Information Security
Fall 2022

Week # 1

Lecture # 1, 2 and 3

Start date: Aug 23, 2022

Dr. Aqsa Aslam

CLO	Course Learning Outcome (CLO)	Domain	Taxonomy Level	PLO	Tools
01	**Explain** key concepts of information security such as design principles, cryptography, risk management, and ethics	Cognitive	C2 (Understanding)	1	A1, A2, M1, M2, P, F
02	**Discuss** legal, ethical, and professional issues in information security.	Cognitive	C2 (Applying)	2	A3, A4, P, M2, F
03	**Apply** various security and risk management tools for achieving information security and privacy.	Cognitive	C3 (Applying)	5	A3, A4 M2, P, F
04	**Identify** appropriate techniques to tackle and solve problems in the discipline of information security.	Cognitive	C4 (Analyzing)	2	A1, A2, M1, M2, P, F
Tool: A = Assignment, P = Project, M = Mid-term (M1 and M2), F=Final (End-term)					

Week #	Topic	Reference Text
1	**Information Security Foundations**: Concepts, Threats and Attacks, Design Principles, Strategy and Standards	Main Textbook, Chapter 1 Sections 1.1, 1.2, 1.4, 1,6, 1,7
2	**Cryptographic Tools**: Confidentiality with Symmetric Encryption, Message Authentication and Hash Functions	Textbook Chapter 2, Sections 2.1 and 2.2 Details in Chapter 20 & 21
3	**Cryptographic Tools:** Public Key Encryption **ASSIGNMENT # 1**	Textbook Chapter 2, Section 2.3 Details in Chapter 21
4	**Cryptographic Tools:** Digital Signatures and Key Management	Textbook Chapter 2, Sections 1.1 and 1.2
5	**User Authentication:** Digital User Authentication Principles, Password based authentication **ASSIGNMENT # 2**	Textbook Chapter 3, Sections 3.1 to 3.6
MIDTERM-I EXAM		

6	**User Authentication:** Token-based, and Biometric authentication and related security issues	Textbook Chapter 3, Sections 3.1 to 3.6
7	**Access Control**: Principles, Discretionary Access Control, Role-based Access Control and Attribute based Access Control **ASSIGNMENT # 3**	Textbook Chapter 4, Sections 4.1 to 4.7
8	**Database Security:** Need, SQL Injection Attacks, Database Access Control and Database Encryption	Textbook Chapter 5, Sections 5.1 to 5.7
9	**Malicious Software:** Types, Propagation, Payload, and Countermeasures **ASSIGNMENT # 4**	Textbook Chapter 6, Sections 6.1 to 6.10
MIDTERM-II EXAM		

10	**Intrusion Detection**: Basics, Types and Examples	Textbook Chapter 8, Sections 8.1 to 8.6
11	**Firewalls and Intrusion Prevention**: Basics, Types, and Prevention Systems	Textbook Chapter 9, Sections 9.1 to 9.3 and 9.6
12	**Software Security:** Software Vulnerabilities and Protection Mechanisms	Textbook Chapter 11, Sections 11.1 to 11.3
13	**IT Security Management and Risk Assessment:** security policies, policy formation and enforcement, risk assessment	Textbook Chapter 14, Sections 14.1 to 14.3
14	**Legal and Ethical Aspects:** Cybercrime, Intellectual Property, Privacy and Anonymity of Data and Ethical Issues. **PROJECT SUBMISSION**	Textbook Chapter 14, Sections 19.1 to 19.4
15	**Topics of Current Interests (Research Topics)** **PROJECT PRESENTATIONS**	IEEE/ ACM and other digital libraries
	END-TERM EXAM	

Assessment Instruments with Weights (homework, quizzes, midterms, final, programming assignments, lab work, etc.)	Labs / Assignments – 10% (minimum 4 Assignments) Project – 10% Mid-Term 1 Exam – 15% Mid-Term 2 Exam – 15% End-Term Exam – 50%

Textbook (or **Laboratory Manual** for Laboratory Courses)	1– Computer Security, Principles and Practice, William Stallings, 4th Edition, Pearson Publication, 2018 (Main Textbook for Theory) 2- Computer and Internet Security, A Hands-On Approach, Wenliang Du, 3rd Edition, Create Space Publications, 2022 (for labs)

Late Submission & Plagiarism Policy Policy	Deadlines are meant to be strictly followed. Any late submission (without and valid reason and justification/ evidence) will be penalized. **The penalty will be 50%. Any delay of more than a week would mean ZERO credit in that particular assessment (assignments, labs, project). Plagiarized assignment will get you ZERO credit.**

