Overview

Computer Security – Principles and Practice (Pearson, fourth edition)

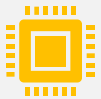
W. Stallings, L. Brown

* These slides are an adaptation of the original slides of the authors of the book

Learning objectives

Describe the key security requirements

Discuss the types of threats and attacks



Summarize the functional requirements for computer security

Explain the fundamental security design principles

…

Before security…

ASK
YOURSELF:

What assets do you need to protect?
How those assets are threatened?
How can you counter those threats?

Computer security concepts

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."

Key Security Concepts (CIA)

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

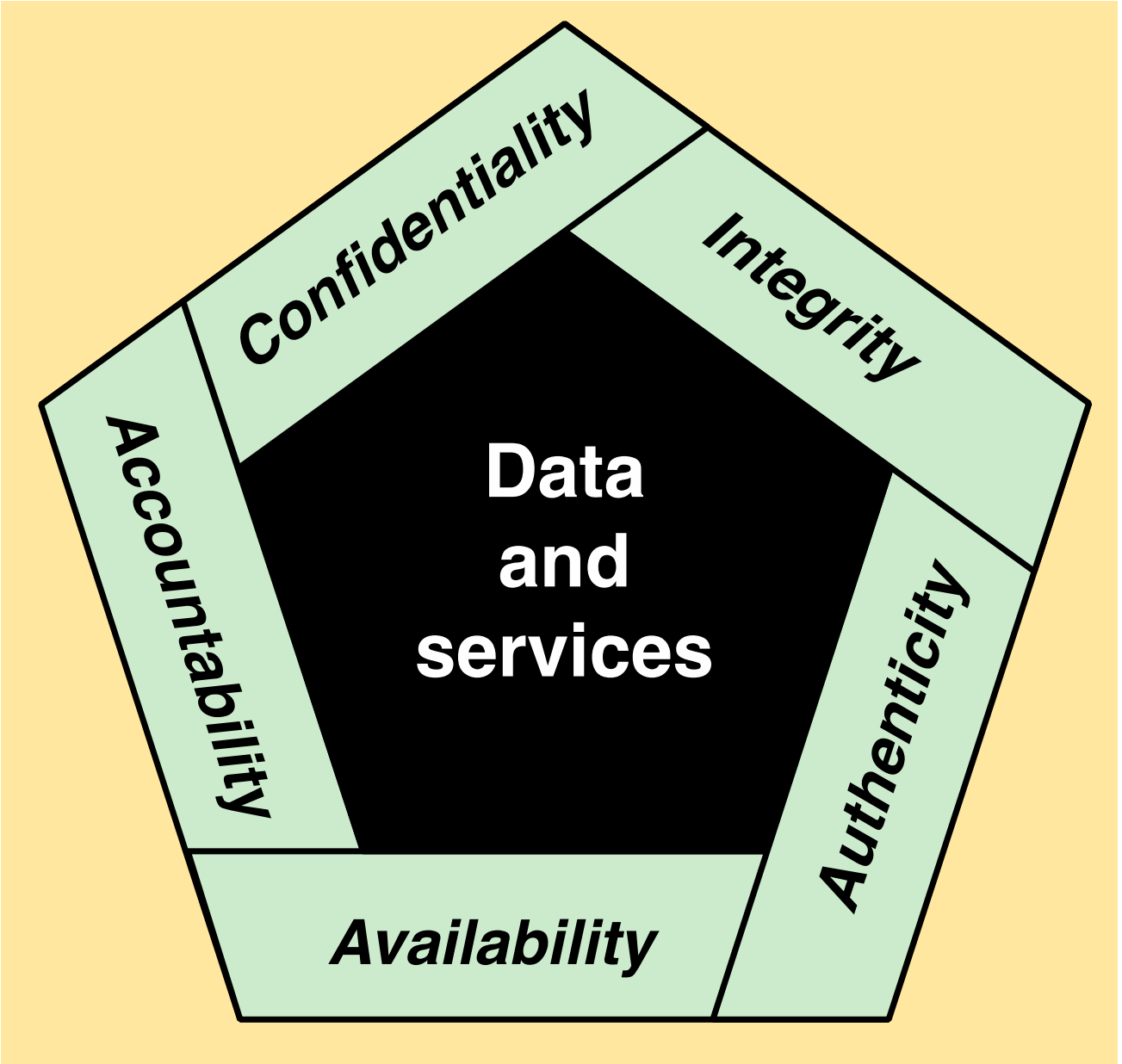
- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

- Ensuring timely and reliable access to and use of information

The CIA Triad

- Confidentiality:
  - Data confidentiality : Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  - Privacy : Assures that individuals control how their information is stored, accessed and shared
- Integrity:
  - 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
- Availability:
  - Ensuring timely and reliable access to and use of information.

