Overview

CSE 565 - Fall 2025

Computer Security

Hongxin Hu (hongxinh@buffalo.edu)

Updates

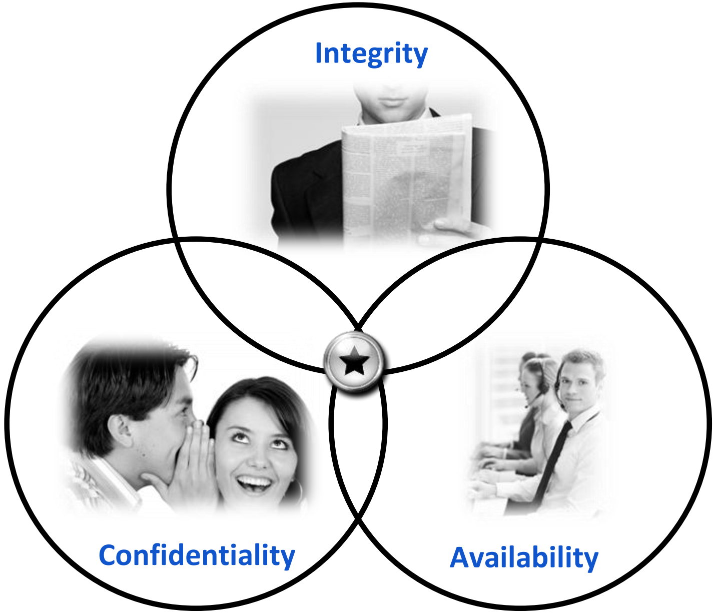
- **AI Quiz**
  - Deadline: Monday, September 10
- **Assignment 1**
  - Deadline: Monday, September 16
- **Environment Setup**
  - SEED Project: http://www.cis.syr.edu/~wedu/seed/
  - Mac OS (M1/M2) users please check the new setup document
  - Other users
    - https://piazza.com/buffalo/fall2025/cse565a/resources
- **Project 1 Secret-Key Encryption**
  - Deadline: Wednesday, September 18

What is Computer Security

The NIST Internal/Interagency Report NISTIR 7298 (Glossary of Key Information Security Terms , May 2013) Defines the Term Computer Security as Follows:

“ Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of information system **assets** including hardware, software, firmware, and information being processed, stored, and communicated.”

Security Objectives (CIA Triad)

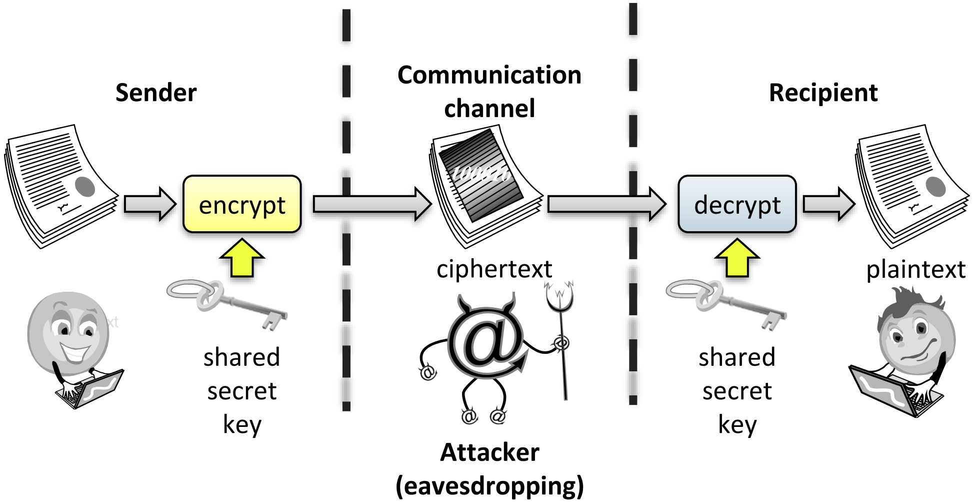


Confidentiality

- **Confidentiality** is the avoidance of the unauthorized disclosure of information.
    - Confidentiality involves the protection of data, providing **access** for those who are allowed to see it while disallowing others from learning anything about its content.