CHAPTER 1

OVERVIEW

LEARNING OBJECTIVES

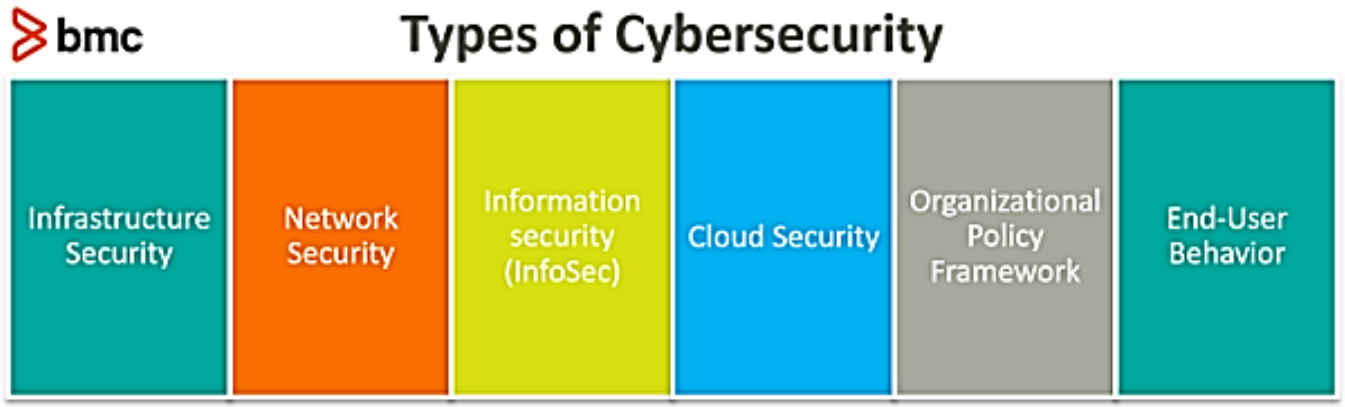
After studying this chapter, you should be able to:

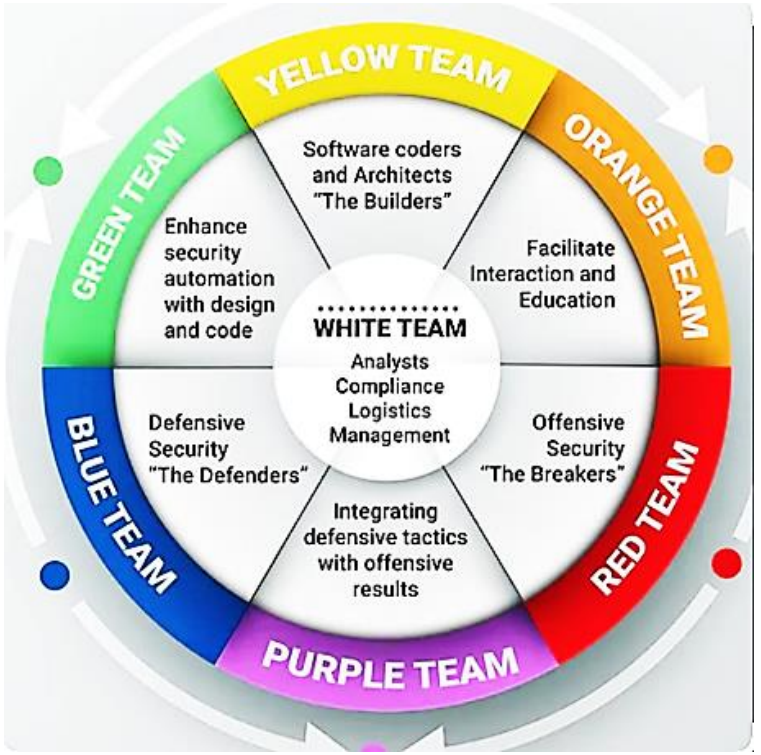
- Describe the key security requirements of confidentiality, integrity, and availability.
- Discuss the types of security threats and attacks that must be dealt with and give examples of the types of threats and attacks that apply to different categories of computer and network assets.
- Summarize the functional requirements for computer security.
- Explain the fundamental security design principles.
- Discuss the use of attack surfaces and attack trees.
- Understand the principle aspects of a comprehensive security strategy.

A Definition of Computer Security

The NIST Internal/Interagency Report NISTIR 7298 (*Glossary of Key Information Security Terms*, May 2013) defines the term *computer security* as follows:

> **Computer Security:** Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.





This definition introduces three key objectives that are at the heart of computer security:

- **Confidentiality:** This term covers two related concepts:

  — **Data confidentiality:**[1] 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.

- **Integrity:** This term covers two related concepts:

  — **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.

