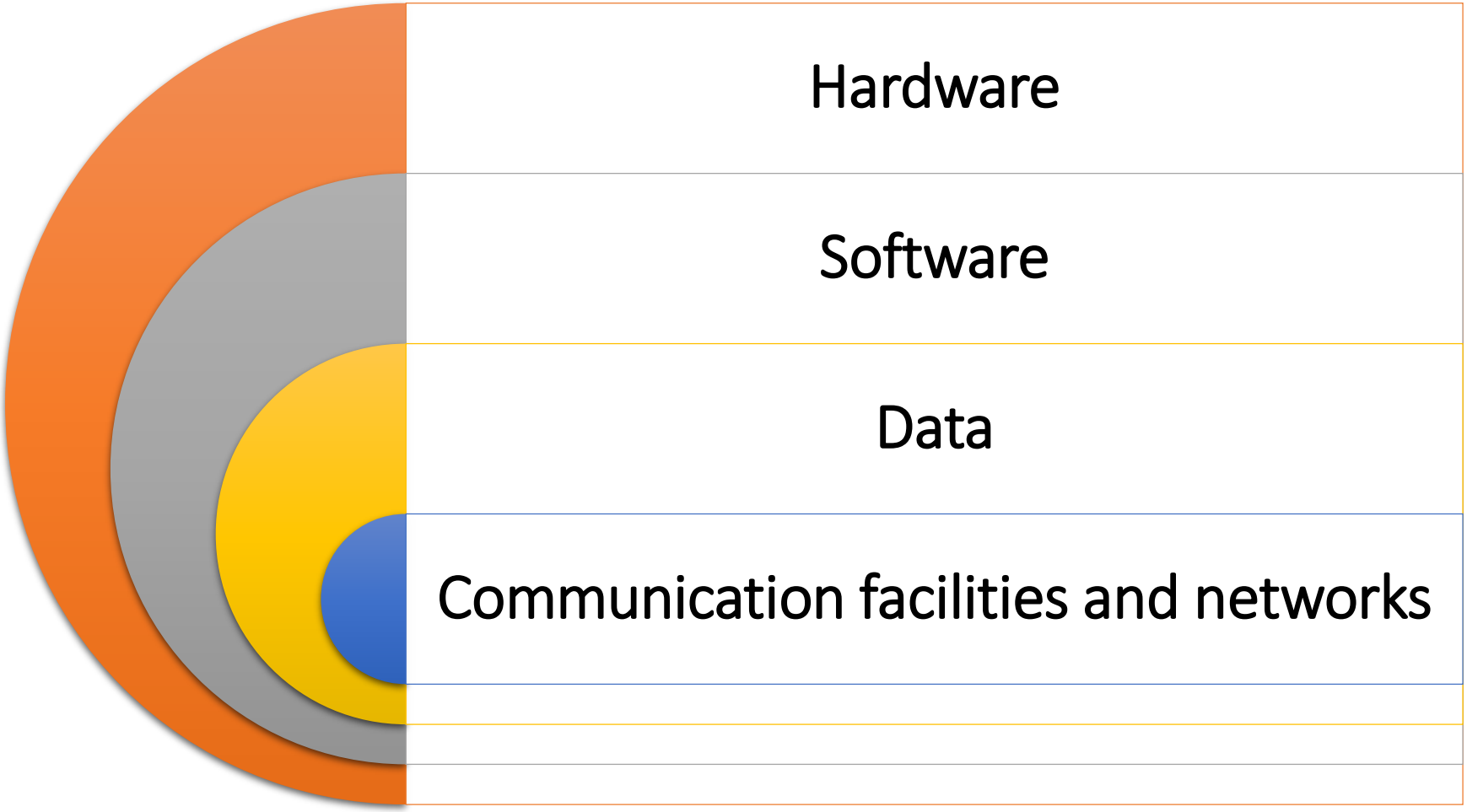
| Low | Moderate | High |
| --- | --- | --- |
| The loss could be expected to have a **limited** adverse effect on... | The loss could be expected to have a **serious** adverse effect on ... | The loss could be expected to have a **severe or catastrophic** adverse effect on... |