Tools for Confidentiality

- **Encryption:** the transformation of information using a secret, called an encryption key, so that the transformed information can only be read using another secret, called the decryption key

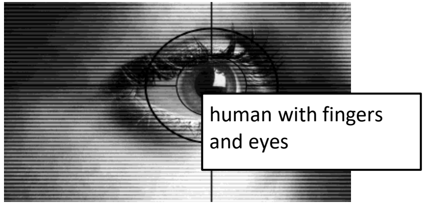


Tools for Confidentiality

- **Authorization (Access control)** : rules and policies that limit access to confidential information to those people and/or systems with a “need to know.”
  - This need to know may be determined by identity, such as a person’s name or a computer’s serial number, or by a role that a person has, such as being a manager or a computer security specialist.
  - The determination if a person or system is allowed access to resources, based on an access control policy.
    - Such authorizations should prevent an attacker from tricking the system into letting him have access to protected resources.

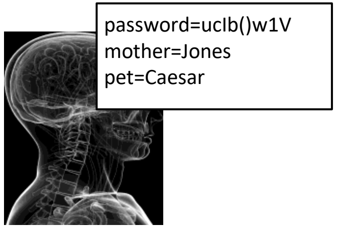
Tools for Confidentiality

- **Authorization** : the determination of the identity or role that someone has. This determination can be done in a number of different ways, but it is usually based on a combination of
  - something the person has (like a smart card or a radio key fob storing secret keys),
  - something the person knows (like a password),
  - something the person is (like a human with a fingerprint).



human with fingers and eyes

Something you are



password=ucIb()w1V
mother=Jones
pet=Caesar

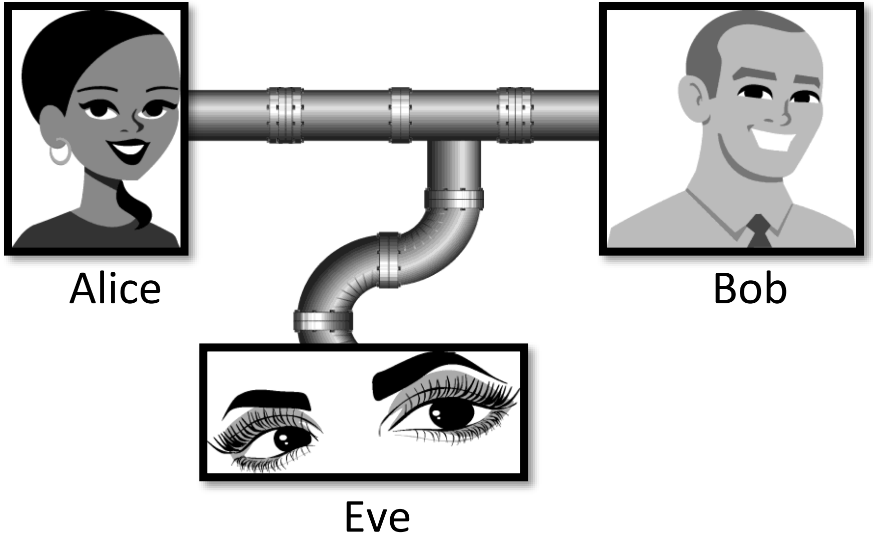
Something you know

radio token with secret keys

Something you have

Examples

- **Eavesdropping:** the interception of information intended for someone else during its transmission over a communication channel.
  - Example: **packet sniffers**
  - This is an attack on confidentiality



Integrity

Integrity: Prevent/detect/deter improper modification of information

- **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.

Tools for Integrity

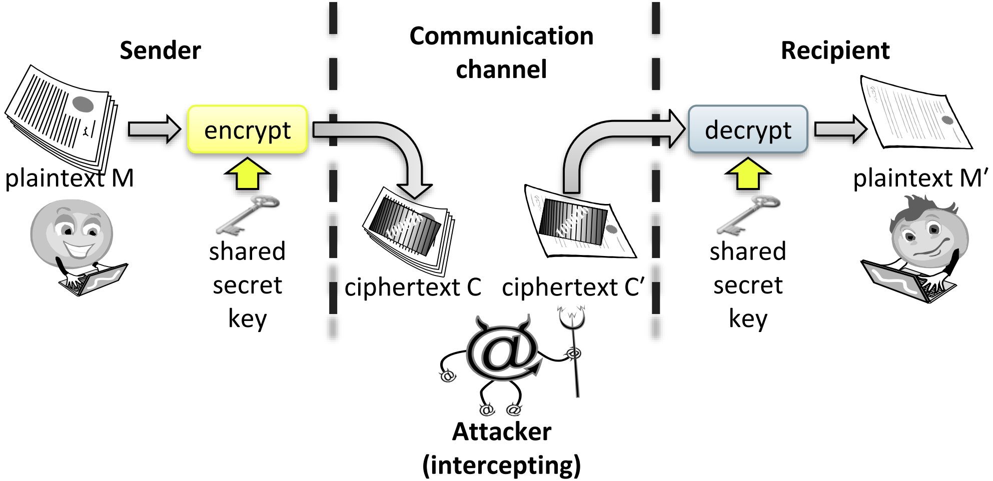
Backups: the periodic archiving of data.