- **Availability:** Assures that systems work promptly and service is not denied to authorized users.

These three concepts form what is often referred to as the **CIA triad**. The three concepts embody the fundamental security objectives for both data and for information and computing services. For example, the NIST standard FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*, February 2004) lists confidentiality, integrity, and availability as the three security objectives for information and for information systems. FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

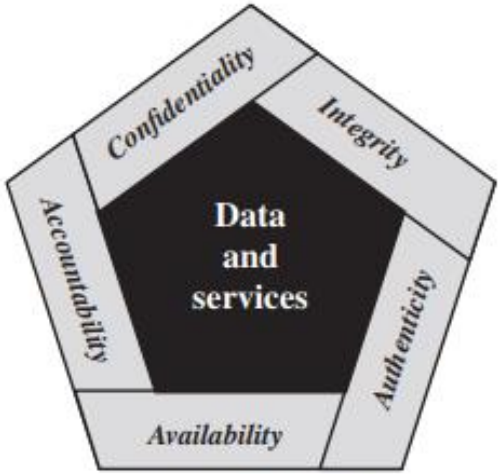


Figure 1.1 **Essential Network and Computer Security Requirements**

three levels of impact on organizations

- Low
- Moderate
- High

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture (see Figure 1.1). Two of the most commonly mentioned are as follows:

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Note that FIPS 199 includes authenticity under integrity.

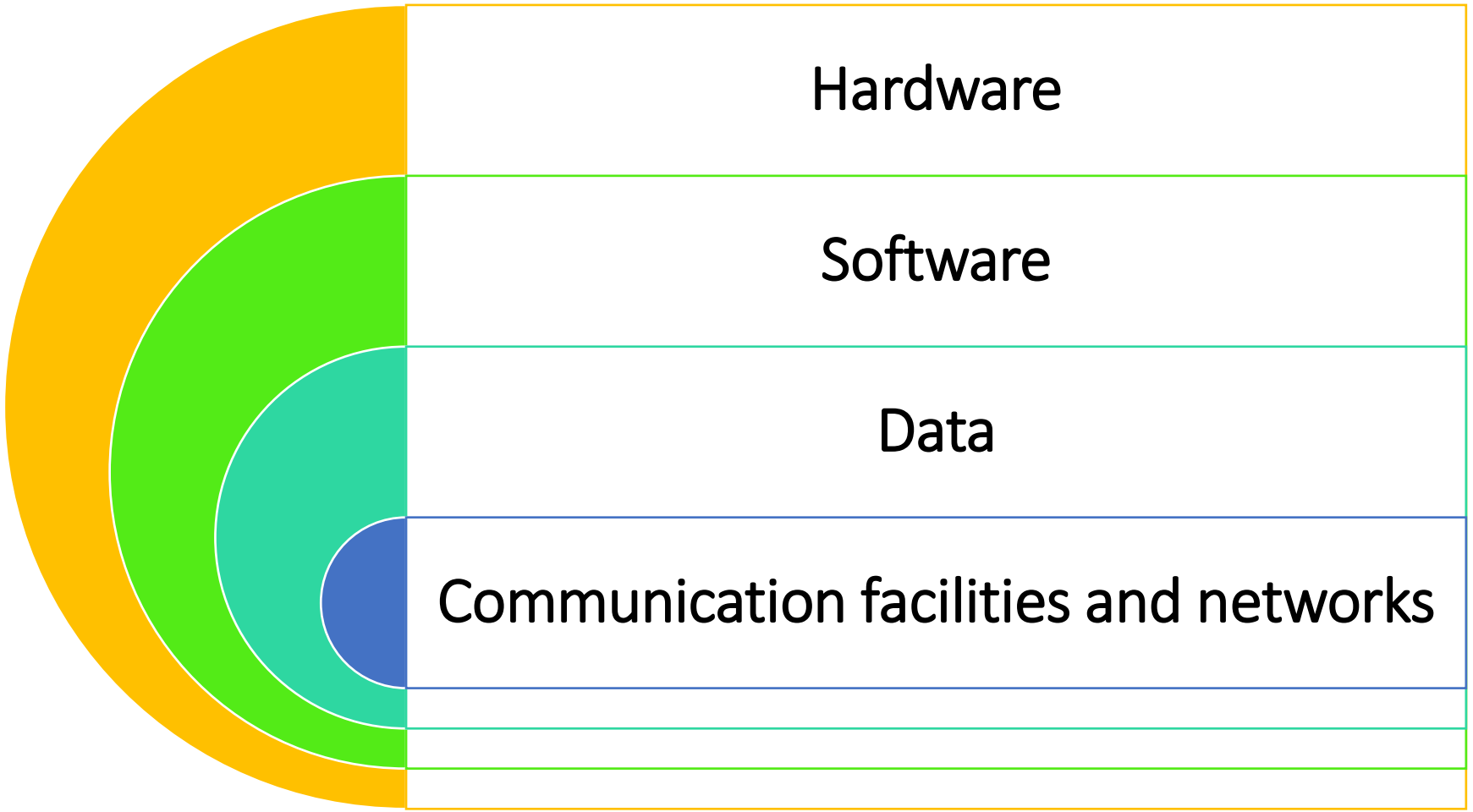
FIPS (**Federal Information Processing Standards**)