Essential network and security requirements



Authenticity & Accountability

- Authenticity: The property of being genuine and being able to be verified and trusted
  - Regards 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: ability to uniquely trace the actions of an entity
  - This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action

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

Germania, attacco hacker a ospedale ha provocato morte donna

Germania, attacco hacker a ospedale ha provocato morte donna

Cure in ritardo perchè pronto soccorso chiuso

Redazione ANSA

ROMA

18 settembre 2020
12:29

NEWS

Question for you

GIVE EXAMPLES OF ASSETS OF LOW, MODERATE AND HIGH IMPACT FOR EACH SECURITY CONCEPT

I MEAN: CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

Computer Security Challenges (I)

1. Computer security is not as simple as it might first appear to the novice
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features
3. Procedures used to provide particular services are often counterintuitive
4. Physical and logical placement of security mechanisms needs to be determined
5. Security mechanisms typically involve several algorithms or protocols and require that participants be in possession of some secret information which raises questions about the creation, distribution, and protection of that secret information

Computer Security Challenges (II)

6. Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security

7. 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

8. Security requires regular and constant monitoring

9. 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

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

Computer Security Terminology

(RFC 2828, Internet Security Glossary, May 2000)

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.

Computer Security Terminology

(RFC 2828, Internet Security Glossary, May 2000)

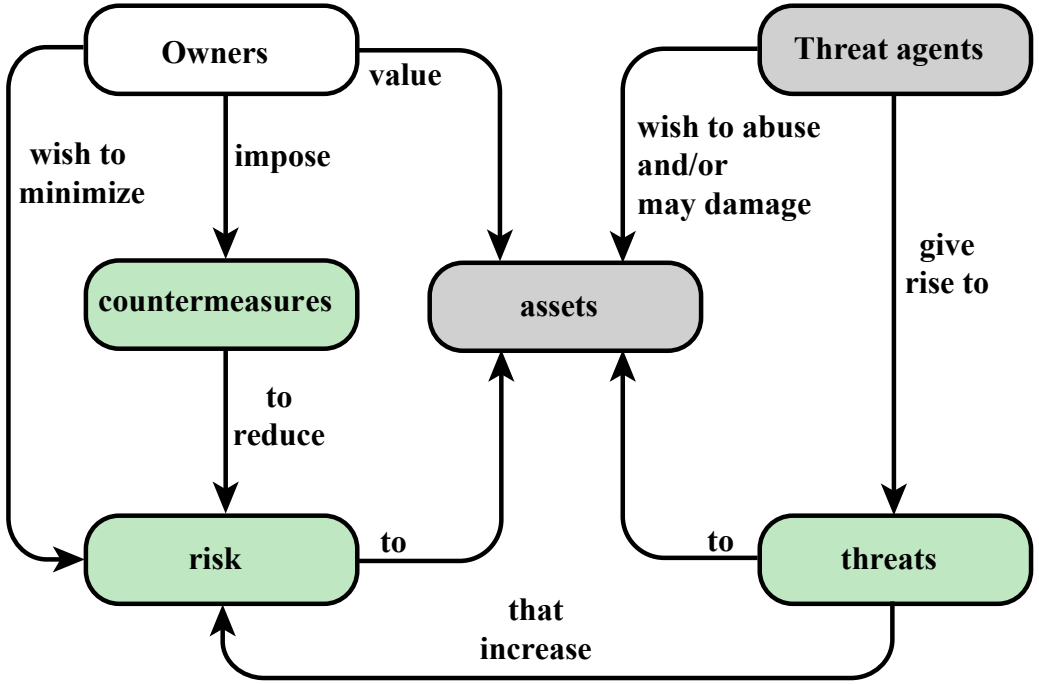
Security Policy: A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

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.

