Overview of Computer Security
Module 1

CSC 3207 Computer Security

Module 1 Outline

- What is Computer Security?
- Why study Computer Security?
- Objectives of Security - the CIA triad
- Terms: Assets, vulnerabilities and threats
- Attacks, controls and countermeasures
- Social engineering
- Security engineering
- *Security and Usability*
- *Security architecture*

What is Computer 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.
Information system resources include hardware, software, firmware, information/data, and telecommunications.

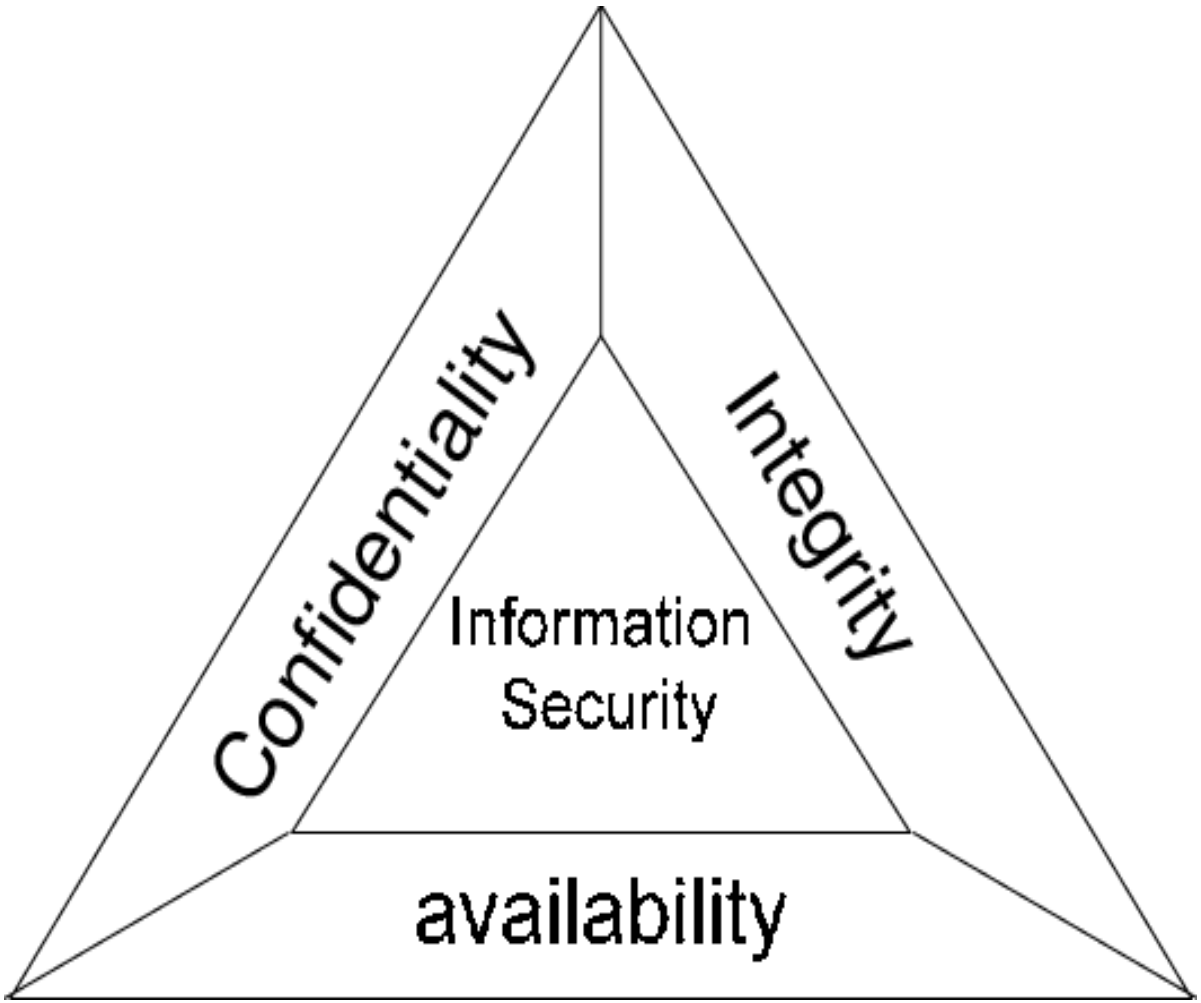
Why Study Computer Security?