The Challenges of Computer Security

Computer security is both fascinating and complex. Some of the reasons are as follows:

1. Computer security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory one-word labels: confidentiality, authentication, nonrepudiation, and integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
3. Because of Point 2, the procedures used to provide particular services are often counterintuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. Only when the various aspects of the threat are considered do elaborate security mechanisms make sense.
4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].
5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There may also be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.
6. Computer security is essentially a battle of wits between a perpetrator who tries to find holes, and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
8. Security requires regular, even constant monitoring, and this is difficult in today's short-term, overloaded environment.
9. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process.
10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

A Model for Computer Security



Vulnerabilities, Threats and Attacks

- **Categories of vulnerabilities**
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)
- **Threats**
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- **Attacks (threats carried out)**
  - Passive – attempt to learn or make use of information from the system that does not affect system resources
  - Active – attempt to alter system resources or affect their operation
  - Insider – initiated by an entity inside the security parameter
  - Outsider – initiated from outside the perimeter

Countermeasures

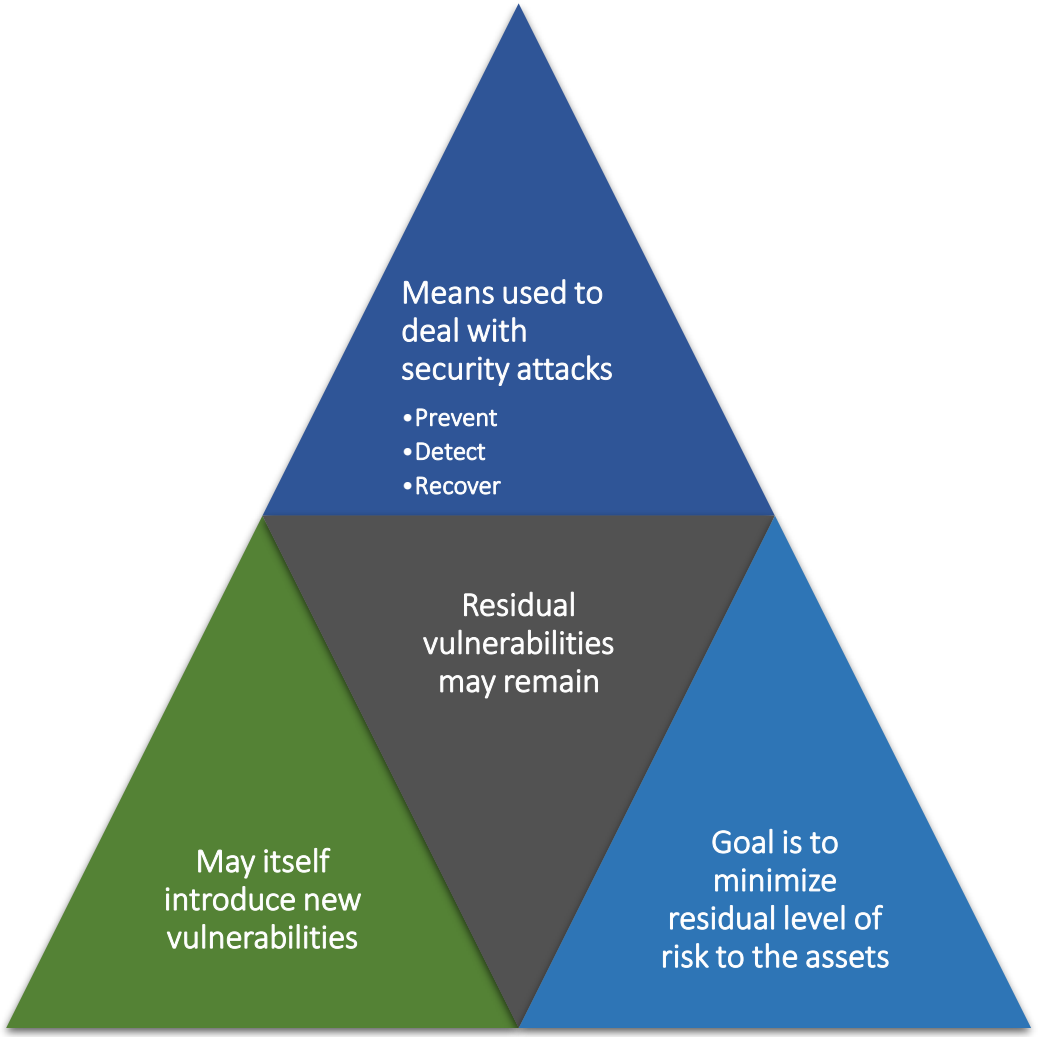


Table 1.1 **Computer Security Terminology**

Adversary (threat agent)
Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Attack
Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Countermeasure
A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