Security concepts and relationships



Assets of a Computer System

Hardware

Software

Data

Communication facilities and networks

Vulnerabilities, Threats and Attacks

Categories of vulnerabilities: the system may become…

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

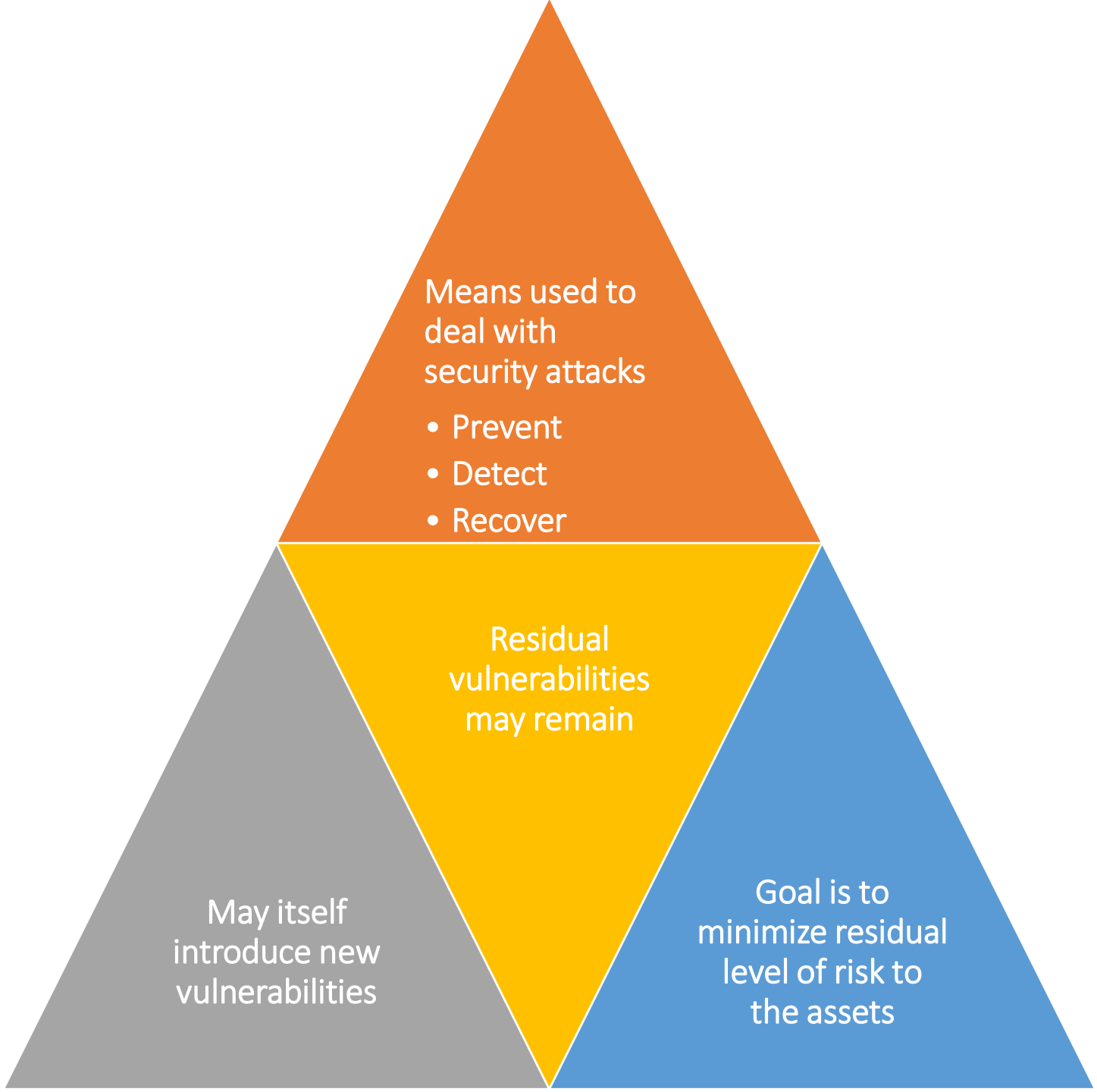
Threats

- 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 perimeter
- Outsider – initiated from outside the perimeter

Counter-measures



Questions & problems

CONSIDER AN ORGANIZATION MANAGING PUBLIC INFORMATION ON ITS WEB SERVER.