**... organizational operations, organizational assets, or individuals**

# Security Terminology



# Assets of a Computer System



# Vulnerabilities and Attacks

- system resource: with vulnerabilities may
  - be corrupted (loss of integrity)
  - become leaky (loss of confidentiality)
  - become unavailable (loss of availability)
- attacks are threats carried out and may be
  - passive
  - active
  - insider
  - outsider

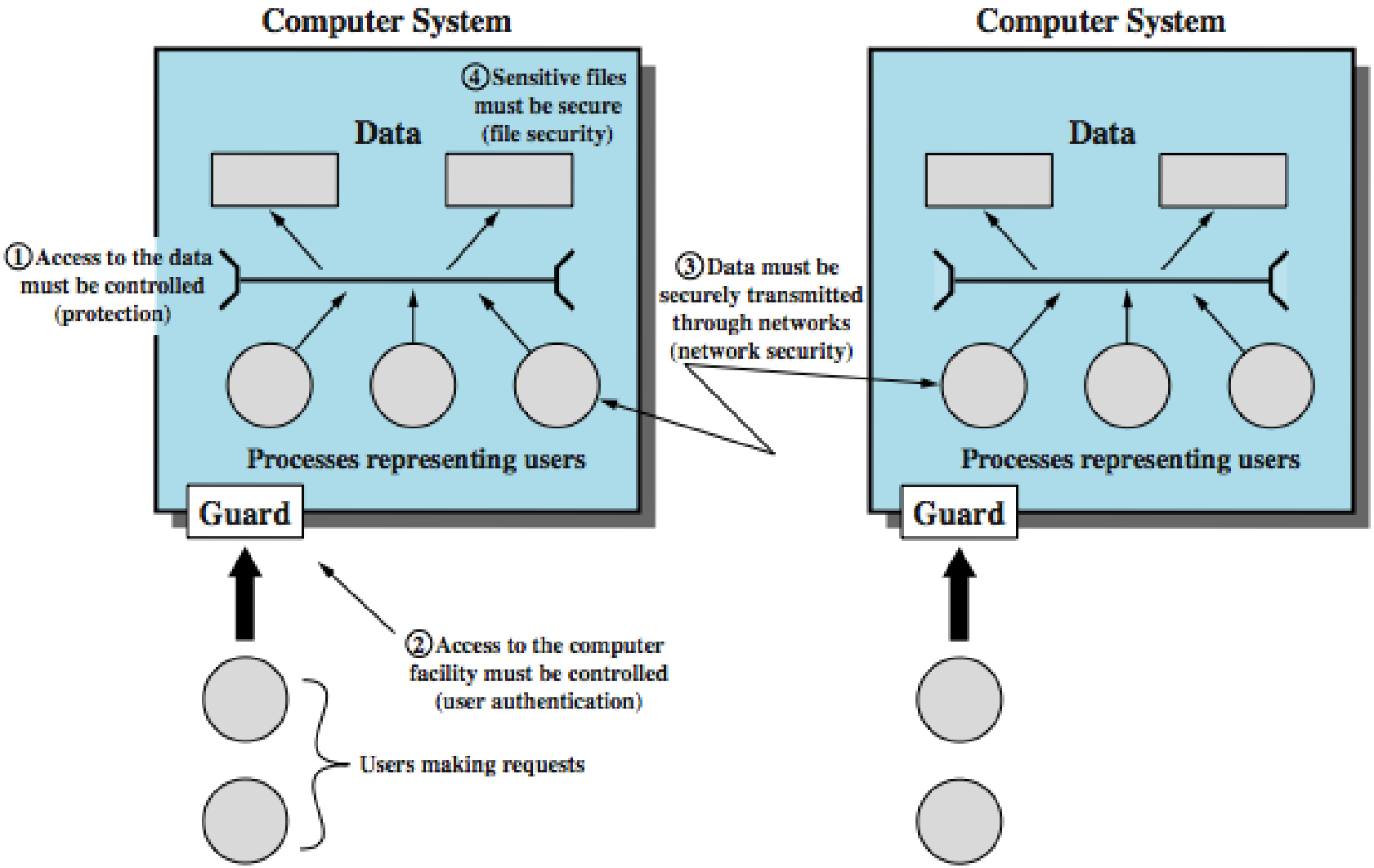
# Countermeasures

- means used to deal with security attacks
  - prevent
  - detect
  - recover
- may result in new vulnerabilities
- will have residual vulnerability
- goal is to minimize risk, given constraints

