Week 1

CPSC253 – Cyber Security Fundamentals and Principles

Course Info

CPSC253 Cyber Security Fundamentals and Principles

- Sections
  Sa 1:00PM – 3:45PM E202
- Course Textbook
  William Stallings, Lawrie Brown - Computer Security: Principles and Practice 4th edition
- Course Objectives
  Computer security involves a broad range of topics that include but are not limited to information, network, endpoint, and software security. This course will aim to give a broad overview of the different types of security threats along with general measures to counter, stop, and prevent them using various tools, algorithms, and management initiatives.

Your Instructor

Jason Choi

- M.B.A - University of Southern California 21’
  M.S Software Engineering – California State University Fullerton 16’
  B.S Electrical Engineering – University of California Los Angeles 09’
- Principal Software Engineer – CVS Health
  Advisory Software Engineer – IBM Security
  Software Engineer – Parasoft Corporation
- Email: jasonchoi@fullerton.edu
- Office Hours
  Thursdays 4:30PM – 5:30PM

Grading

Category	**% of Final Grade**
Attendance *	10%
Assignments **	15%
Project / Research Paper	15%
Midterm	30%
Final	30%

** Attendance will be taken every class. Students are required to stay for the entire duration of instruction to receive full attendance marks. Emergencies and other reasons for non-attendance will be reasonably accommodated with submission of proof.*
*** Late assignments will be accepted with 10% deducted per day for each day past due.*

Attendance

- Students are expected to be present in-person each class unless otherwise noted and will receive attendance points. Students are also given 2 free absences without penalty for their personal use. Absences that are due to extreme emergencies may be excused with proper documentation.

Virtual Instruction

- Based on the instructor’s circumstances, virtual instruction (up to 3 times) may be given during the semester. Students will be informed no later than 3 days prior to such days.

Assignments & Project / Research Paper

- Assignments

  Mixture of solving problems from the textbook and responding to assigned reading

- Project / Research Paper

  5 pages single spaced (excluding table of contents / works cited pages). Given a cybersecurity scenario, analyze the situation and give recommendations based on topics learned. Maximum 5 pages single spaced (excluding table of contents / works cited pages). More details will be presented in Week 11.

Exams

Midterm	Week 8	Chapters 1 – 13
Final	Week 17	Chapters 14 – 25

- There is absolutely no collaboration or use of electronic devices during the exam – no exceptions. Proctoring software may be used to monitor any anomalies.
- Exams may not be taken after they have been given in class. Due to an act of nature, personal medical emergency, a family crisis, an act of terrorism, severe civil unrest, etc. students have 10 calendar days to petition the instructor to retake any exam/quiz or submit an assignment without late penalty.

Academic Honesty

It is your responsibility to be aware of and follow the spirit of CSU Fullerton's academic honesty policy which can be found here. Academic dishonesty will not be tolerated. The University Catalog and the Class Schedule provide a detailed description of Academic Dishonesty under University Regulations. By submitting work for evaluation, you acknowledge that you have adhered to the spirit of the university's academic honesty policy and that your submission is an original work by you unless otherwise directed to work in groups. Failure to follow the spirit of the academic honesty policy will result in a severely negative evaluation of the work in question and may result in involving the Department Chair and the Judicial Affairs office to seek a disciplinary remedy.

Overview

Chapter 1

i. Computer Security Concepts

ii. Threats, Attacks, and Assets

iii. Security Functional Requirements

iv. Fundamental Security Design Principles

v. Attack Surfaces and Attack Trees

vi. Computer Security Strategy

vii. Standards

Assessment of Your Computer Security Knowledge

- Test your current knowledge of basic computer security https://www.pewresearch.org/internet/quiz/cybersecurity-knowledge/
- How do you feel?
- More advanced quiz https://www.proprofs.com/quiz-school/story.php?title=njixmdmxnu90

Computer Security Concepts

- Definition of Computer Security as defined by NIST (National Institute of Standards and Technology)

  “ Measures and controls that ensure **Confidentiality**, **Integrity**, **Availability** of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.”