Checksums: the computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.

Data correcting codes: methods for storing data in such a way that small changes can be easily detected and automatically corrected.

Examples

- **Alteration:** unauthorized modification of information.
  - **Example:** the **man-in-the-middle attack,** where a network stream is intercepted, modified, and retransmitted.
  - This is an attack on data integrity



Availability

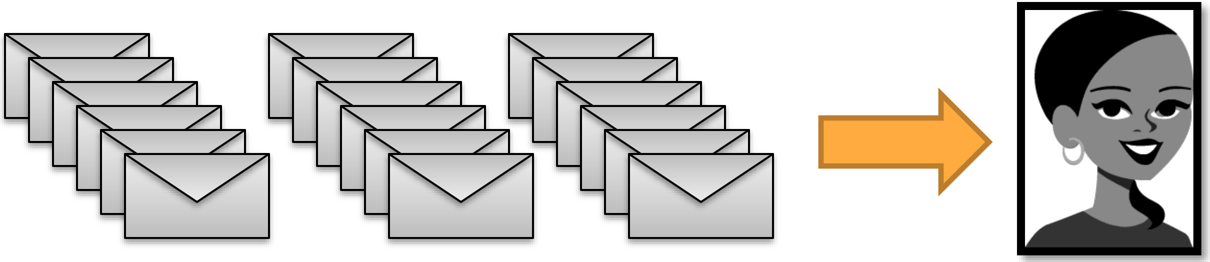
Availability: Prevent/detect/deter improper denial of access to services provided by the system

Tools:

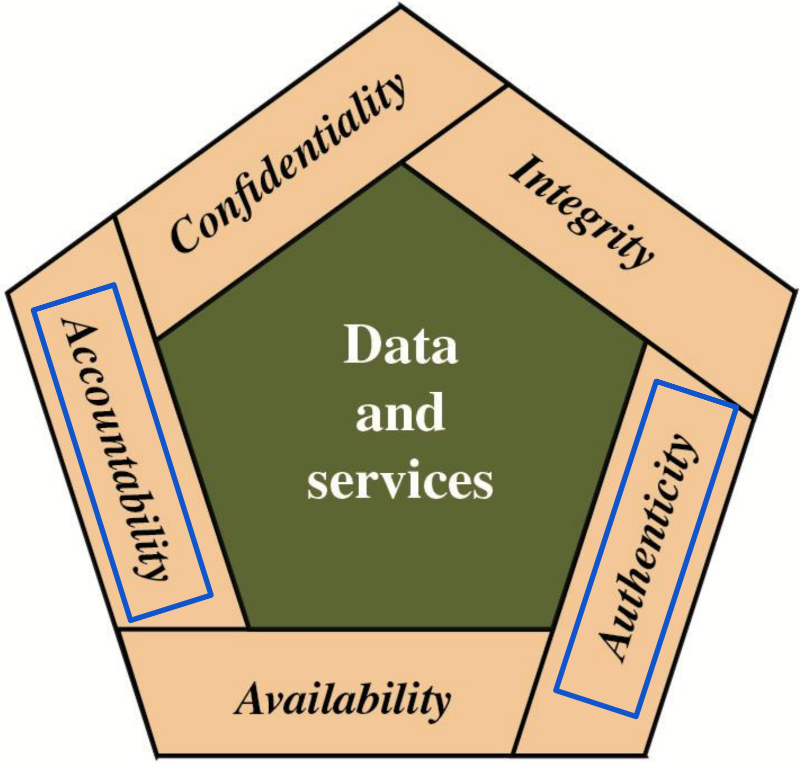
- Computational redundancies: computers and storage devices that serve as fallbacks in the case of failures
- Physical protections: infrastructure meant to keep information available even in the event of physical challenges.