Security Policy
A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

System Resource (Asset)
A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

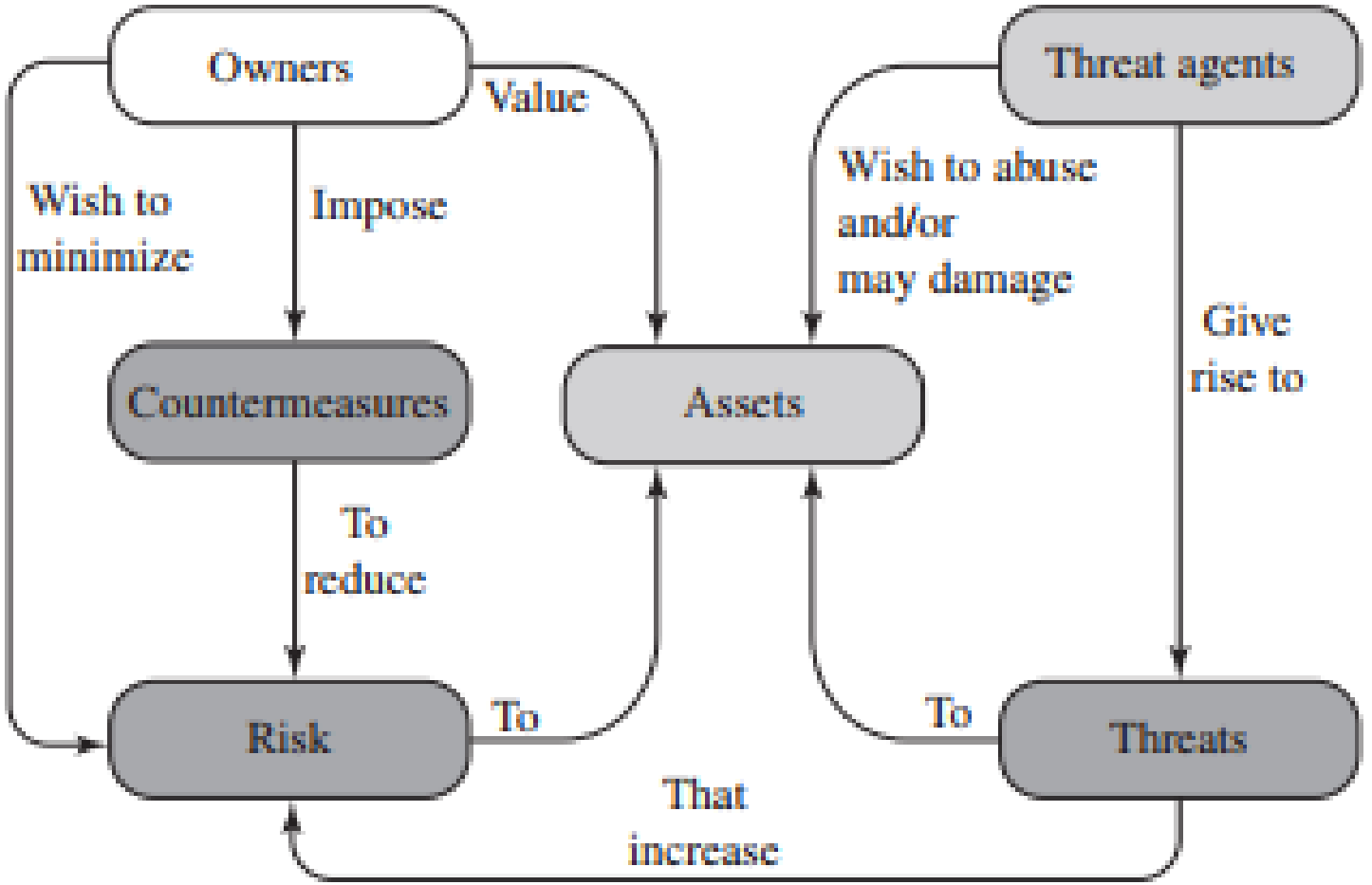


Figure 1.2 Security Concepts and Relationships

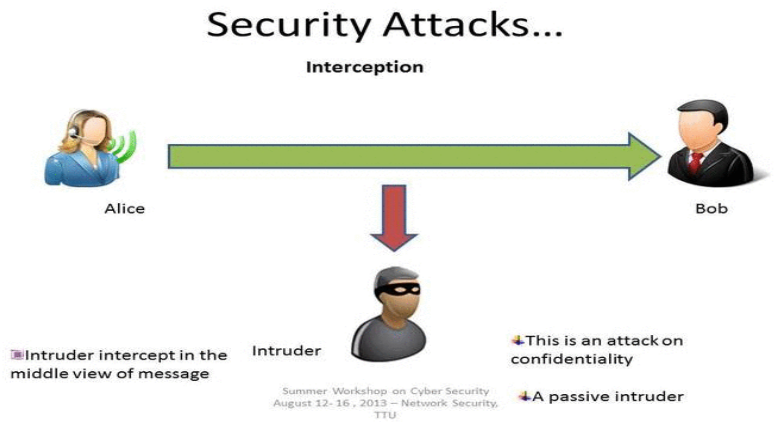
Table 1.2 **Threat Consequences, and the Types of Threat Actions that Cause Each Consequence**

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**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 A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**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 A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**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 A circumstance or event that results in control of system services or functions by an unauthorized entity.	**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.

Source: Based on RFC 4949

Threat Consequences, and the Types of Threat Actions that Cause Each Consequence

- **Unauthorized Disclosure** → *is a threat to confidentiality.*
  - **Exposure:** This can be deliberate, as when an insider intentionally releases sensitive information
    - **Examples:** credit card numbers, to an outsider.