- Cyber/computer security is about securing computers, digital information stored on computers, and services made possible by computers.
- Services including payments, water and electrical supplies, and processes in industry are increasingly dependent upon IT and their security is crucial.
- We hear news of digital attacks, leaked databases with private information, and new vulnerabilities almost on a daily basis. The attacks are progressively carried out by well-organized criminal hackers or even foreign powers instead of script kiddies or people who hack for fun.
- Cyber security experts are some of the most wanted specialists. Especially now that an increasing number of companies and governments are realizing how important computer security and privacy protection is.

Computer Security Objectives

- **Confidentiality**: prevention of unauthorized disclosure of information
- **Integrity**: prevention of unauthorized modification of information
- **Availability**: prevention of unauthorized withholding of information or resources.

CIA Triad


Confidentiality
Integrity
Information
Security
availability

Security Components - Confidentiality

- Confidentiality - the concealment of information or resources
- The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry
- access to information is restricted to those who need that information
- first formal work in computer security was motivated by the military's attempt to implement controls to enforce a "need to know" principle
  - This principle also applies to industrial firms, which keep their proprietary designs secure lest their competitors try to steal the designs
- All types of institutions keep personnel records secret.

Security Components - Confidentiality

- 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.
- Access control mechanisms support confidentiality
- One access control mechanism for preserving confidentiality is **cryptography**, which scrambles data to make itincomprehensible.
- A cryptographic key controls access to the unscrambled data, but then the cryptographic key itself becomes another datum to be protected.

Security Components - Integrity

- Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change
- Integrity includes data integrity(the content of the information) and origin integrity (the source of the data, often called authentication)
- Data integrity: Assures that information and programs are changed only in a specified and authorized manner
- System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- Example: A newspaper may print information obtained from a leak at the State House but attribute it to the wrong source. The information is printed as received(preserving data integrity), but its source is incorrect (corrupting origin integrity)

Security Components - Integrity

- Integrity mechanisms fall into two classes: *prevention* mechanisms and *detection* mechanisms
- **Prevention mechanisms** seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways
- **Detection mechanisms** do not try to prevent violations of integrity; they simply report that the data's integrity is no longer trustworthy

  - Detection mechanisms may analyze system events (user or system actions) to detect problems or (more commonly) may analyze the data itself to see if required or expected constraints still hold

  - The mechanisms may report the actual cause of the integrity violation (a specific part of a file was altered), or they may simply report that the file is now corrupt