  Commonly referred to as the **CIA Triad**

- **Confidentiality** – Preserve authority over information access and protection of private or proprietary information
- **Integrity** – Guard against improper information modification and destruction
- **Availability** – Ensure timely and reliable access to and use of information

Additional Concepts

Authenticity – Property of being genuine and trusted

Accountability – Ability for a system to be traced to a responsible entity

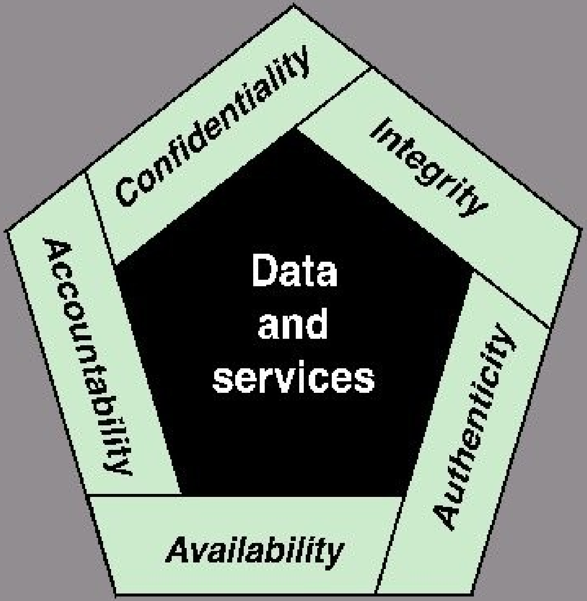
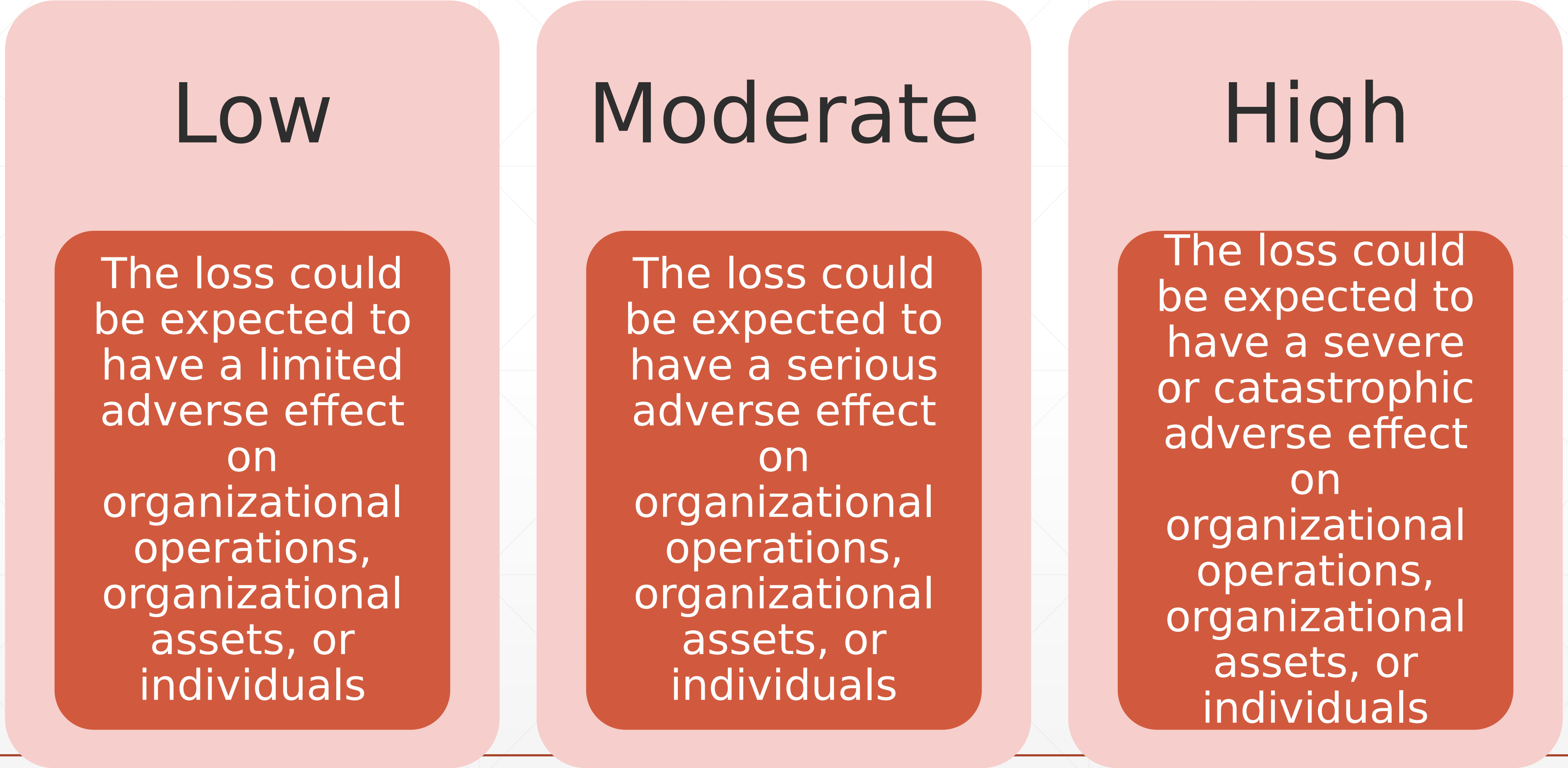