# Threat Consequences

- unauthorized disclosure
  - exposure, interception, inference, intrusion
- deception
  - masquerade, falsification, repudiation
- disruption
  - incapacitation, corruption, obstruction
- usurpation
  - misappropriation, misuse

# Scope of Computer Security



# Computer and Network Assets, with Examples of Threats

| | Availability | Confidentiality | Integrity |
|---|---|---|---|
| **Hardware** | Equipment is stolen or disabled, thus denying service. | An unencrypted CD-ROM or DVD is stolen. | |
| **Software** | Programs are deleted, denying access to users. | An unauthorized copy of software is made. | A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task. |
| **Data** | Files are deleted, denying access to users. | An unauthorized read of data is performed. An analysis of statistical data reveals underlying data. | Existing files are modified or new files are fabricated. |
| **Communication Lines and Networks** | Messages are destroyed or deleted. Communication lines or networks are rendered unavailable. | Messages are read. The traffic pattern of messages is observed. | Messages are modified, delayed, reordered, or duplicated. False messages are fabricated. |

# Network Security Attacks

- classify as **passive** or **active**

- **passive attacks** are eavesdropping
  - release of message contents
  - traffic analysis
  - are hard to detect so aim to prevent

- **active attacks** modify/fake data
  - masquerade
  - replay
  - modification
  - denial of service
  - hard to prevent so aim to detect

# Security Functional Requirements

- technical measures:
  - access control; identification & authentication; system & communication protection; system & information integrity
- management controls and procedures
  - awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
- overlapping technical and management:
  - configuration management; incident response; media protection

# Fundamental Security Design Principles

| | | | |
|---|---|---|---|
| Economy of mechanism | Fail-safe defaults | Complete mediation | Open design |
| Separation of privilege | Least privilege | Least common mechanism | Psychological acceptability |
| Isolation | Encapsulation | Modularity | Layering |
| Least astonishment | | | |

# Attack surfaces

Consist of the reachable and exploitable vulnerabilities in a system

Examples:

- Open ports on outward facing Web and other servers, and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
- Interfaces, SQL, and Web forms
- An employee with access to sensitive information vulnerable to a social engineering attack

# Attack surfaces Categories

## Network Attack Surface

- Vulnerabilities over an enterprise network, wide-area network, or the Internet
- Network protocol vulnerabilities: Used by denial-of-service attack, disruption of communications links, and various forms of intruder attacks