    - It can also be the result of a human, hardware, or software error, which results in an entity gaining unauthorized knowledge of sensitive data.
  - **Interception Attack**
    - **Examples:** On the Internet, a determined hacker can gain access to e-mail traffic and other data transfers.
      - Create the potential for unauthorized access to data.
    - Packet sniffing and key logging to capture data from a computer system or network

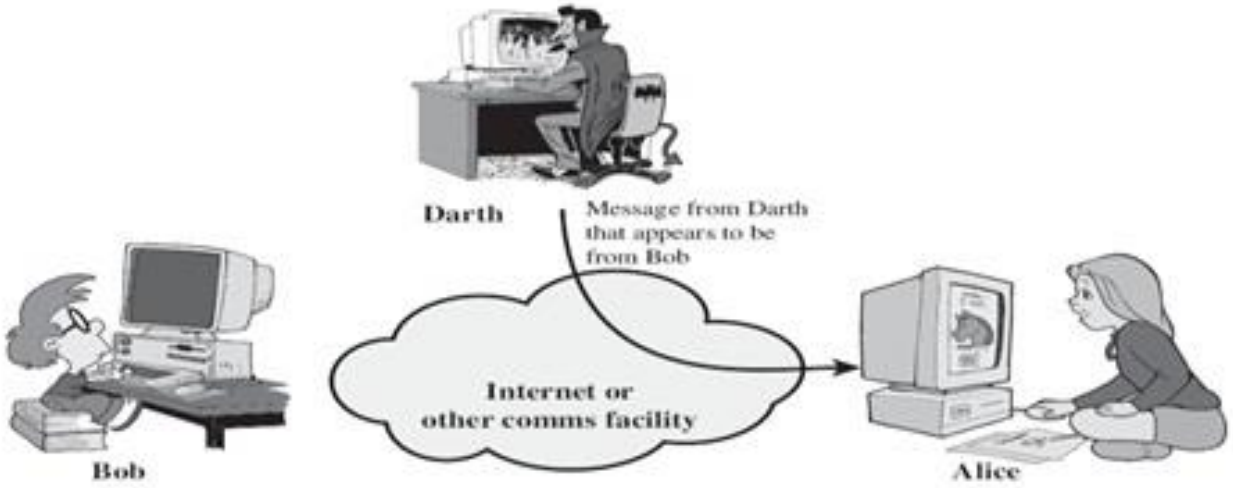


Threat Consequences, and the Types of Threat Actions that Cause Each Consequence

- **Unauthorized Disclosure:**
  - **Inference Attack**
    - **Examples:** An example of inference is known as traffic analysis
      1. Adversary is able to gain information from observing the pattern of traffic on a network
         - Such as the amount of traffic between particular pairs of hosts on the network.
      2. Another example is the inference of detailed information from a database by a user who has only limited access
         - This is accomplished by repeated queries whose combined results enable inference.
  - **Intrusion Attack**
    - **Examples:** An example of intrusion is an adversary gaining unauthorized access to sensitive data by overcoming the system's access control protections.
      -