Security Components - Availability

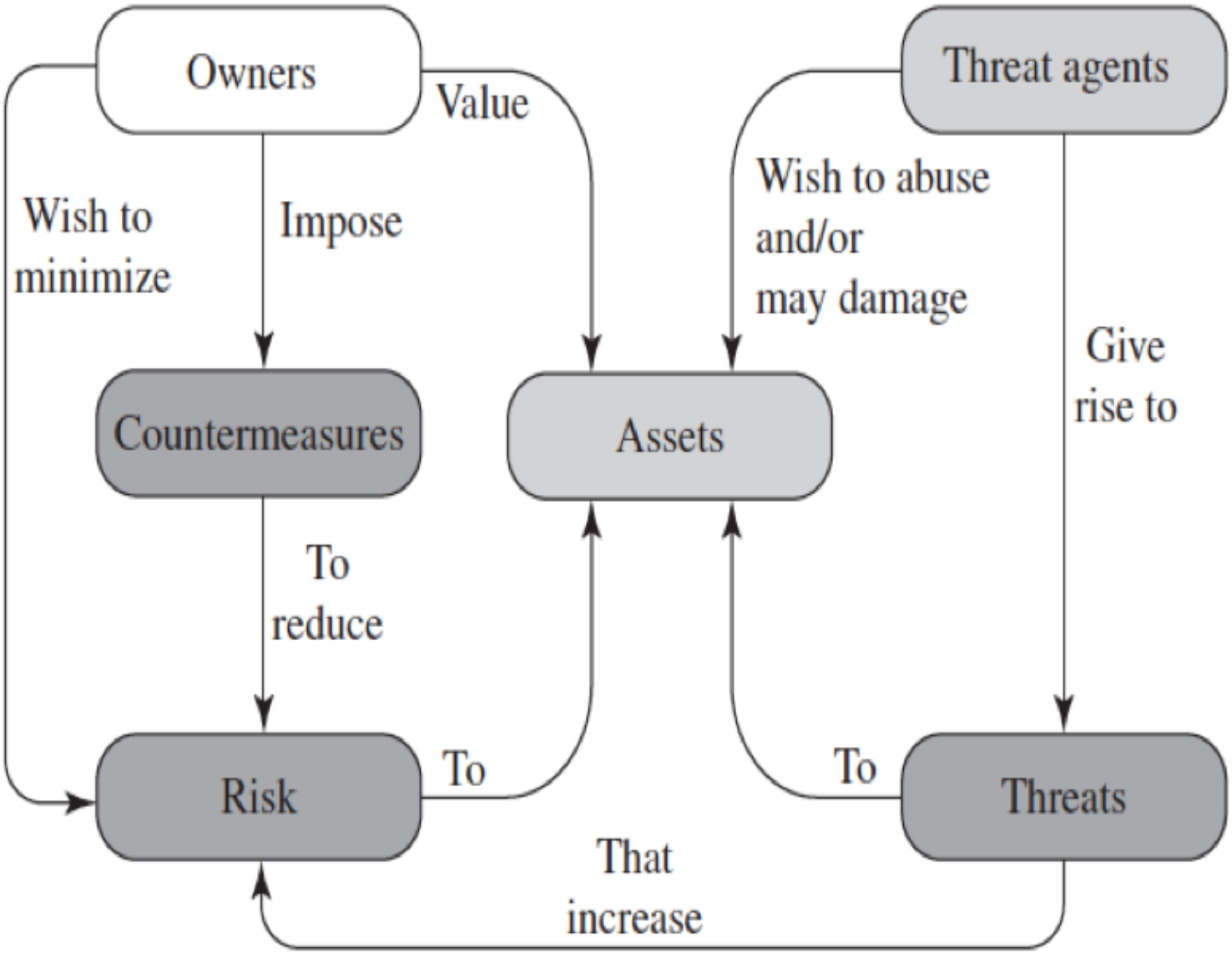
- Availability refers to the ability to use the information or resource desired.
- Assures that systems work promptly and service is not denied to authorized users.
- Is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all
- The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable
- Attempts to block availability, called **denial of service attacks**, can be the most difficult to detect, because the analyst must determine if the unusual access patterns are attributable to deliberate manipulation of resources or of environment

CIA Triad

Two additional security goals have been added to the original three in the CIA of security:

- **Authentication**: the ability of a system to confirm the identity of a sender.
  - The need for this in an online transaction is obvious
- **Nonrepudiation** or **accountability**: the ability of a system to confirm that a sender cannot convincingly deny having sent something.
  - The requirement for this capability in online transaction should also be readily apparent.

Computer Security Terms



Computer Assets

- Computer security is the protection of the items you value, called the **assets** of a computer or computer system.
- There are many types of assets, involving hardware, software, data, people, processes, or combinations of these.
- To determine what to protect, we must first identify what has value and to whom.
- Other assets—such as access to data, quality of service, processes, human users, and network connectivity—deserve protection, too; they are affected or enabled by the hardware, software, and data.