ASSIGN A LOW, MODERATE, OR HIGH IMPACT LEVEL FOR THE LOSS OF CONFIDENTIALITY, AVAILABILITY, AND INTEGRITY, RESPECTIVELY.

JUSTIFY YOUR ANSWER.

Threats, attacks and assets

Threat Consequences

The four kinds of threat consequences (based on RFC 4949):

- **Unauthorized disclosure**:
  - It is a threat to confidentiality
  - occurs when an unauthorized entity gains access to data
- **Deception**:
  - It is a threat to either system integrity or data integrity
  - Occurs when an authorized entity receives false data and believe it is true
- **Disruption**:
  - It is a threat to availability or system integrity
  - Occurs when the correct system functionality is interrupted or prevented
- **Usurpation**:
  - It is a threat to system integrity
  - Occurs when an unauthorized entity gains control of system services or functions

Attacks resulting in unauthorized disclosure

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:

- 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.

Attacks resulting in Deception

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.

Attacks resulting in Disruption

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.

Attacks resulting in Usurpation

Misappropriation:

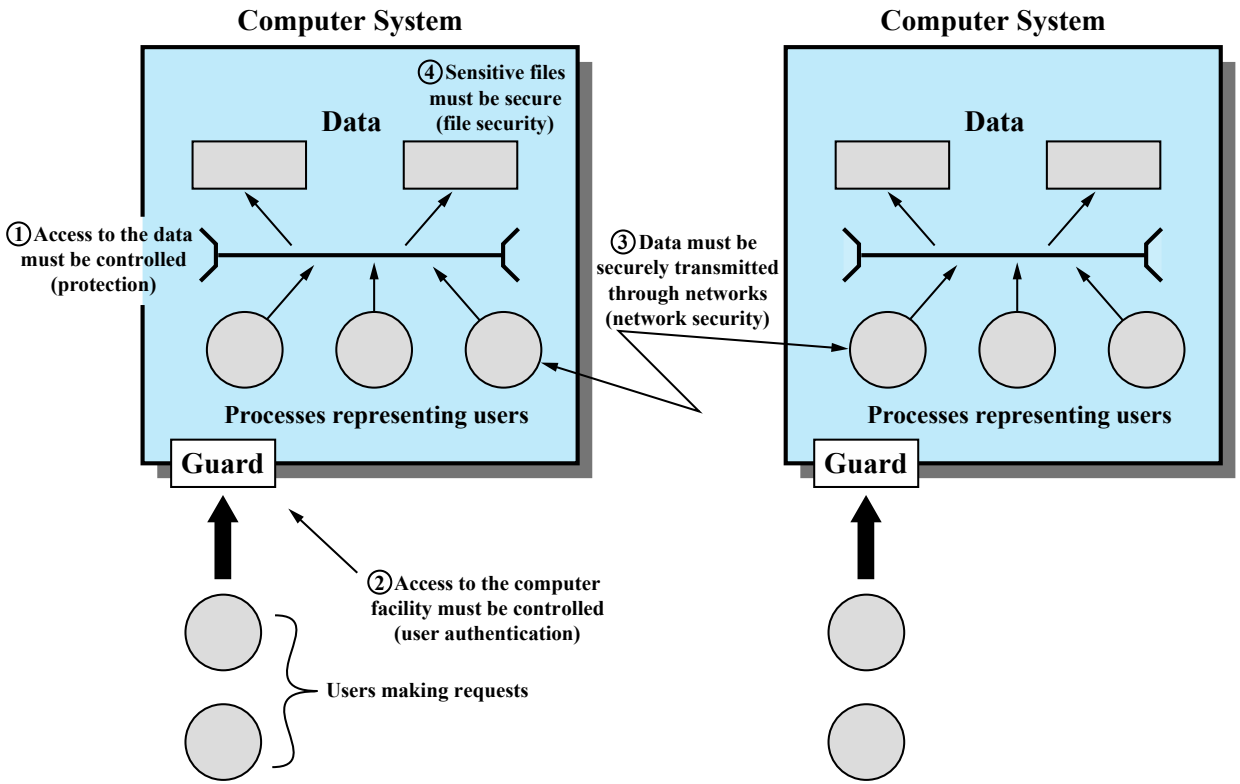
- An entity assumes unauthorized logical or physical control of a system resource.

Misuse:

- Causes a system component to perform a function or service that is detrimental to system security.