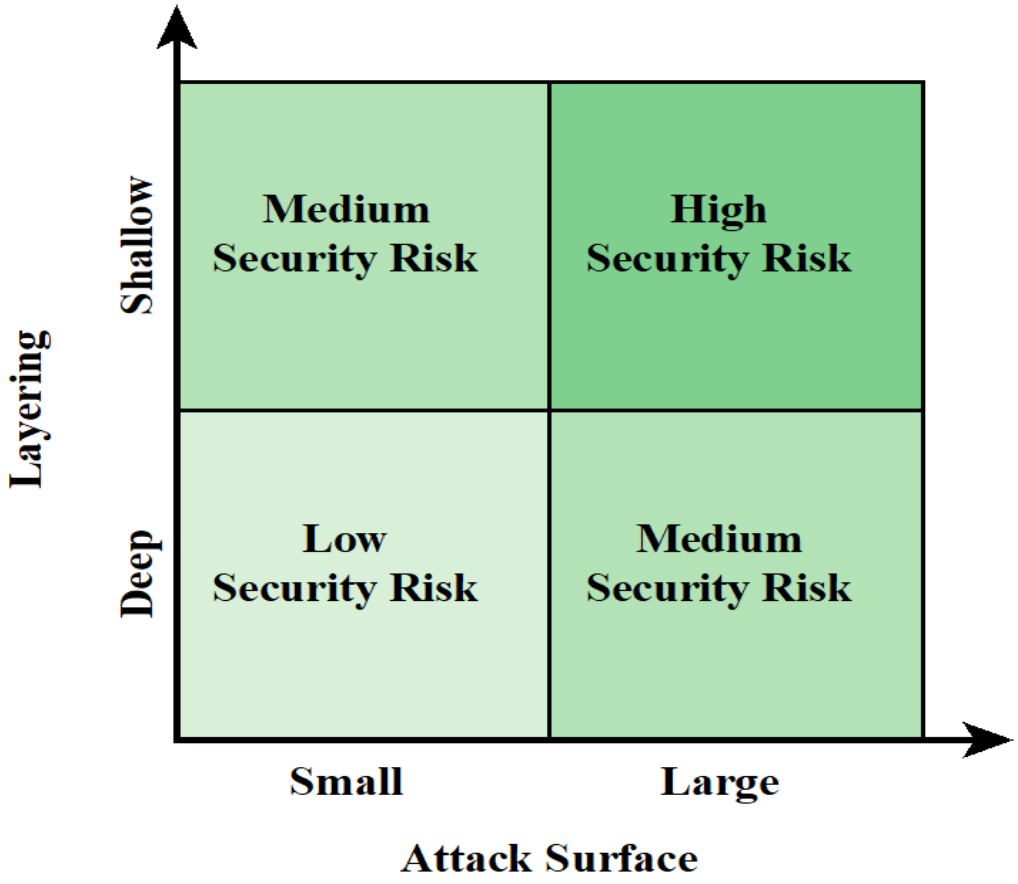
## Software Attack Surface

- Vulnerabilities in application, utility, or operating system code
- Particular focus is Web server software