Other Assets

- Networks are specialized collections of hardware, software, and data.
  - Can easily multiply the problems of computer security
  - Insecure shared links
  - Inability to identify remote users (anonymity)
- Key People: People can be crucial weak points in security
  - If only one person knows how to use or maintain a particular program, trouble can arise if that person is ill, suffers an accident, or leaves the organization (taking her knowledge with her).

Computer Assets

Hardware:

- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:

- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:

- Documents
- Photos
- Music, videos
- Email
- Class projects

Threats

- **A threat** is a potential violation of security
- The violation need not actually occur for there to be a threat
- The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for). Those actions are called **attacks**. Those who execute such actions, or cause them to be executed, are called **attackers**
- A human who exploits a vulnerability perpetrates an **attack** on the system.
  - An attack can also be launched by another system, as when one system sends an overwhelming flood of messages to another, virtually shutting down the second system's ability to function

Threats

- The three security services—confidentiality, integrity, and availability—counter threats to the security of a system
- A **threat** to a computing system is a set of circumstances that has the potential to cause loss or harm.
  - Threats include human-initiated and computer-initiated ones, results of inadvertent human errors, hardware design flaws, software failures, and natural disasters.

Types of Attacks

There are two types of attacks: passive attacks and active attacks

- **Active attack**: An attempt to alter system resources or affect their operation.
  - it is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times
  - the goal is to detect them and to recover from any disruption or delays caused by them
  - involve some modification of the data stream or the creation of a false stream

Types of Attacks

- **Passive attack**: An attempt to learn or make use of information from the system that does not affect system resources
  - are difficult to detect,but measures are available to prevent their success.
  - are in the nature of eavesdropping on, or monitoring of, transmissions.
  - The goal of the attacker is to obtain information that is being transmitted

Types of Attacks

classify attacks based on the origin of the attack:

- **Inside attack**: Initiated by an entity inside the security perimeter (an " insider").
  - The insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
- **Outside attack**: Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider").

Classes of Threats

- Threats are divided into four broad classes:
  - **disclosure**: unauthorized access to information
  - **deception**: acceptance of false data
  - **disruption**: interruption or prevention of correct operation
  - **usurpation**: unauthorized control of some part of a system

Unauthorized disclosure

- **Unauthorized disclosure** is a circumstance or event whereby an entity gains access to data for which the entity is not authorized. Is a threat to confidentiality
- The following types of attacks can result in this threat consequence:
  - **Exposure**: Sensitive data are directly released to an unauthorized entity.
  - **Interception**: An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.
  - **Inference**: A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications.
  - **Intrusion**: An unauthorized entity gains access to sensitive data by circumventing a system's security protections.

Deception

- **Deception**: A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. Is a threat to either system or data integrity
- The following types of attacks can result in this threat consequence:
  - **Masquerade**: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.
  - **Falsification**: False data deceive an authorized entity.
  - **Repudiation**: An entity deceives another by falsely denying responsibility for an act.

Disruption

- **Disruption**: A circumstance or event that interrupts or prevents the correct operation of system services and functions. Is a threat to availability or system integrity
- The following types of attacks can result in this threat consequence:
  - **Incapacitation**: Prevents or interrupts system operation by disabling a system component.
  - **Corruption**: Undesirably alters system operation by adversely modifying system functions or data.
  - **Obstruction**: A threat action that interrupts delivery of system services by hindering system operation.

Usurpation

- **Usurpation**: A circumstance or event that results in control of system services or functions by an unauthorized entity. Is a threat to system integrity
- The following types of attacks can result in this threat consequence:
  - **Misappropriation**: An entity assumes unauthorized logical or physical control of a system resource.
  - **Misuse**: Causes a system component to perform a function or service that is detrimental to system security.