Figure 1.1 Essential Network and Computer Security Requirements

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

Challenges

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 needs to be determined
5. Security mechanisms typically involve more than a particular algorithm or protocol and also require that participants be in possession of some secret information which raises questions about the creation, distribution, and protection of that secret information
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

Scope of Computer Security

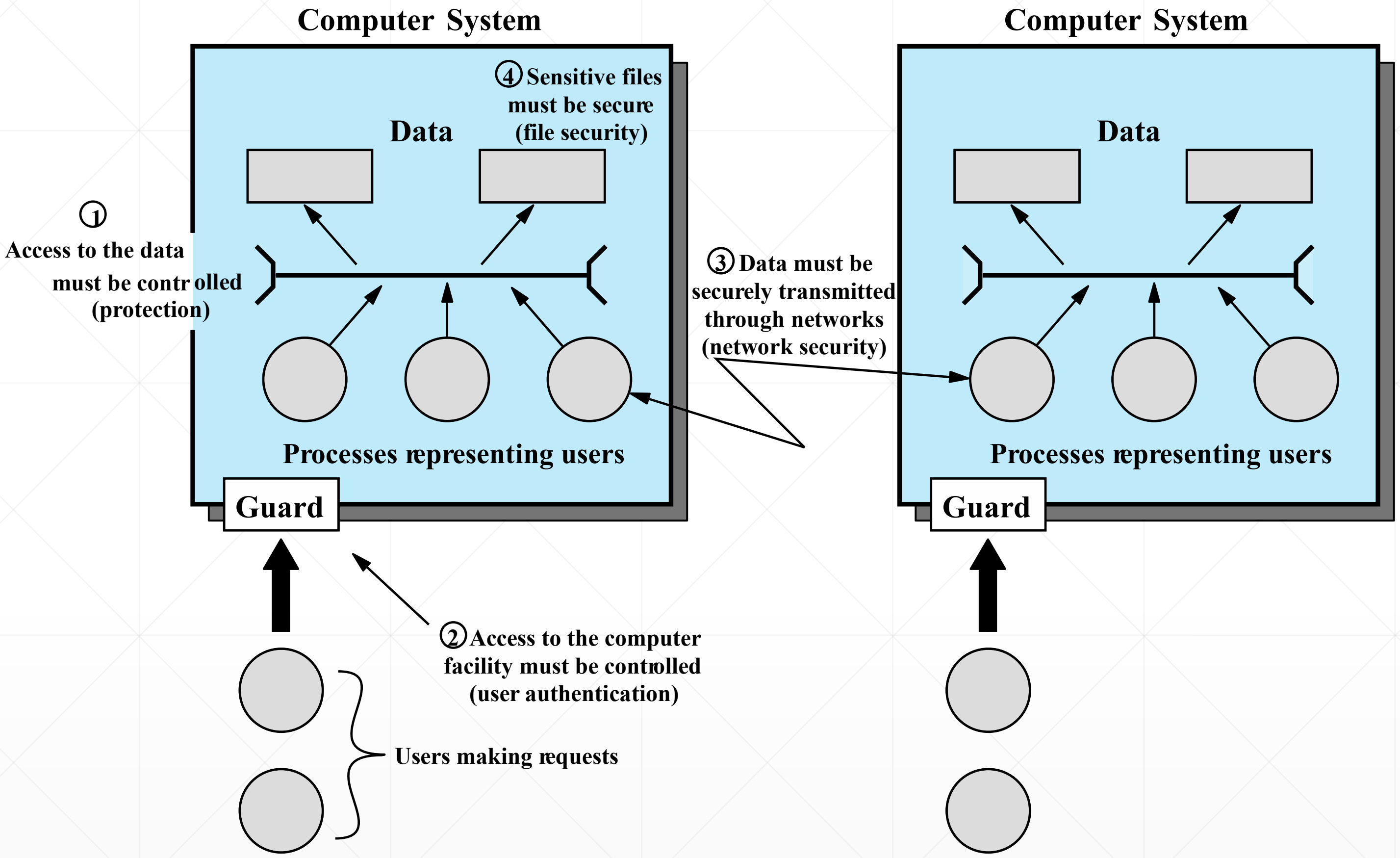
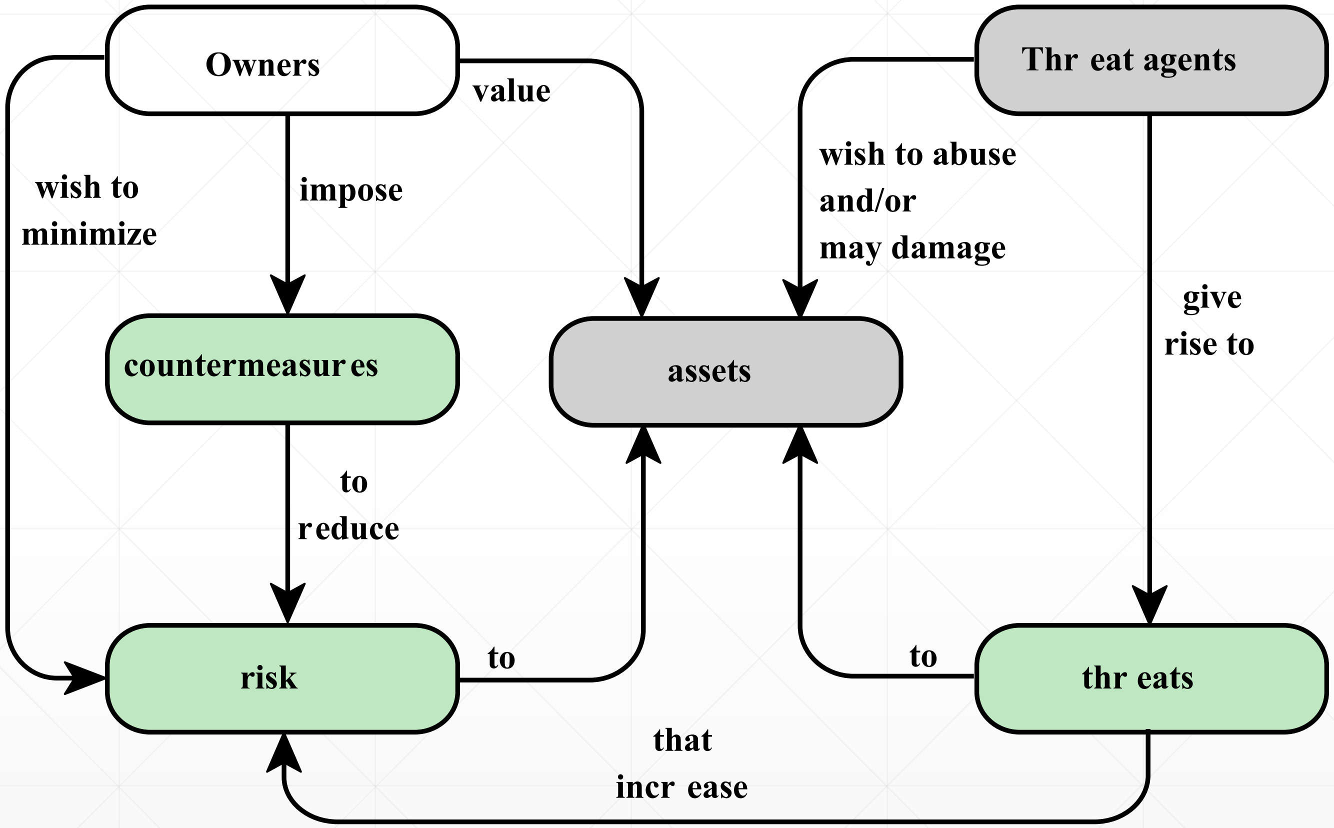

Computer System
Computer System
④ Sensitive files must be secure (file security)
Data
Data
① Access to the data must be contr olled (protection)
③ Data must be securely transmitted through networks (network security)
Processes representing users
Processes representing users
Guard
Guard
② Access to the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

Figure 1.3 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.