Examples

- **Denial-of-service:** the interruption or degradation of a data service or information access.
  - **Example:** email **spam,** to the degree that it is meant to simply fill up a mail queue and slow down an email server.
  - This is an attack on availability



In Addition to CIA Triad



In Addition to CIA Triad

- **Authenticity**: The assurance that a message, transaction, or other exchange of information is from the source it claims to be from.

- **Primary tool:**
  - **Digital signatures**. These are cryptographic computations that allow a person or system to commit to the authenticity of their documents in a unique way that achieves nonrepudiation, which is the property that authentic statements issued by some person or system cannot be denied.

Examples

- **Masquerading:** the fabrication of information that is purported to be from someone who is not actually the author.
  - Example: **phishing** (BankofAmarica.com looks like BankofAmerica.com), **spoofing** (Send a network packet with the wrong return IP address)
  - This is an attack on authenticity

"From: Alice"
(really is from Eve)

In Addition to CIA Triad

- **Accountability**: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

- Example: Data Breach in a Healthcare Organization
  - A large healthcare organization holds sensitive medical records of millions of patients. Due to lax security measures, an unauthorized individual gains access to their database and downloads confidential patient data, which includes names, medical histories, and social security numbers.
  - This is an attack on accountability

Authentication vs Authorization

- **Authentication** —— Who goes there?
  - Restrictions on who (or what) can access system

- **Authorization** —— Are you allowed to do that?
  - Restrictions on actions of authenticated users
  - Authorization is a form of **access control**

How to we achieve the objectives? What are the possible measures and controls?

The means of achieving these objectives greatly differ

- cryptographic techniques
- access control policies
- software checking tools
- virus scanners
- firewalls
- spam filters, etc.

Each system must be evaluated uniquely in terms of its requirements

- security mechanisms must be adequately chosen in accordance with those
- requirements

Levels of Impact

- Low
  - The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
- Moderate
  - The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals
- High
  - The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Why is Computer Security Hard?

- Identifying security requirements of a system is non-trivial
  - must take into account services, environment, etc.
- Finding adequate (often complex) solutions is not easier
  - the decision must take into account known and unknown attacks and threats
  - security mechanisms must be logically placed
- Securing a system is not a one-time task
  - the system must be constantly monitored in face of changing threats
  - security mechanisms need to be re-evaluated

Why is Computer Security Hard?

- Managers do not perceive value in security investment (until a security failure occurs)
  - system administrators might not influence decisions or not make good decisions
- Users view security measures as an obstacle on the way of getting their work done
  - we would like security mechanisms to be as intuitive and robust as possible
- Adding security to an existing system might not be pretty
  - ideally, security is an integral part of the design

Computer Security Terminology (1 of 3)

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 technique 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.

Computer Security Terminology (2 of 3)

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.

Computer Security Terminology (3 of 3)