Denial of service

- Denial of service: a long-term inhibition of service, is a form of usurpation, although it is often used with other mechanisms to deceive
- The attacker prevents a server from providing a service
- The denial may occur at the source (by preventing the server from obtaining the resources needed to perform its function), at the destination(by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, or both)
- Denial of service poses the same threat as an infinite delay
- Availability mechanisms counter this threat

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.

Vulnerabilities

- A **vulnerability** is a weakness in the system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm.
- For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

Vulnerabilities of Computing Systems

- Hardware Vulnerabilities: adding devices, changing them, removing them, intercepting the traffic to them, or flooding them with traffic until they can no longer function. (many other ways to harm the hardware).
- Software Vulnerabilities: Software can be replaced, changed, or destroyed maliciously, or it can be modified, deleted, or misplaced accidentally. Whether intentional or not, these attacks exploit the software's vulnerabilities
- Data Vulnerabilities: data have a definite value, even though that value is often difficult to measure
  - Ex1: confidential data leaked to a competitor, may narrow a competitive edge
  - Ex2: flight coordinate data used by an airplane that is guided partly or fully by software. Can cost human lives if modified

Methods of Defense

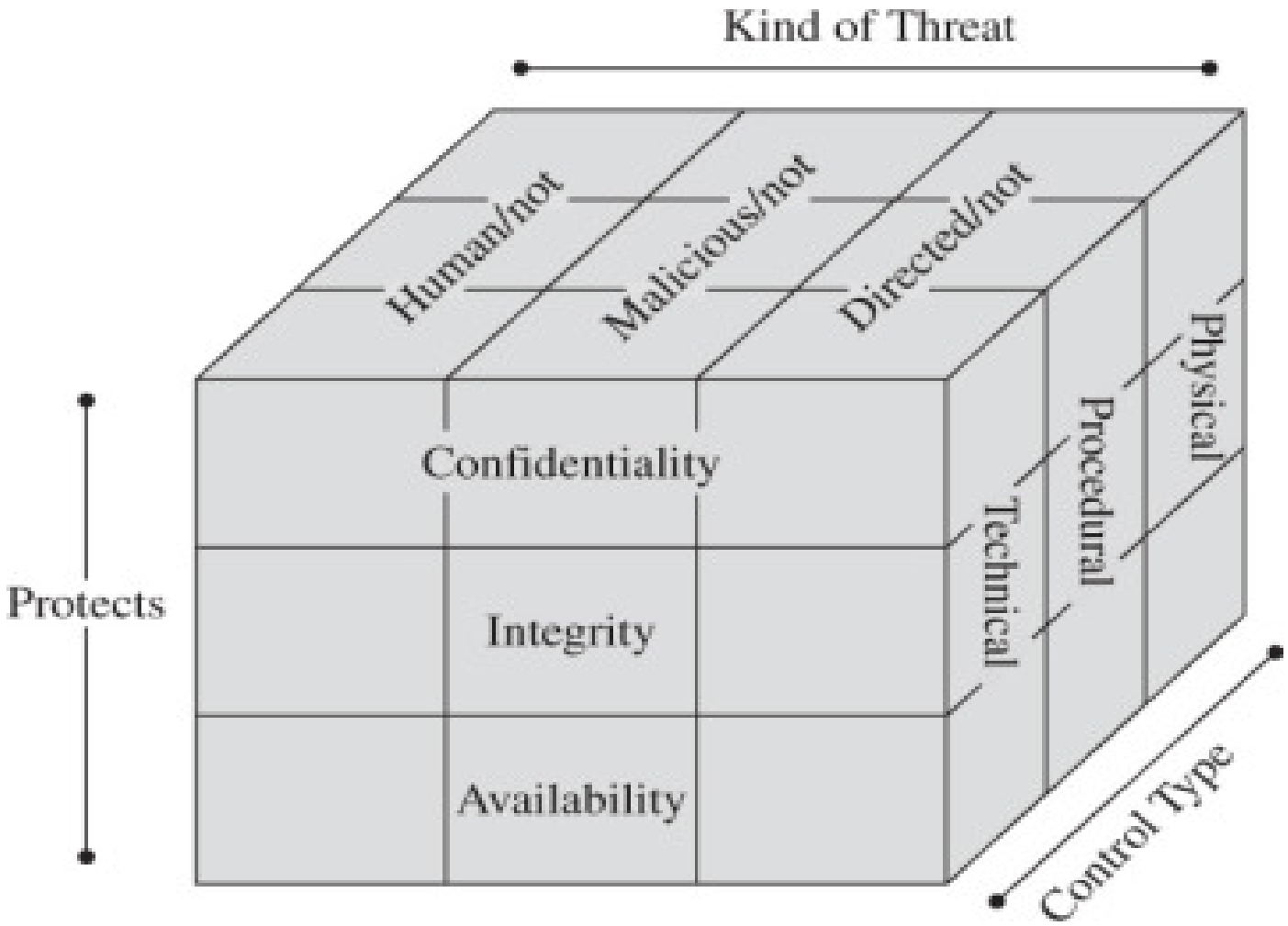
We can deal with harm in several ways:

- prevent it, by blocking the attack or closing the vulnerability
- deter it, by making the attack harder but not impossible
- deflect it, by making another target more attractive (or this one less so)
- mitigate it, by making its impact less severe
- detect it, either as it happens or some time after the fact
- recover from its effects

Types of Controls

- **Physical controls** stop or block an attack by using something tangible such as walls and fences, locks, (human) guards, sprinklers and other fire extinguishers
- **Procedural or administrative controls** use a command or agreement that requires or advises people how to act; for example,
  - laws, regulations
  - policies, procedures, guidelines
  – copyrights, patents
  – contracts, agreements
- **Technical controls** counter threats with technology (hardware or software), including passwords, program or operating system access controls, network protocols, firewalls, intrusion detection systems, encryption, network traffic flow regulators

Types of Countermeasures



Social Engineering

- The psychological manipulation of people into performing actions or divulging confidential information
- Social engineering attacks manipulate people into sharing information they shouldn't share, downloading software they shouldn't download, visiting websites they shouldn't visit, sending money to criminals, or making other mistakes that compromise their personal or organizational security
- Exploits human error or weakness rather than technical or digital system vulnerabilities

Social Engineering Examples

- An individual walks into a building and posts an official-looking announcement to the company bulletin that says the number for the help desk has changed. So, when employees call for help the individual asks them for their passwords and IDs thereby gaining the ability to access the company's private information
- The hacker contacts the target on a social networking site and starts a conversation with the target. Gradually the hacker gains the trust of the target and then uses that trust to get access to sensitive information like password or bank account details