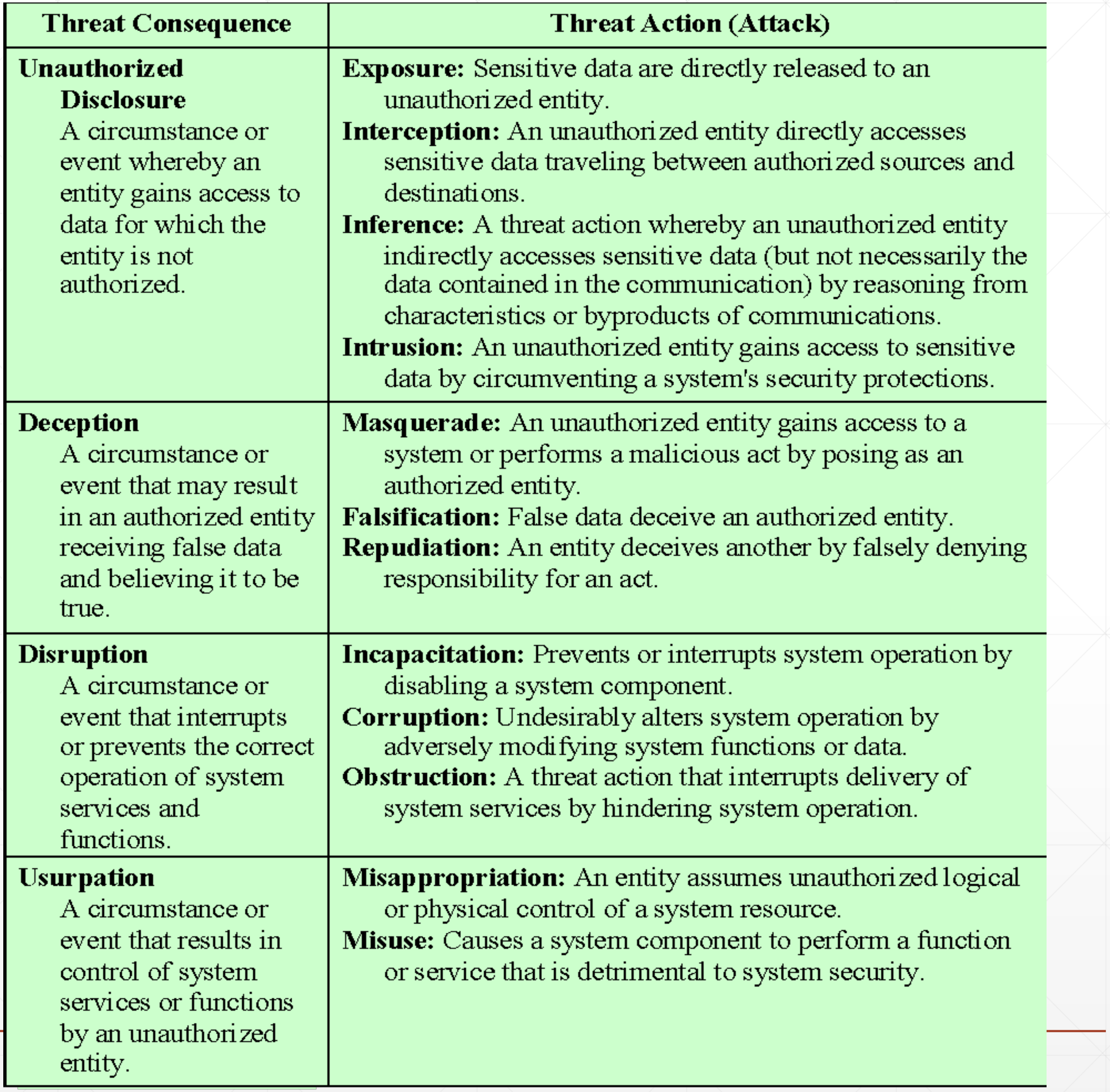
Security Concepts & Relationships

Threats, Risks, assets, and countermeasures



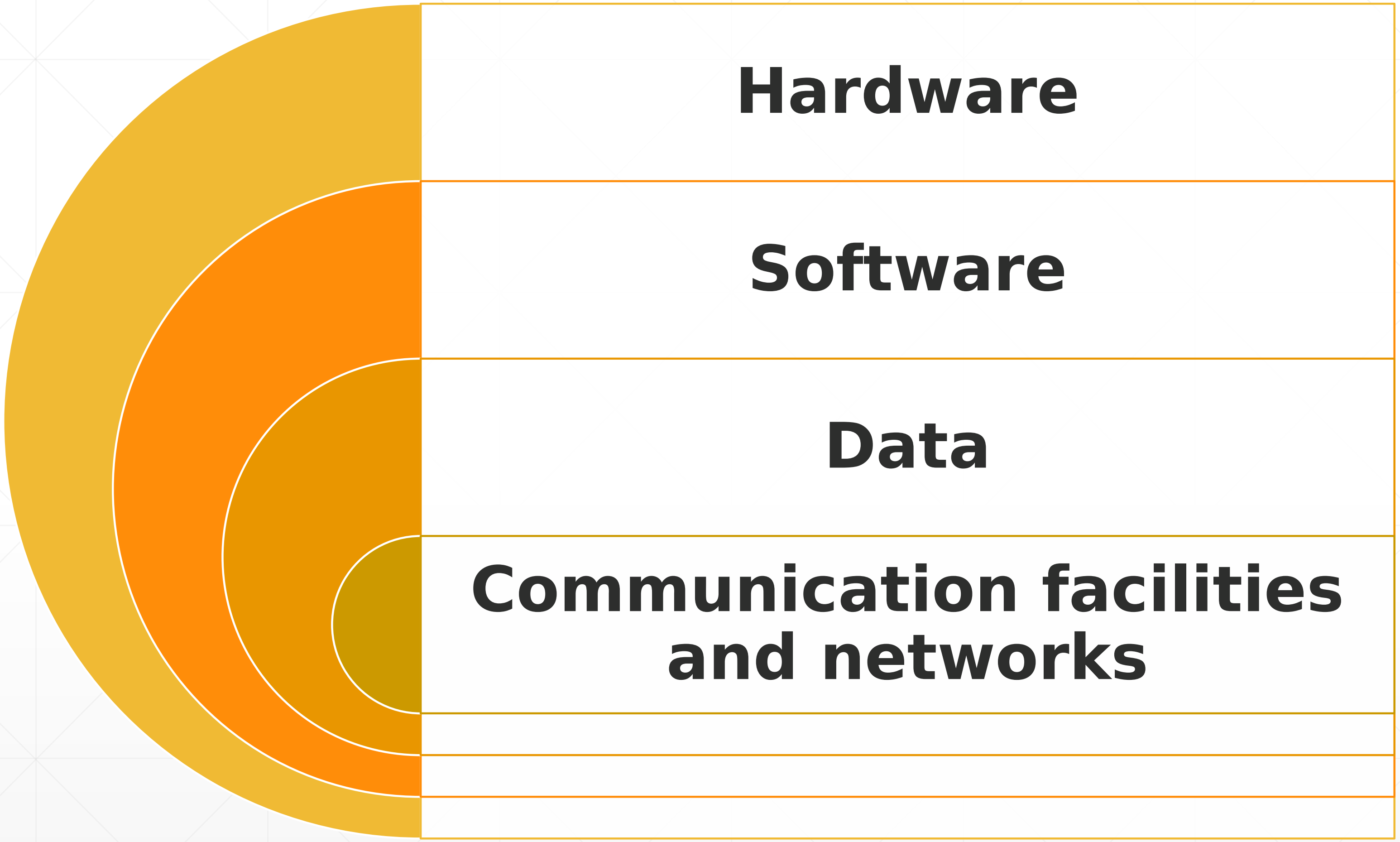
© Jason Choi @ CSU Fullerton

Threat Actions, Consequences



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 byproducts 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.