Scope of computer security

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



Computer and network assets and 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 encrypted or 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.

Passive and active attacks

—

in network security

Passive attacks:

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
  - Release of message contents
  - Traffic analysis

Active attacks:

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - Replay
  - Masquerade
  - Modification of messages
  - Denial of service

Review question

HOW WOULD YOU CLASSIFY THE FOLLOWING ATTACK?

UPON STEALING A BANK CUSTOMER'S COMMERCIAL IDENTITY (E.G., THEIR CREDIT CARD OR ACCOUNT INFORMATION), THE ATTACKER PRESENTS THOSE CREDENTIALS FOR THE MALICIOUS PURPOSE OF USING THE CUSTOMER'S CREDIT LINE TO STEAL MONEY

Functional requirements

Classification of countermeasures

- Several classifications of countermeasures aimed at reducing vulnerabilities and dealing with threats
- Classification according to functional requirements:
  - defined in FIPS 200 (*Minimum Security Requirements for Federal Information and Information Systems*).
- This standard enumerates 17 security-related areas:
  - They encompass a wide range of countermeasures to security vulnerabilities and threats.
  - Roughly, they can be divided into two categories:
    - Those that involve technical measures
    - Those that involve management issues

Classification of countermeasures

Each functional area may involve both technical and management measures:

- **Technical measures**: access control, identification and authentication, system and communication protection, and system and information integrity.
- **Management measures:** awareness and training; audit and accountability; certification, accreditation, and security assessments; contingency planning; maintenance; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition.
- Functional areas that overlap technical and management measures include configuration management, incident response, and media protection.

Counter-measures (I)

- **Access Control:**
  - Limit information system access to authorized users and of processes that act on their behalf
  - limit the types of transactions and functions that authorized users are permitted to exercise.
- **Awareness and Training:**
  - Address managers and users of organizational information systems
  - Make them aware of the security risks and of the applicable laws, regulations, and policies;
  - Train all the personnel to carry out their duties according to the security protocols
- **Audit and Accountability:**
  - Create, protect, and retain information system audit records
  - to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity
  - Ensure that the actions of individual users can be uniquely traced so they can be held accountable for their actions.

Counter-measures (II)

- **Certification, Accreditation, and Security Assessments:**
  - Periodically assess the security controls to determine their effectiveness
  - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities
  - Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- **Configuration Management:**
  - Establish and maintain baseline configurations and inventories of organizational information systems (HW, SW, docs,…) throughout the respective system development life cycles
  - Establish and enforce security configuration settings for information technology products employed.
- **Contingency Planning:**
  - Establish, maintain, and implement plans for emergency response, backup operations, and post-disaster recovery
  - Ensure the availability of critical information resources and continuity of operations in emergency situations.

Counter-measures (III)

- **Identification and Authentication:**
  - Identify system users, processes acting on behalf of users, or devices
  - Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access.
- **Incident Response:**
  - Establish an operational incident-handling capability (includes preparation, detection, analysis, containment, recovery, and user-response activities)
  - Track, document, and report incidents to appropriate organizational officials and/or authorities.
- **Maintenance:**
  - Perform periodic and timely maintenance on organizational information systems
  - Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Counter-measures (IV)

- **Media Protection:**
  - Protect information system media, both paper and digital
  - Limit access to information on information system media to authorized users
  - Sanitize or destroy information system media before disposal or release for reuse.
- **Physical and Environmental Protection:**
  - Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals
  - protect the physical plant and support infrastructure for information systems
  - provide supporting utilities for information systems
  - protect information systems against environmental hazards
  - provide appropriate environmental controls in facilities containing information systems.
- **Planning:**
  - Develop, document, periodically update, and implement security plans
  - The security plans describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the system.

Counter-measures (V)

- **Personnel Security:**
  - Ensure that individuals with positions of responsibility (including third-parties) are trustworthy and meet the security criteria for those positions
  - Ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers
  - Employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
- **Risk Assessment:**
  - Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
  - Risks may result from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
- **Systems and Services Acquisition:**
  - Allocate sufficient resources to adequately protect organizational information systems
  - Employ system development life cycle processes that incorporate information security considerations
  - Employ software usage and installation restrictions
  - Ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

Counter-measures (VI)

- **System and Communications Protection:**
  - Monitor, control, and protect organizational communications (both transmitted and received) at the external boundaries and key internal boundaries of the information systems
  - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.
- **System and Information Integrity:**
  - Identify, report, and correct information and information system flaws in a timely manner
  - Provide protection from malicious code at appropriate locations within organizational information systems
  - Monitor information system security alerts and advisories and take appropriate actions in response.

