Computer and Network Security Concepts

Instructor: C. Pu (Ph.D., Assistant Professor)

puc@marshall.edu

Computer Security Concepts

- **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 (includes hardware, software, firmware, information/data, and telecommunications).
    - A Definition of Computer Security from The NIST Computer Security Handbook

Computer Security Concepts

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

Computer Security Concepts

- This definition introduces *three key objectives* that are at the heart of computer security:
  - **Integrity**:
    - **Data integrity**: Assures that information (both stored and in transmitted packets) 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.

Computer Security Concepts

- These three concepts form what is often referred to as the ***CIA*** triad.

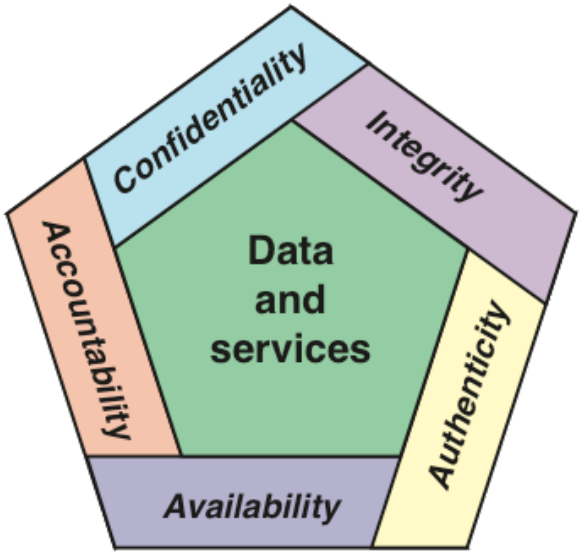
- The three concepts embody the fundamental security objectives for both **data** and for **information and computing services**.
  - The NIST standard FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems) lists confidentiality, integrity, and availability as the three security objectives for information and for information systems.

Computer Security Concepts

- 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.

Computer Security Concepts

- 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



Essential Network and Computer Security Requirements

Computer Security Concepts

- 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 afteraction 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.

Computer Security Concepts

- Three levels of **impact** on organizations or individuals are defined in FIPS 199:
  - **Low**: The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
    - A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might
      - (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
      - (ii) result in minor damage to organizational assets;
      - (iii) result in minor financial loss; or
      - (iv) result in minor harm to individuals.

Computer Security Concepts

- Three levels of **impact** on organizations or individuals are defined in FIPS 199:
  - **Moderate**: The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
    - A serious adverse effect means that, for example, the loss might
      - (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
      - (ii) result in significant damage to organizational assets;
      - (iii) result in significant financial loss; or
      - (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

Computer Security Concepts

- Three levels of **impact** on organizations or individuals are defined in FIPS 199:
  - **High**: The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
    - A severe or catastrophic adverse effect means that, for example, the loss might
      - (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
      - (ii) result in major damage to organizational assets;
      - (iii) result in major financial loss; or
      - (iv) result in severe or catastrophic harm to individuals involving loss of life or serious, life-threatening injuries.

Computer Security Concepts

- Confidentiality
  - Student grade information is an asset whose confidentiality is considered to be highly important by students. In the United States, the release of such information is regulated by the Family Educational Rights and Privacy Act (FERPA). Grade information should only be available to students, their parents, and employees that require the information to do their job.
  - Student enrollment information may have a moderate confidentiality rating. While still covered by FERPA, this information is seen by more people on a daily basis, is less likely to be targeted than grade information, and results in less damage if disclosed.
  - Directory information, such as lists of students or faculty or departmental lists, may be assigned a low confidentiality rating or indeed no rating. This information is typically freely available to the public and published on a school's Web site.

Computer Security Concepts

- Integrity
  - Several aspects of integrity are illustrated by the example of a hospital patient's allergy information stored in a database.
  - The doctor should be able to trust that the information is correct and current.
  - Now suppose that an employee (e.g., a nurse) who is authorized to view and update this information deliberately falsifies the data to cause harm to the hospital. The database needs to be restored to a trusted basis quickly, and it should be possible to trace the error back to the person responsible.
  - Patient allergy information is an example of an asset with a high requirement for integrity. Inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability.

Computer Security Concepts

- Availability
  - The more critical a component or service, the higher is the level of availability required.
  - Consider a system that provides authentication services for critical systems, applications, and devices.
  - An interruption of service results in the inability for customers to access computing resources and staff to access the resources they need to perform critical tasks.
  - The loss of the service translates into a large financial loss in lost employee productivity and potential customer loss.

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:

1. 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, or integrity.
   - But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:
  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.

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:
  3. Because of previous point, 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.
     - It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:
  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)
       - 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).

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:

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 also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism.

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:
  6. Computer and network 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.

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:

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.

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:
  8. Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:

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.

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:

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.

The OSI Security Architecture

- To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.

- Systematic approach: Security Architecture for OSI
  - The OSI security architecture is useful to managers as a way of organizing the task of providing security.
  - Furthermore, because this architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.

The OSI Security Architecture

- The OSI security architecture focuses on *security attacks*, *mechanisms*, and *services*, and can be defined briefly
  - **Security attack**: Any action that compromises the security of information owned by an organization.
  - **Security mechanism**: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
  - **Security service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
    - The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

The OSI Security Architecture

- In the literature, the terms *threat* and *attack* are commonly used to mean more or less the same thing.