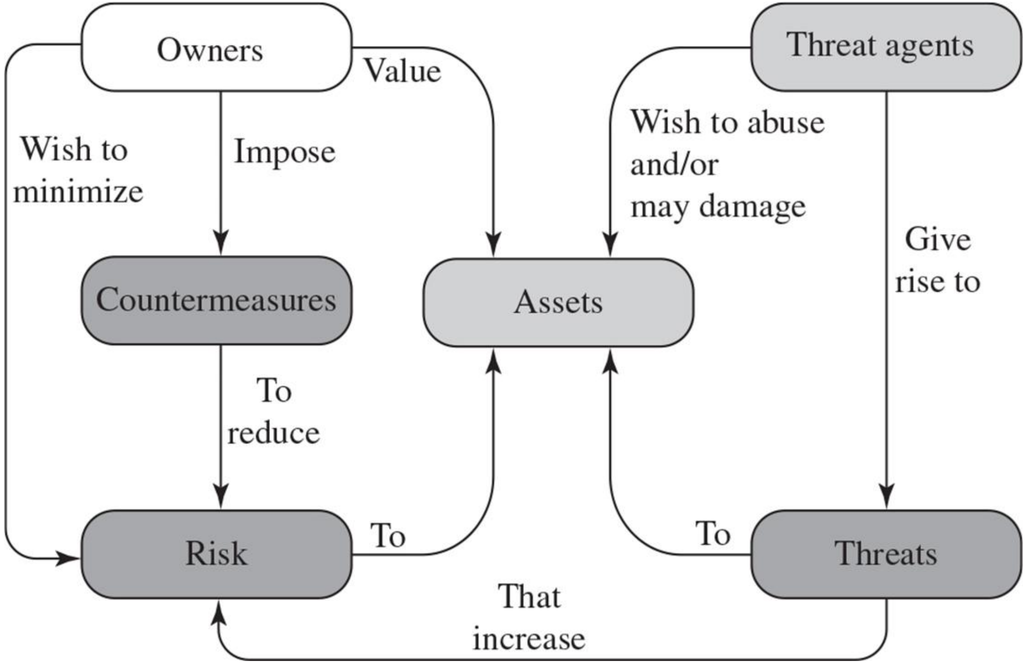
Threat

- 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.

Security Concepts and Relationships



Assets of a Computer System

Hardware

Data storage, data communication devices, etc.

Software

Operating system, system utilities, and applications.

Data

Files and databases, security-related data/password files.

Communication facilities and networks

Local and wide area network communication links, bridges, routers, etc.

Vulnerabilities, Threats and Attacks

- Categories of vulnerabilities
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)

Vulnerabilities, Threats and Attacks

- Threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset

Vulnerabilities, Threats and Attacks

Attacks (threats carried out)

- passive: observes information without intervention
  - e.g., passively monitoring a communication link
- active: changes system resources or affects their operation
  - e.g., changing messages, replaying old messages on the network, corrupting users, etc.

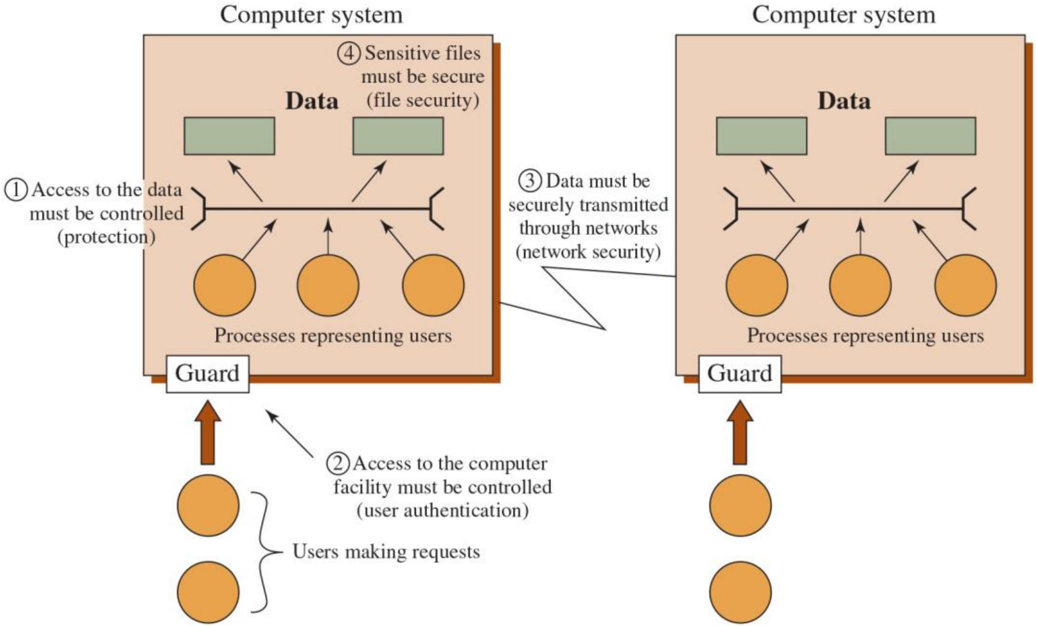
- insider: is legitimately a part of the system with access to internal data or is inside the security perimeter
- outsider: is outside of the security perimeter or is not a legitimate user

Countermeasures

- Means used to deal with security attacks
  - Prevent
  - Detect
  - Response
  - Recover
- May itself introduce new vulnerabilities

Scope of Computer Security

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


Computer system
Computer system
(4) Sensitive files must be secure (file security)
Data
Data
(1) Access to the data must be controlled (protection)
(3) Data must be securely transmitted through networks (network security)
Processes representing users
Processes representing users
Guard
Guard
(2) Access to the computer facility must be controlled (user authentication)
Users making requests

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 that is vulnerable to a social engineering attack