Fundamental Security Design Principles

Review question

WHAT KIND OF COUNTERMEASURES ARE THE FOLLOWING:

1) ENCRYPTION OF THE SSD OF A LAPTOP

2) KEEPING THE HASH OF EXECUTABLE FILES OF THE OS IN A CD

3) UNINSTALLATION FROM THE SYSTEM OF UNUSED APPLICATIONS

Problem

Consider the following general code for allowing access to a resource:

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == ERROR_ACCESS_DENIED) {
        // Security check failed.
        // Inform user that access is denied.
} else {
        // Security check OK.
}
```

a. Explain the security flaw in this program.

b. Rewrite the code to avoid the flaw.

Attack surfaces and security strategies

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 surface categories

Network Attack Surface

Vulnerabilities over an enterprise network, wide-area network, or the Internet

Network protocol vulnerabilities (e.g. those used for DoS attacks);

disruption of communications links;

various forms of intruder attacks

Software Attack Surface

Vulnerabilities in application, utility, or operating system code

Particular focus is Web server software

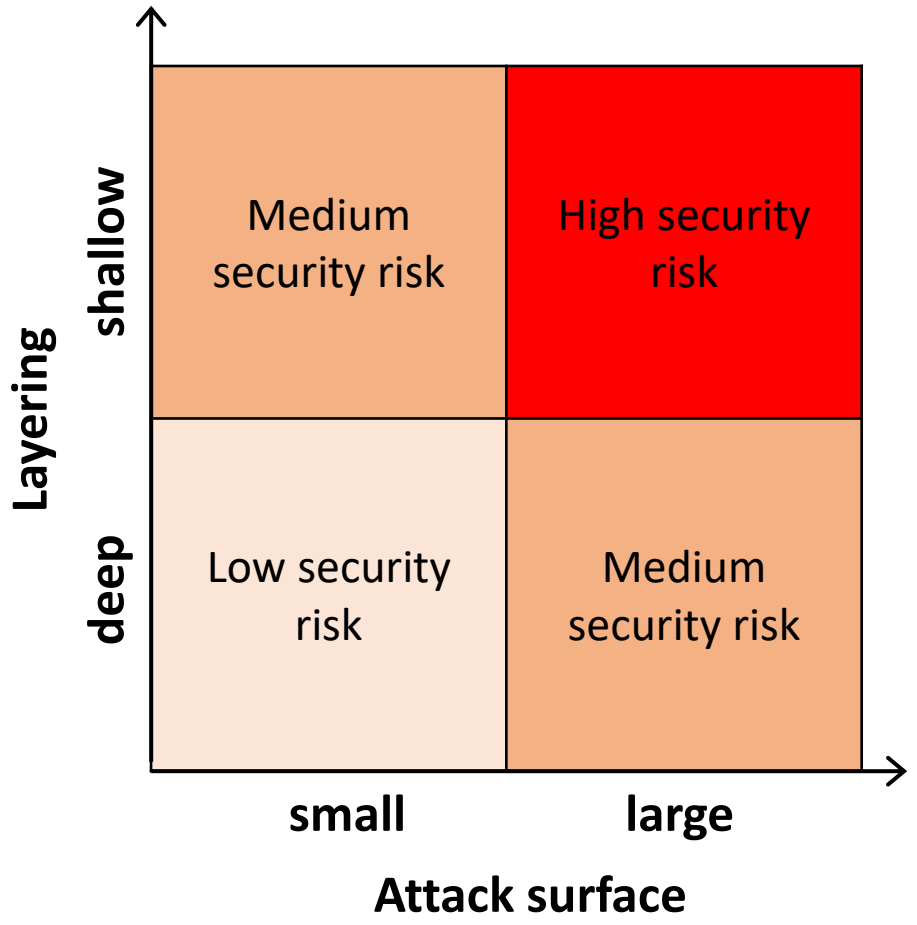
Human Attack Surface

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

Attack surface analysis

- To assess the scale and severity of threats to a system:
  - Identifies the points of vulnerability
  - Identifies the most appropriate security mechanisms and their deployment
- Uses:
  - Makes developers and security analysts aware of where security mechanisms are required.
  - Designers may be able to find ways to make the surface smaller, thus making the task of the adversary more difficult.
  - It also provides guidance on setting priorities for testing, strengthening security measures, or modifying the service or application.

Defense in depth and attack surface



Attack trees

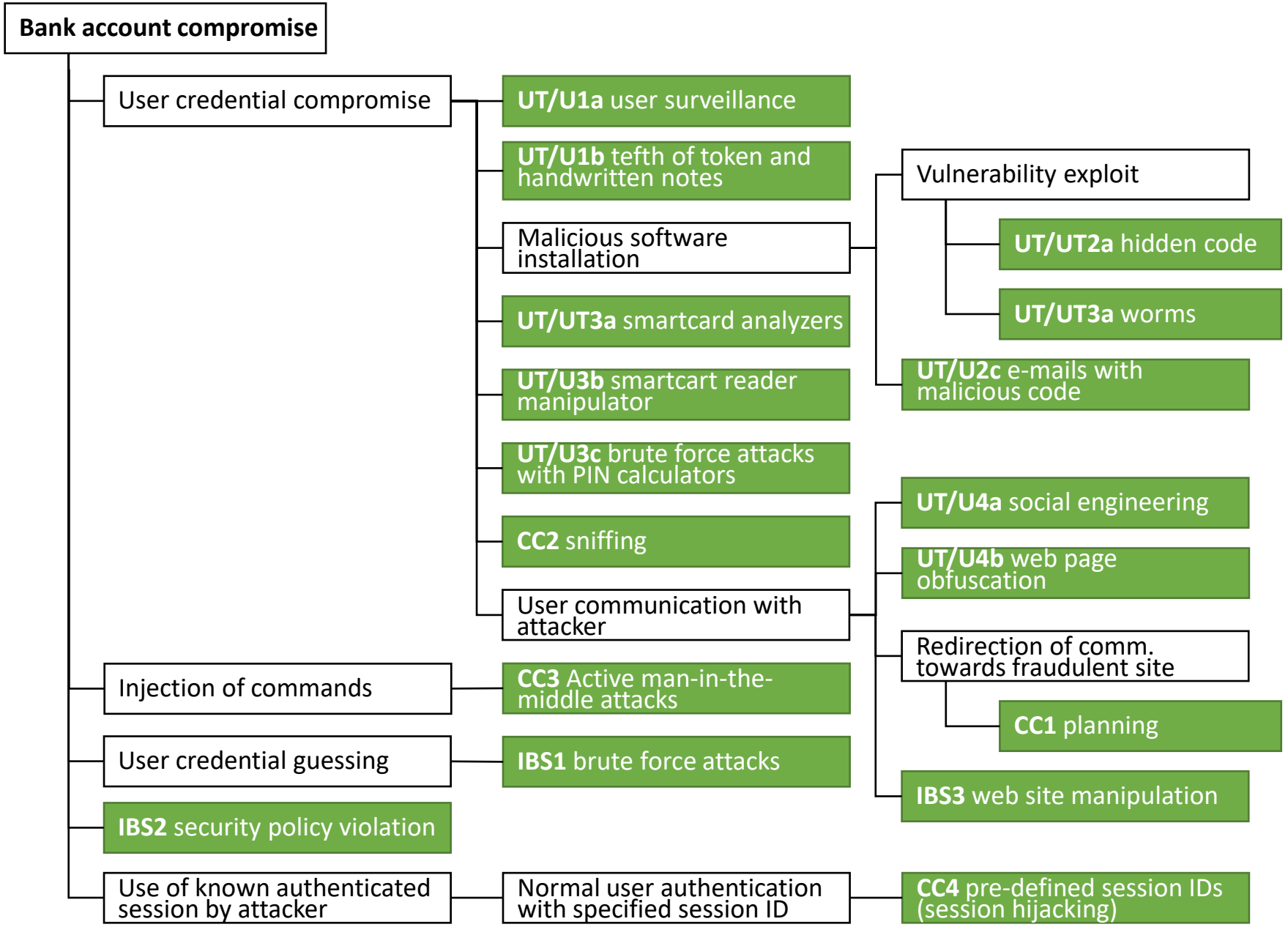
- An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities:
  - The root of the tree is the *security incident* (the goal of the attack)
  - The branches and subnodes of the tree are the ways that an attacker could reach that goal
  - Each subnode defines a subgoal, and each subgoal may have its own set of further subgoals, etc.
  - The leaf nodes, represent different ways to initiate an attack.

Attack trees