Threat Consequences, and the Types of Threat Actions that Cause Each Consequence

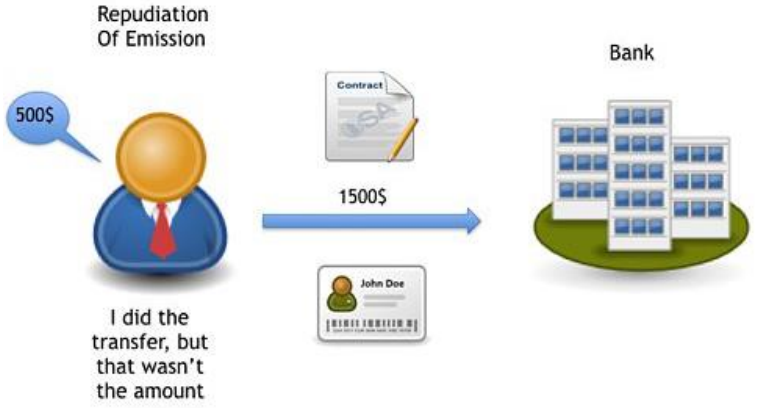
- **Deception:** *Deception is a threat to either system integrity or data integrity.*
  - **Masquerade:**
    - One example of masquerade is an attempt by an unauthorized user to gain access to a system by posing as an authorized user
      - This could happen if the unauthorized user has learned another user's logon ID and password.



Masquerade

Threat Consequences, and the Types of Threat Actions that Cause Each Consequence

- **Deception**
  - **Falsification:** Altering or replacing of valid data or the introduction of false data into a file or database.
    - For example, a student may alter his or her grades on a school database
  - **Repudiation:**
    - In this case, a user either denies sending data, or a user denies receiving or possessing the data.
    - An example of a repudiation attack might be someone accessing your e-mail server and sending inflammatory information to others.
      - This information can prove embarrassing to you or your company if this happens.



Threat Consequences, and the Types of Threat Actions that Cause Each Consequence

- **Disruption:** *Disruption is a threat to availability or system integrity.*
  - **Incapacitation:** This is an attack on system availability.
    - *This could occur as a result of physical destruction of or damage to system hardware.*
    - **Example:** Malicious software, such as Trojan horses, viruses, or worms, could operate in such a way as to disable a system or some of its services.
  - **Corruption:** This is an attack on system integrity.
    - *Malicious software in this context could operate in such a way that system resources or services function in an unintended manner.*
      - Or a user could gain unauthorized access to a system and modify some of its functions.
    - **Example:** a user placing backdoor logic in the system to provide subsequent access to a system and its resources by other than the usual procedure.
  - **Obstruction:** One way to obstruct system operation is to interfere with communications by disabling communication links or altering communication control information.
    - Another way is to overload the system by placing excess burden on communication traffic or processing resources.

Threat Consequences, and the Types of Threat Actions that Cause Each Consequence

- **Usurpation:** *is a threat to system integrity*
  - **Misappropriation:** This can include theft of service.
    - **Example:** a distributed denial of service attack, when malicious software is installed on a number of hosts to be used as platforms to launch traffic at a target host.
      - In this case, the malicious software makes unauthorized use of processor and operating system resources.
  - **Misuse:** Misuse can occur by means of either malicious logic or a hacker that has gained unauthorized access to a system.
    - In either case, security functions can be disabled or thwarted.