Security Engineering

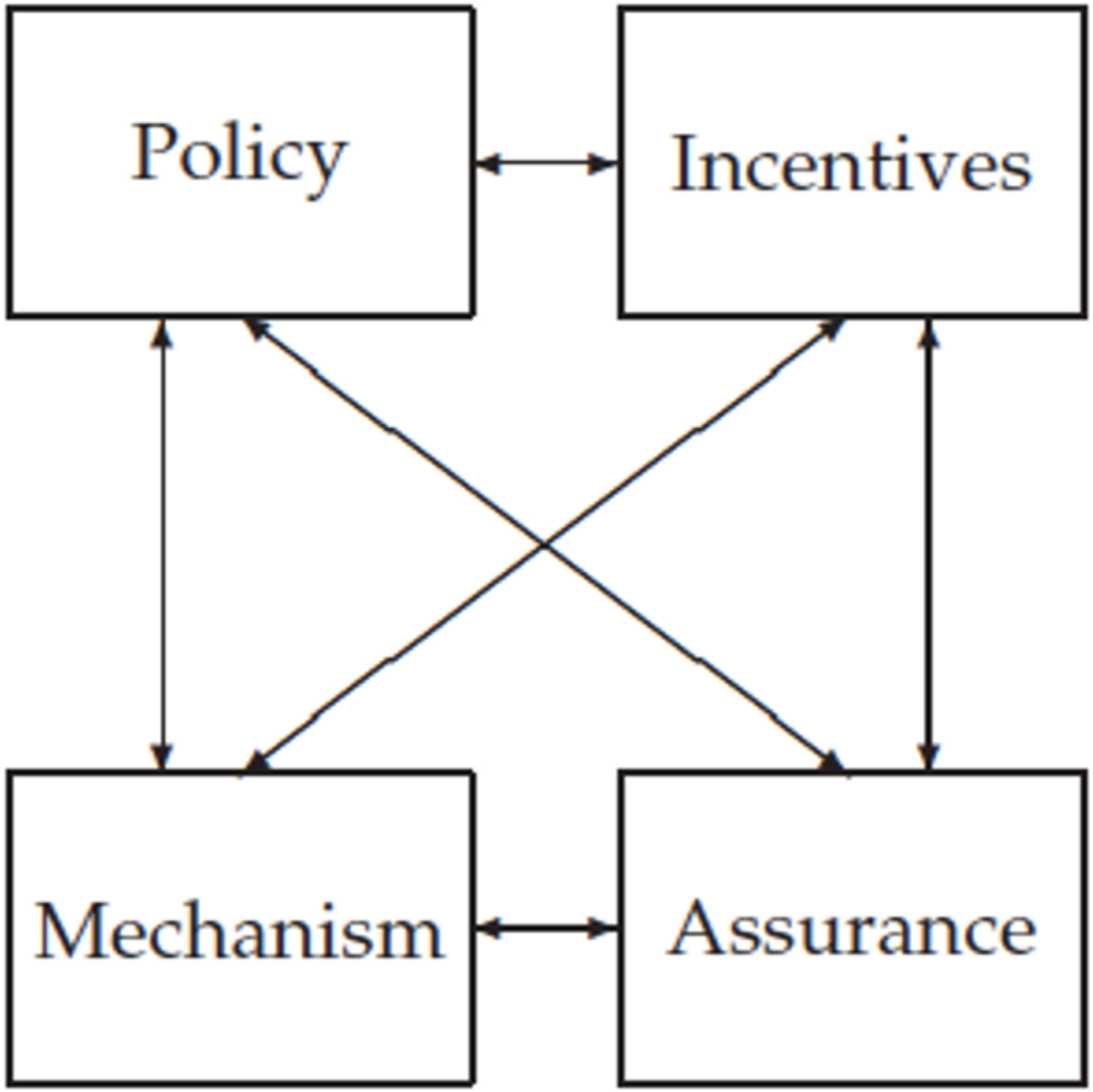
- Building systems to remain dependable in the face of malice, error, or mischance
- Focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves
- Is cross-disciplinary involving:
  - cryptography and computer security: hardware tamper-resistance, formal methods, knowledge of economics
  - applied psychology, organizations and the law
  - system engineering skills i.e business process analysis, software engineering, evaluation and testing

Security Engineering Framework

Good security engineering requires four things to come together

- Policy: what you're supposed to achieve
- Mechanism: the ciphers, access controls, hardware tamper-resistance and other machinery that you assemble in order to implement the policy
- Assurance: the amount of reliance you can place on each particular mechanism
- Incentive: the motive that the people guarding and maintaining the system have to do their job properly, and also the motive that the attackers have to try to defeat your policy

Security Engineering Framework



Discussion Questions

- What are the challenges of Computer Security?
- Giving relevant examples, describe the following social engineering attacks:
  - Pretexting
  - Phishing

References

- Chapter 1: Introduction to Computer Security by Matt Bishop