- Each node other than a leaf is either an AND-node or an OR-node:
  - To achieve the goal represented by an AND-node, the subgoals represented by all of that node's subnodes must be achieved
  - for an OR-node, at least one of the subgoals must be achieved.
- Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared.
- Attack trees allow analysis attack patterns:
  - to build a body of knowledge about both attack strategies and patterns.
  - to document security attacks in a structured form that reveals key vulnerabilities.
  - to guide the design of systems and applications, and the choice and strength of countermeasures.

Attack trees

An attack tree for internet banking authentication



Review question

CAN YOU MAKE AN EXAMPLE OF SOMETHING THAT MAY ENLARGE THE ATTACK SURFACE ON YOUR PC?

Questions & problems

DRAW AN ATTACK TREE FOR GAINING ACCESS TO THE CONTENT OF A PHYSICAL SAFE

Computer security strategies

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 (RFC 4949)

Security Implementation

- Involves four complementary courses of action:
  - Prevention
  - Detection
  - Response
  - Recovery

Assurance

- It is an attribute of an information system that encompasses both system design and implementation
- 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

Security policy

- Several factors to be considered in the development of a security policy:
  - The value of the assets being protected
  - The vulnerabilities of the system
  - Potential threats and the likelihood of attacks
- Relevant tradeoffs:
  - Ease of use versus security
  - Cost of security versus cost of failure and recovery

- The security policy is a business decision, possibly influenced by legal requirements.

Security imple-mentation

Prevention: an ideal security scheme is one in which no attack is successful…

- Example: transmission of encrypted data

Detection: absolute protection is often not feasible, but it is practical to detect security attacks.

- Example: intrusion detection systems designed to detect the presence of unauthorized individuals logged onto a system.

Response: if security mechanisms detect an ongoing attack, the system may be able to respond in such a way as to halt the attack and prevent further damage.

Recovery: an example of recovery is the use of backup systems, so that if data integrity is compromised, a prior, correct copy of the data can be reloaded.