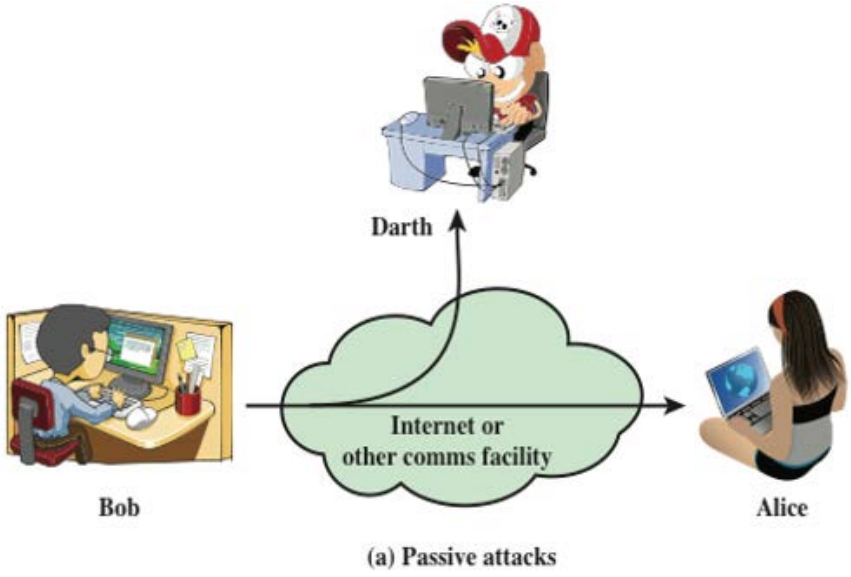
Threats and Attacks (RFC 4949)

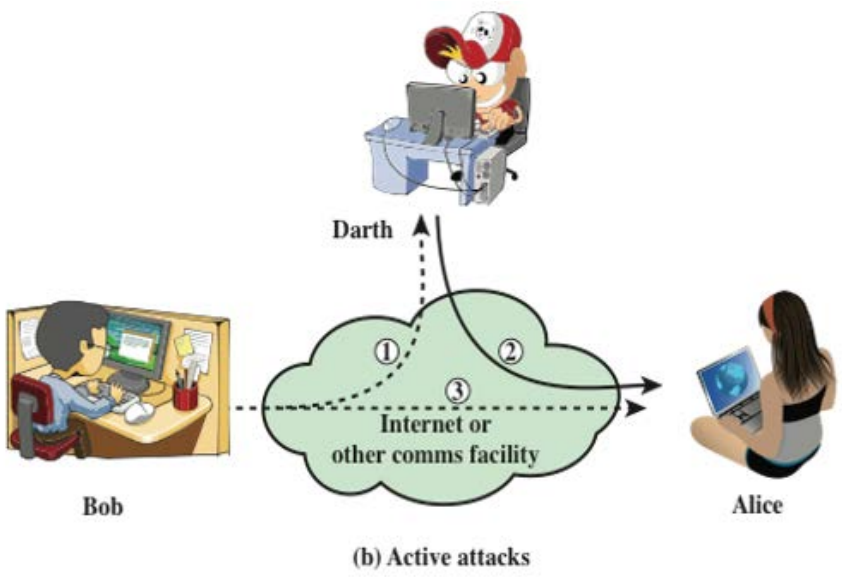
Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security Attacks

- A useful means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*



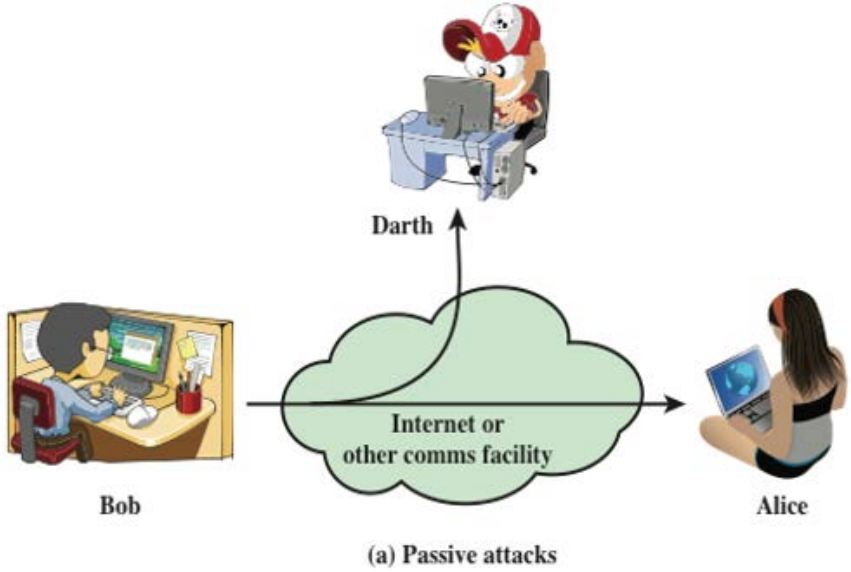


A passive attack attempts to learn or make use of information from the system but does not affect system resources.

An active attack attempts to alter system resources or affect their operation.

Security Attacks: Passive Attacks

- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to obtain information that is being transmitted.



(a) Passive attacks

A passive attack attempts to learn or make use of information from the system but does not affect system resources.

Security Attacks: Passive Attacks

- Two types of passive attacks are the **release of message contents** and **traffic analysis**:
  - **Release of message contents**
    - The release of message contents is easily understood.
    - A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
    - We would like to prevent an opponent from learning the contents of these transmissions.
  - **Traffic analysis**
    - The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.
    - This information might be useful in guessing the nature of the communication that was taking place.

Security Attacks: Passive Attacks

- Passive attacks are very difficult to detect, because they do not involve any alteration of the data.
  - Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
  - However, it is feasible to prevent the success of these attacks, usually by means of encryption.
  - Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.