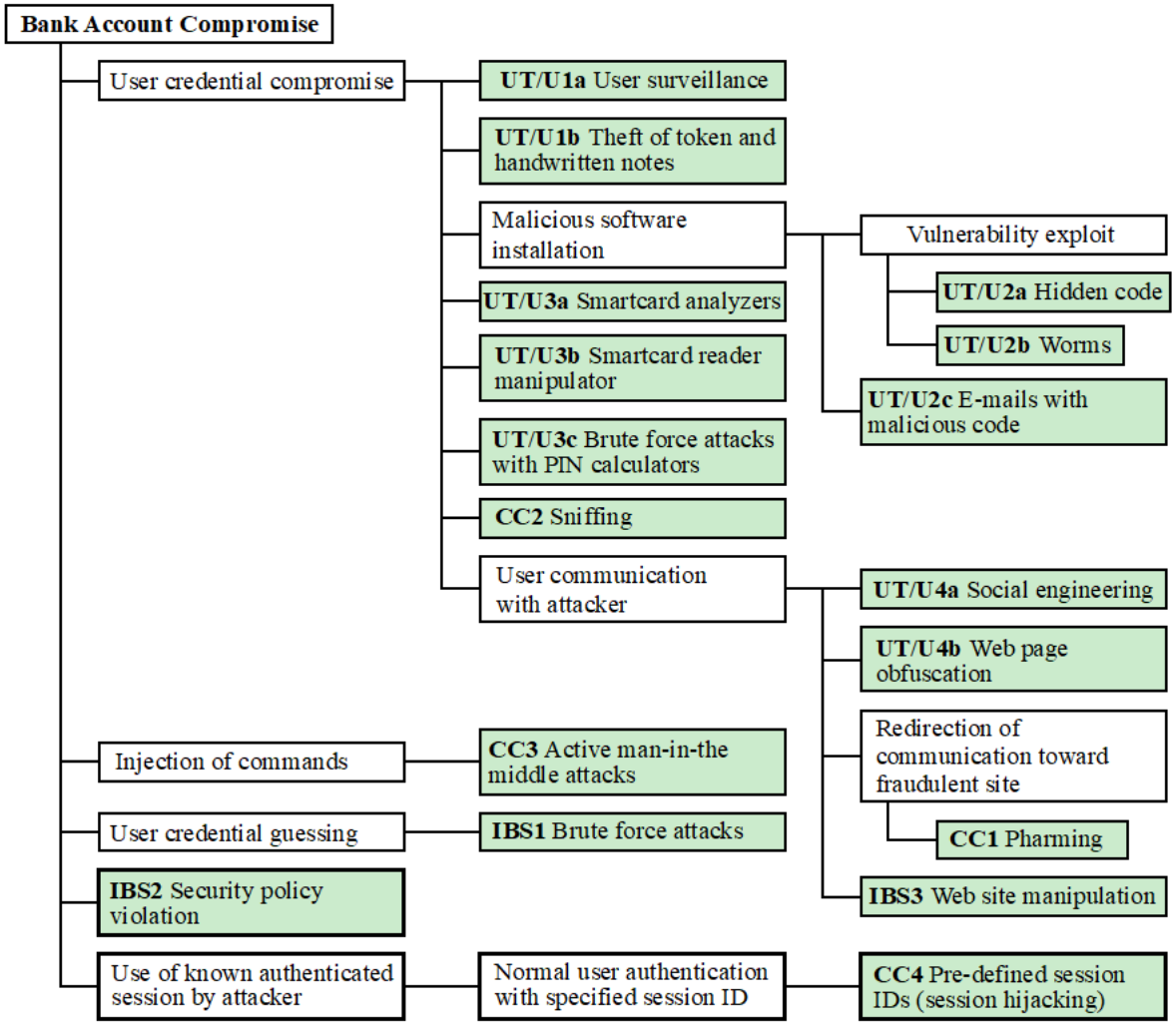
## Human Attack Surface

- Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

# Attack surfaces Categories



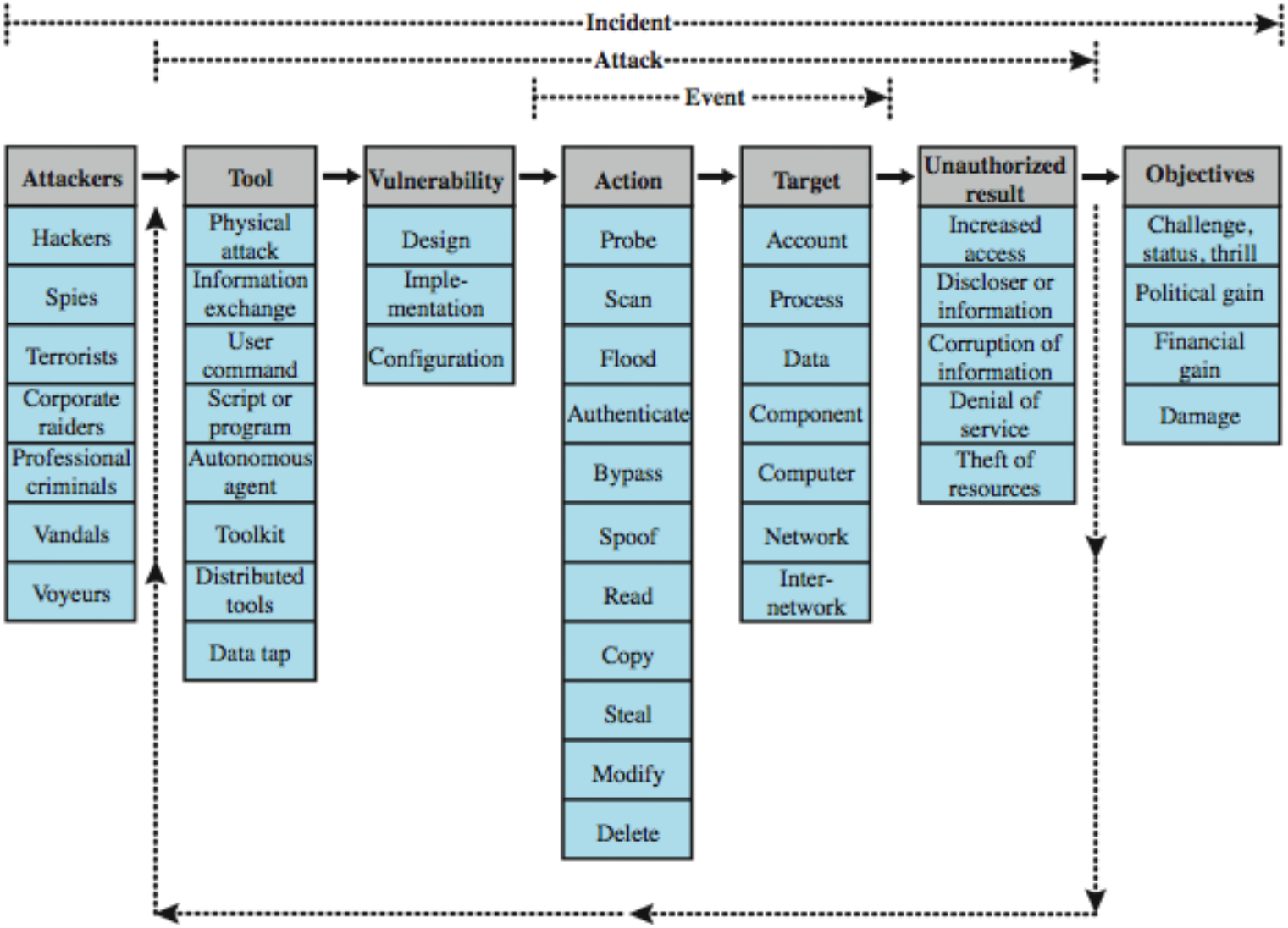
# Attacks example: Online banking



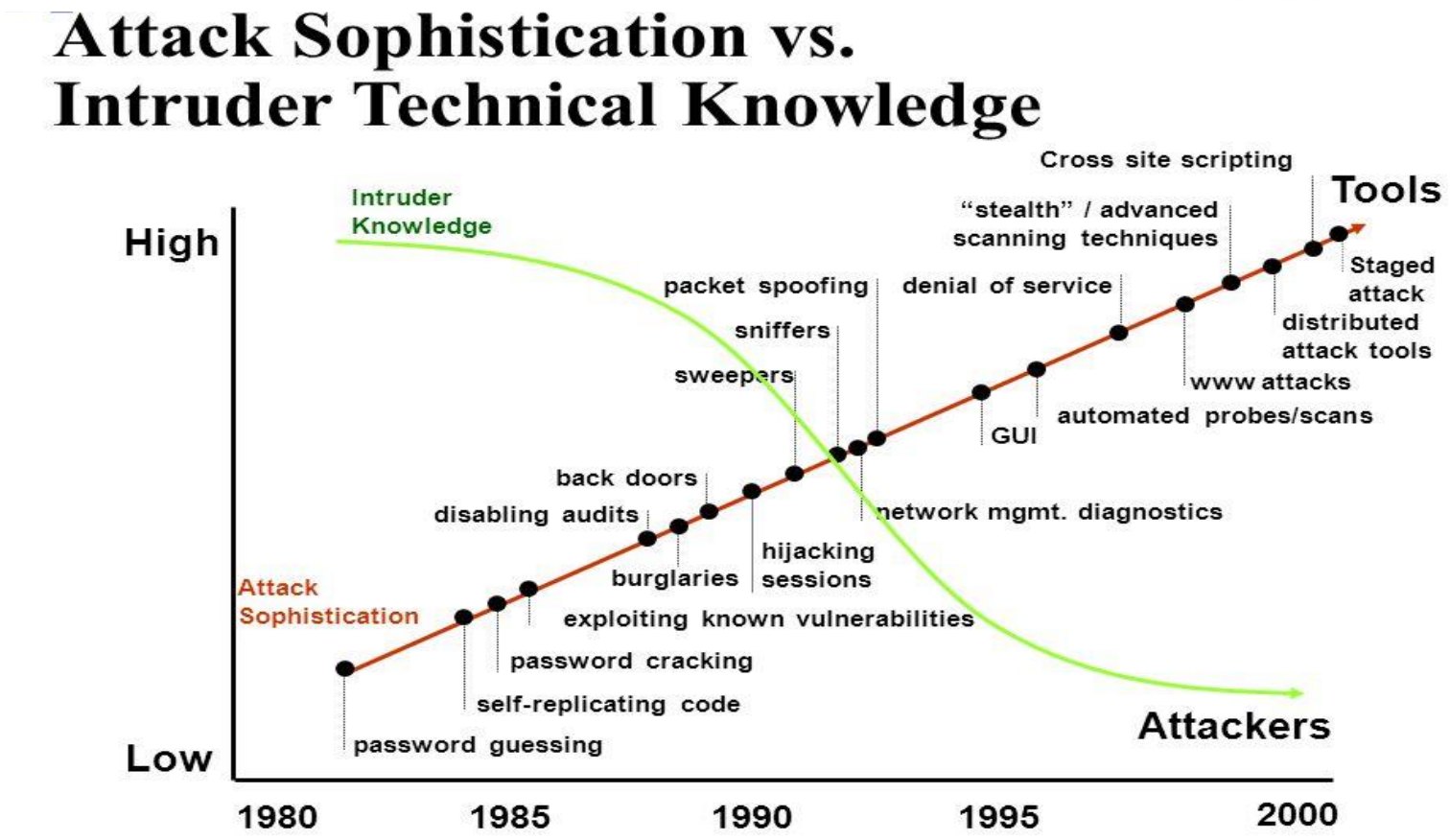
# X.800 Security Architecture

- X.800, *Security Architecture for OSI*
- systematic way of defining requirements for security and characterizing approaches to satisfying them
- defines:
  - security attacks - compromise security
  - security mechanism - act to detect, prevent, recover from attack
  - security service - counter security attacks