Assurance and evaluation

Assurance is an attribute of a system that provides confidence that the system operates such that the system's security policy is enforced.

- Encompasses both system design and implementation.
- Deals with the questions:
  - "Does the security system design meet its requirements?"
  - "Does the security system implementation meet its specifications?"
- It is expressed as a degree of confidence, not in terms of a formal proof that a design or implementation is correct.
  - Absolute proofs not possible at the state of the art

Evaluation is the process of examining a computer product or system with respect to certain criteria.

- involves testing, formal analytic or mathematical techniques.

Conclusions

Standards

- Standards have been developed to cover management practices and the overall architecture of security mechanisms and services
- The most important of these organizations are:
  - **National Institute of Standards and Technology (NIST)**
    - 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
  - **Internet Society (ISOC)**
    - ISOC is a professional membership society that 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
  - **International Telecommunication Union (ITU-T)**
    - ITU is a United Nations agency in which governments and the private sector coordinate global telecom networks and services
  - **International Organization for Standardization (ISO)**
    - ISO is a nongovernmental organization whose work results in international agreements that are published as International Standards

Summary

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

Questions & problems

CONSIDER AN INFORMATION SYSTEM OF A SMART CITY IN WHICH CITIZENS PROVIDE AN ID NUMBER AND A E-DOCUMENT FOR ACCOUNT ACCESS THROUGH AUTOMATIC MACHINES.

GIVE EXAMPLES OF CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY REQUIREMENTS ASSOCIATED WITH THE SYSTEM. IN EACH CASE, INDICATE THE DEGREE OF THE IMPORTANCE OF THE REQUIREMENT.

Questions & problems

CONSIDER A LAW ENFORCEMENT ORGANIZATION MANAGING EXTREMELY SENSITIVE INVESTIGATIVE INFORMATION.

ASSIGN A LOW, MODERATE, OR HIGH IMPACT LEVEL FOR THE LOSS OF CONFIDENTIALITY, AVAILABILITY, AND INTEGRITY, RESPECTIVELY.

JUSTIFY YOUR ANSWER.