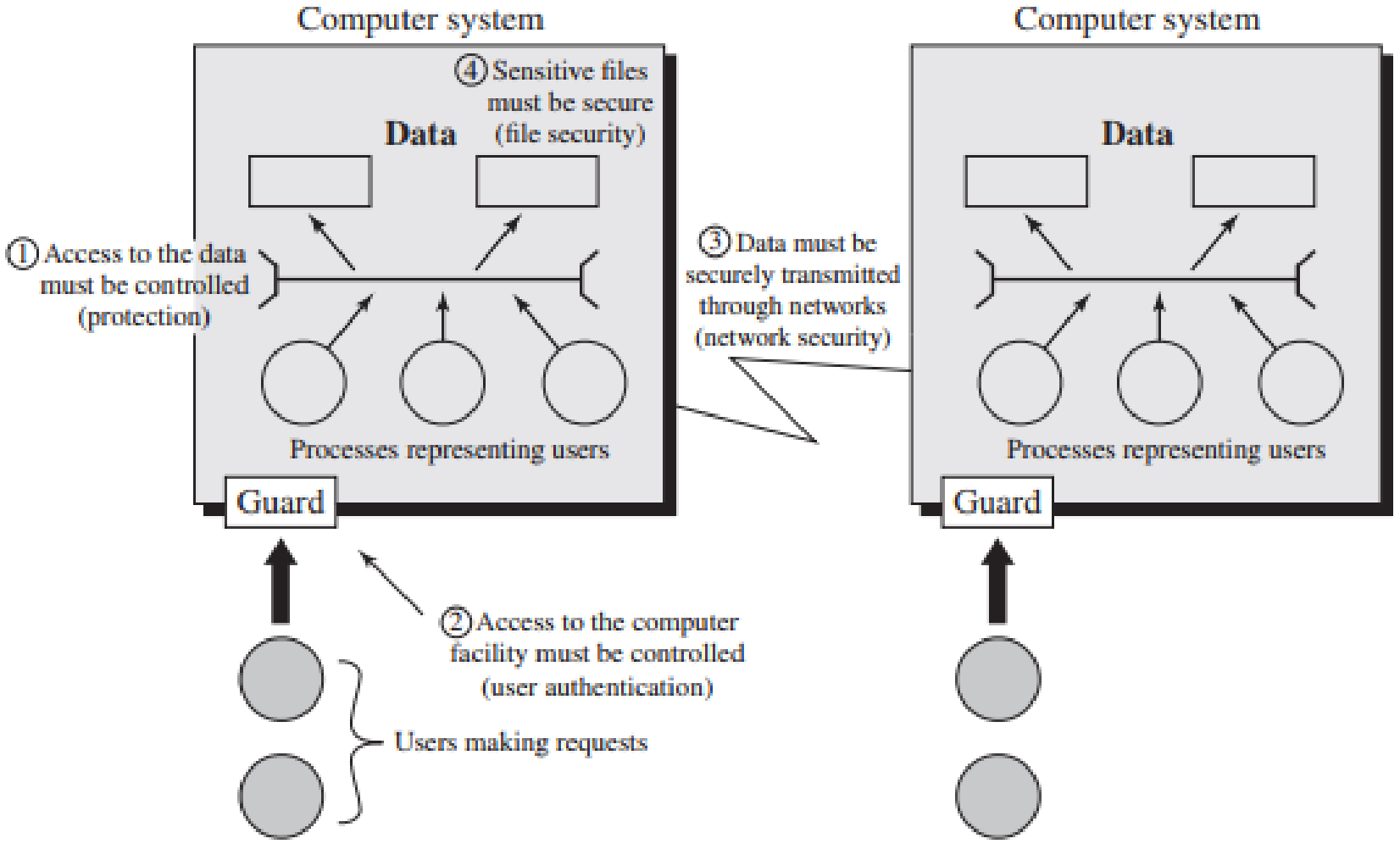


Figure 1.3 **Scope of Computer Security**

Note: This figure depicts security concerns other than physical security, including controlling of access to computers systems, safeguarding of data transmitted over communications systems, and safeguarding of stored data.

Table 1.3 **Computer and Network Assets, with Examples of Threats**

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted USB drive 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.

1.4 FUNDAMENTAL SECURITY DESIGN PRINCIPLES

Despite years of research and development, it has not been possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions. In the absence of such foolproof techniques, it is useful to have a set of widely agreed design principles that can guide the development of protection mechanisms. The National Centers of Academic Excellence in Information Assurance/Cyber Defense, which is jointly sponsored by the U.S. National Security Agency and the U. S. Department of Homeland Security, list the following as fundamental security design principles [NCAE13]:

- 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

1.6 COMPUTER SECURITY STRATEGY

We conclude this chapter with a brief look at the overall strategy for providing computer security. [LAMP04] suggests that a comprehensive security strategy involves three aspects:

- **Specification/policy:** What is the security scheme supposed to do?
- **Implementation/mechanisms:** How does it do it?
- **Correctness/assurance:** Does it really work?

1.7 STANDARDS

- **National Institute of Standards and Technology:** 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. Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact.

- **ITU-T:** The International Telecommunication Union (ITU) is a United Nations agency in which governments and the private sector coordinate global telecom networks and services. The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU. ITU-T's mission is the production of standards covering all fields of telecommunications. ITU-T standards are referred to as Recommendations.

- **Internet Society:** ISOC is a professional membership society with worldwide organizational and individual membership. It 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, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). These organizations develop Internet standards and related specifications, all of which are published as Requests for Comments (RFCs).

- **ISO:** The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from more than 140 countries. ISO is a nongovernmental organization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity. ISO's work results in international agreements that are published as International Standards.