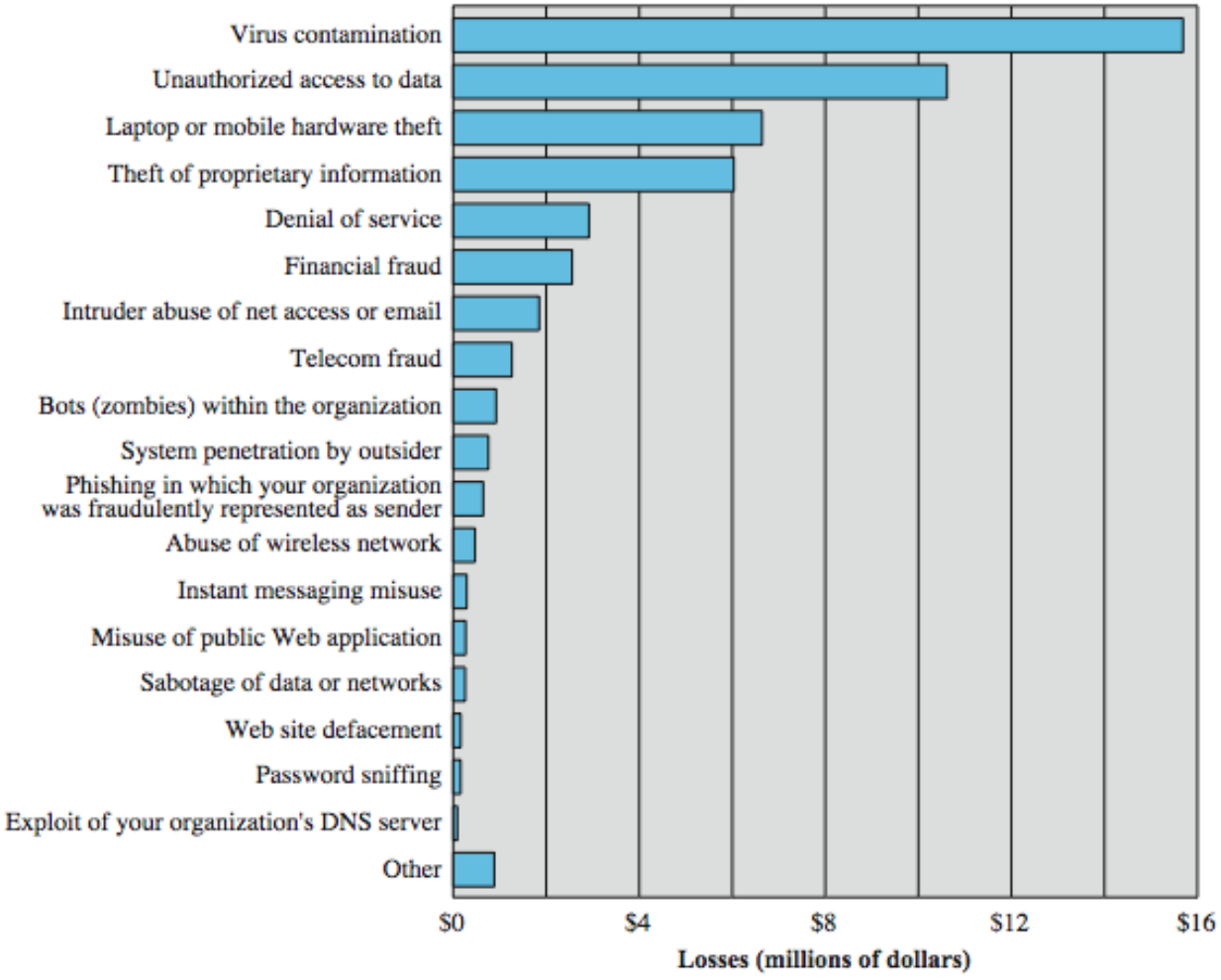
# Security Taxonomy



# Security Trends

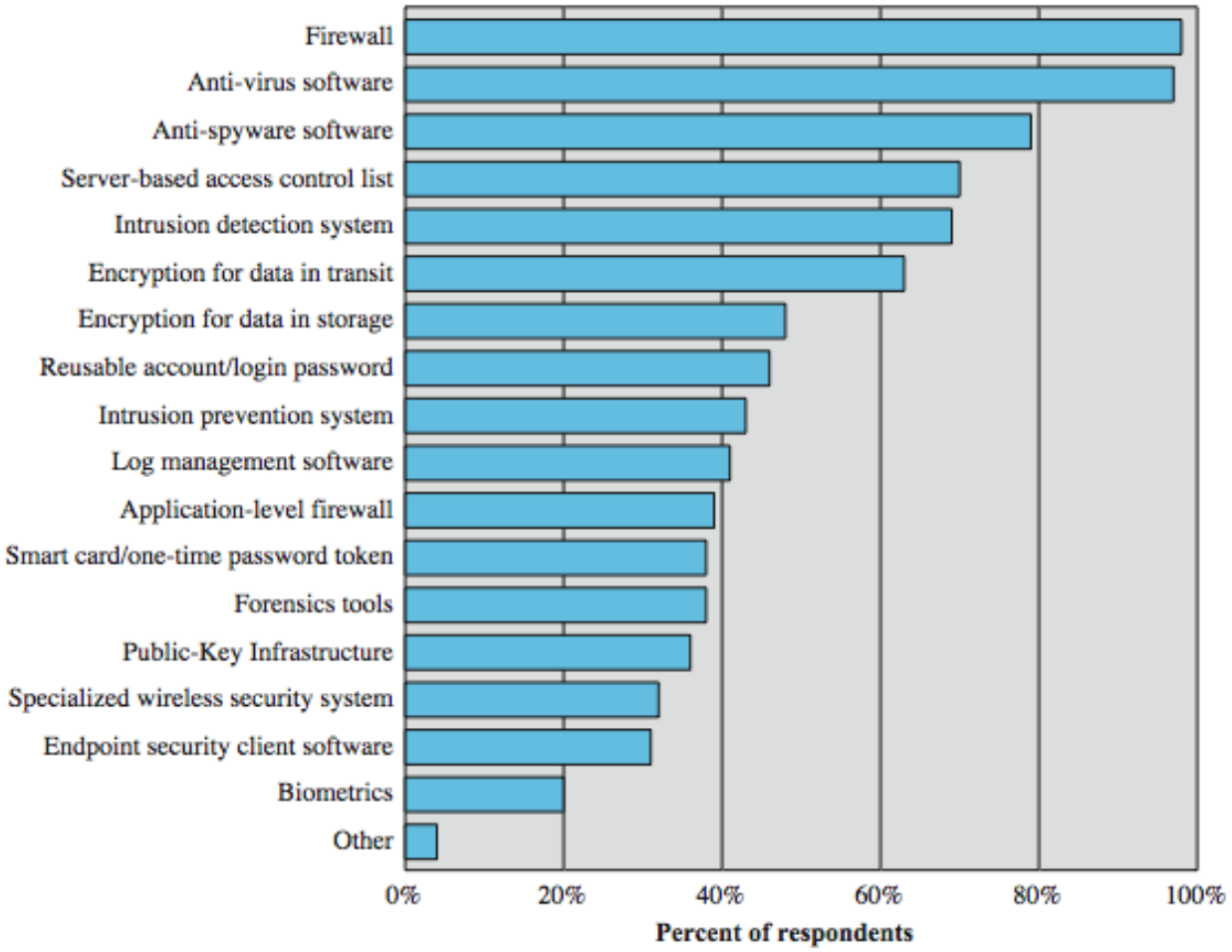


# Computer Security Losses




Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

# Security Technologies Used




Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

# Computer Security Strategy

- specification/policy
  - what is the security scheme supposed to do?
  - codify in policy and procedures
- implementation/mechanisms
  - how does it do it?
  - prevention, detection, response, recovery
- correctness/assurance
  - does it really work?
  - assurance, evaluation

# Summary

- security concepts
- terminology
- functional requirements
- security architecture
- security trends
- security strategy