Attack Surface Categories

Network Attack Surface

- Vulnerabilities over an enterprise network, wide-area network, or the Internet
- Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks

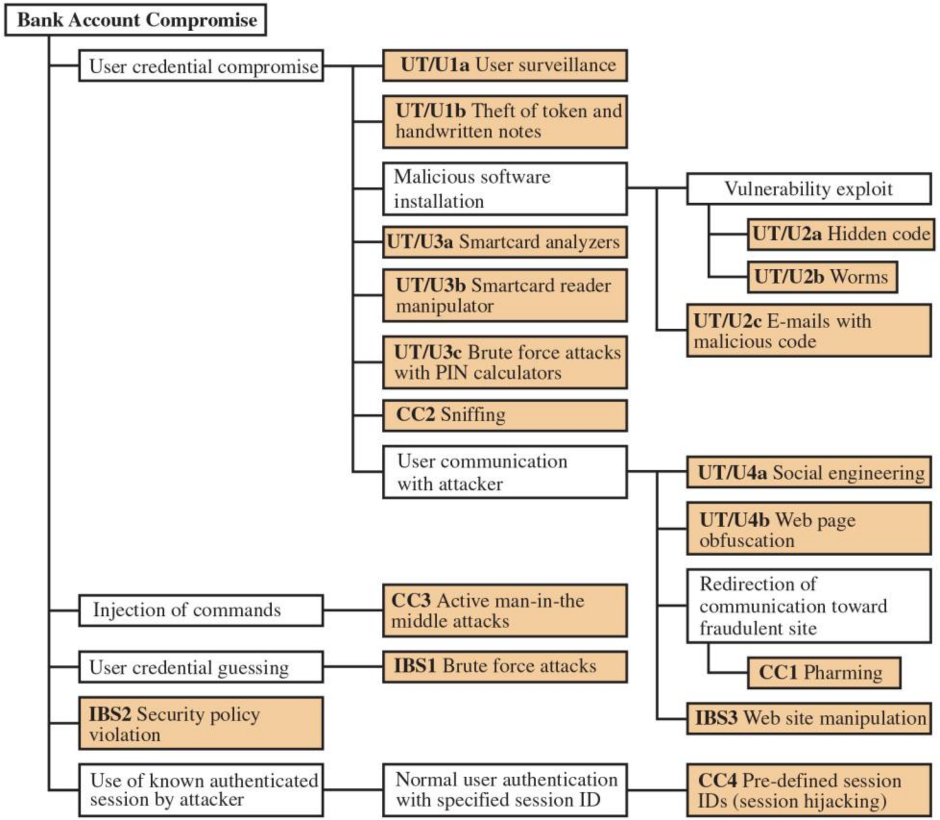
Software Attack Surface

- 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

An Attack Tree for Internet Banking Authentication



Bank Account Compromise

- User credential compromise
  - **UT/U1a** User surveillance
  - **UT/U1b** Theft of token and handwritten notes
  - Malicious software installation
    - Vulnerability exploit
      - **UT/U2a** Hidden code
      - **UT/U2b** Worms
    - **UT/U2c** E-mails with malicious code
  - **UT/U3a** Smartcard analyzers
  - **UT/U3b** Smartcard reader manipulator
  - **UT/U3c** Brute force attacks with PIN calculators
  - **CC2** Sniffing
  - User communication with attacker
    - **UT/U4a** Social engineering
    - **UT/U4b** Web page obfuscation
    - Redirection of communication toward fraudulent site
      - **CC1** Pharming
    - **IBS3** Web site manipulation
- Injection of commands
  - **CC3** Active man-in-the middle attacks
- User credential guessing
  - **IBS1** Brute force attacks
- **IBS2** Security policy violation
- Use of known authenticated session by attacker
  - Normal user authentication with specified session ID
    - **CC4** Pre-defined session IDs (session hijacking)

Computer Security Strategy (1 of 2)

Security Policy

Formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

Security Implementation

Involves four complementary courses of action:

- Prevention
- Detection
- Response
- Recovery

Computer Security Strategy (2 of 2)

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

Summary

- Computer security concepts
  - Definition: CIA
  - Challenges
  - Model
- Threats, attacks, and assets
  - Threats and attacks
  - Threats and assets
- Fundamental security design principles
- Attack surfaces and attack trees
  - Attack surfaces
  - Attack trees
- Computer security strategy
  - Security policy
  - Security implementation
  - Assurance and evaluation