Assets of a Computer System



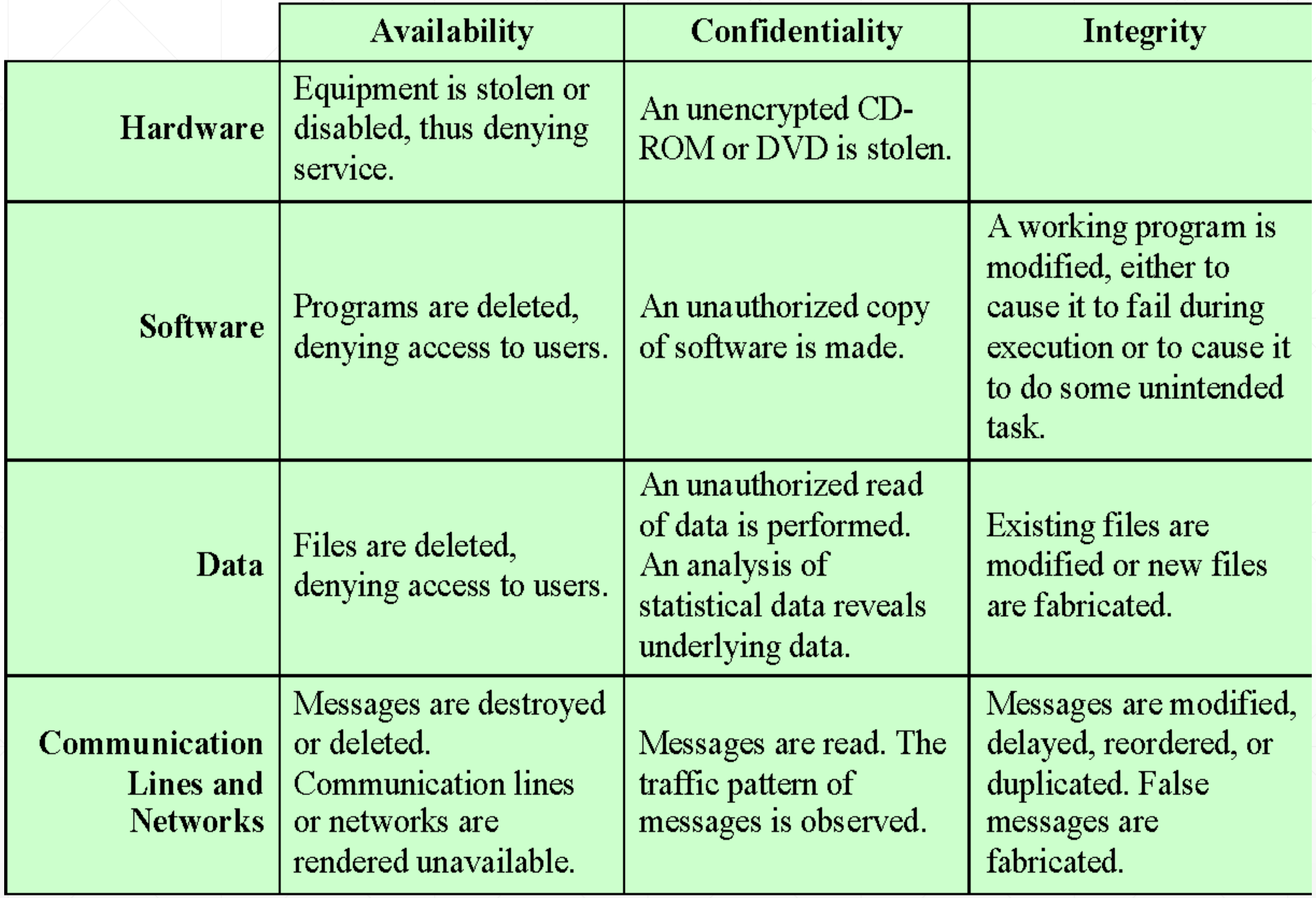
Hardware

Software

Data

Communication facilities and networks

Examples of Threats to Assets



	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Passive vs. Active Attacks

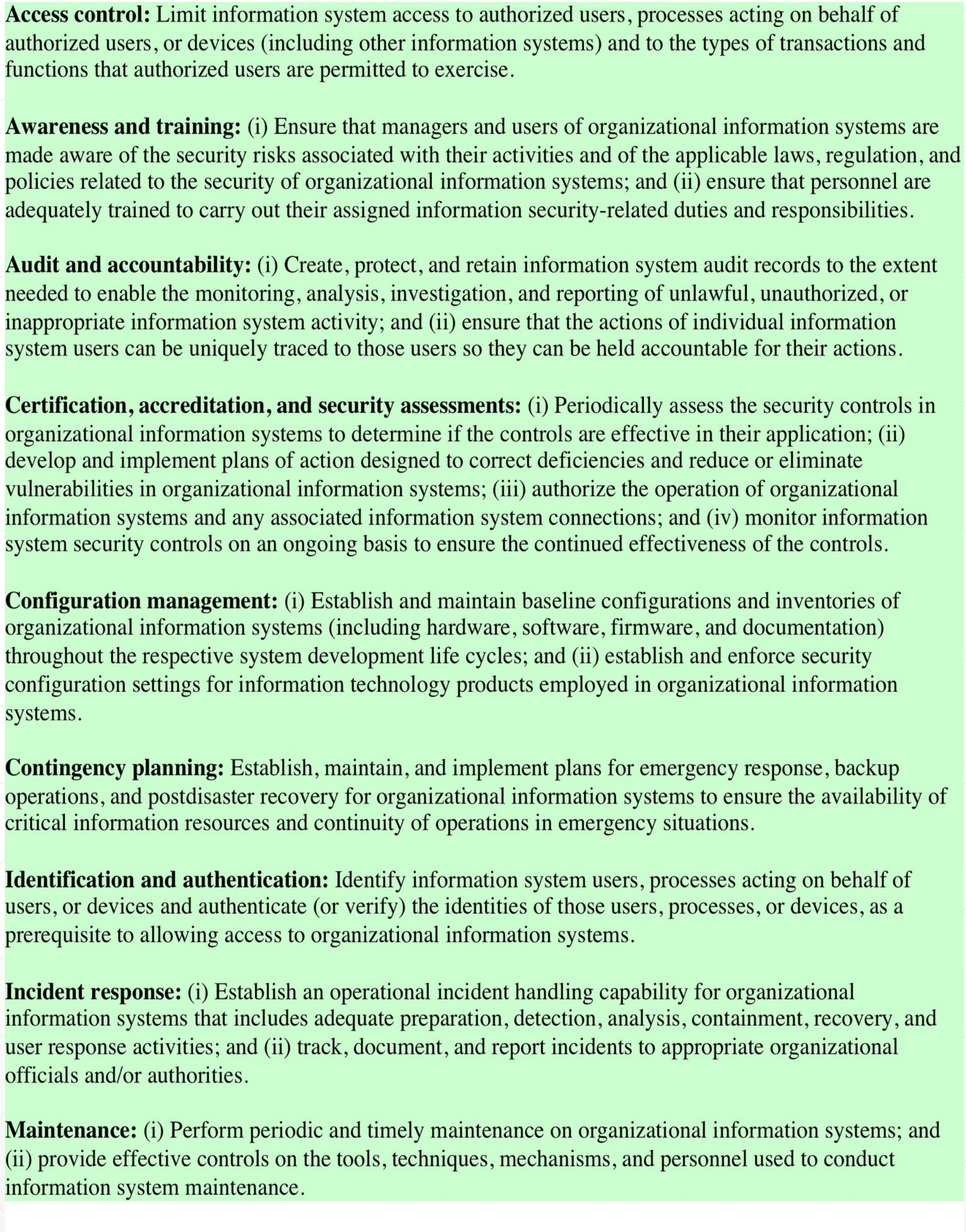
Passive

- Attempts to learn or make use of information without affecting the system resource
- Eavesdropping, monitoring
- Goal is to obtain information being transmitted
- Categories
  - Release of message contents, traffic analysis

Active

- Attempts to alter system resources or affect operation
- Modifies data stream or falsifies data
- Categories
  - Replay, masquerade, modification of messages, DoS

Security Requirements (FIPS 200)



Access control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and training: (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and accountability: (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, accreditation, and security assessments: (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

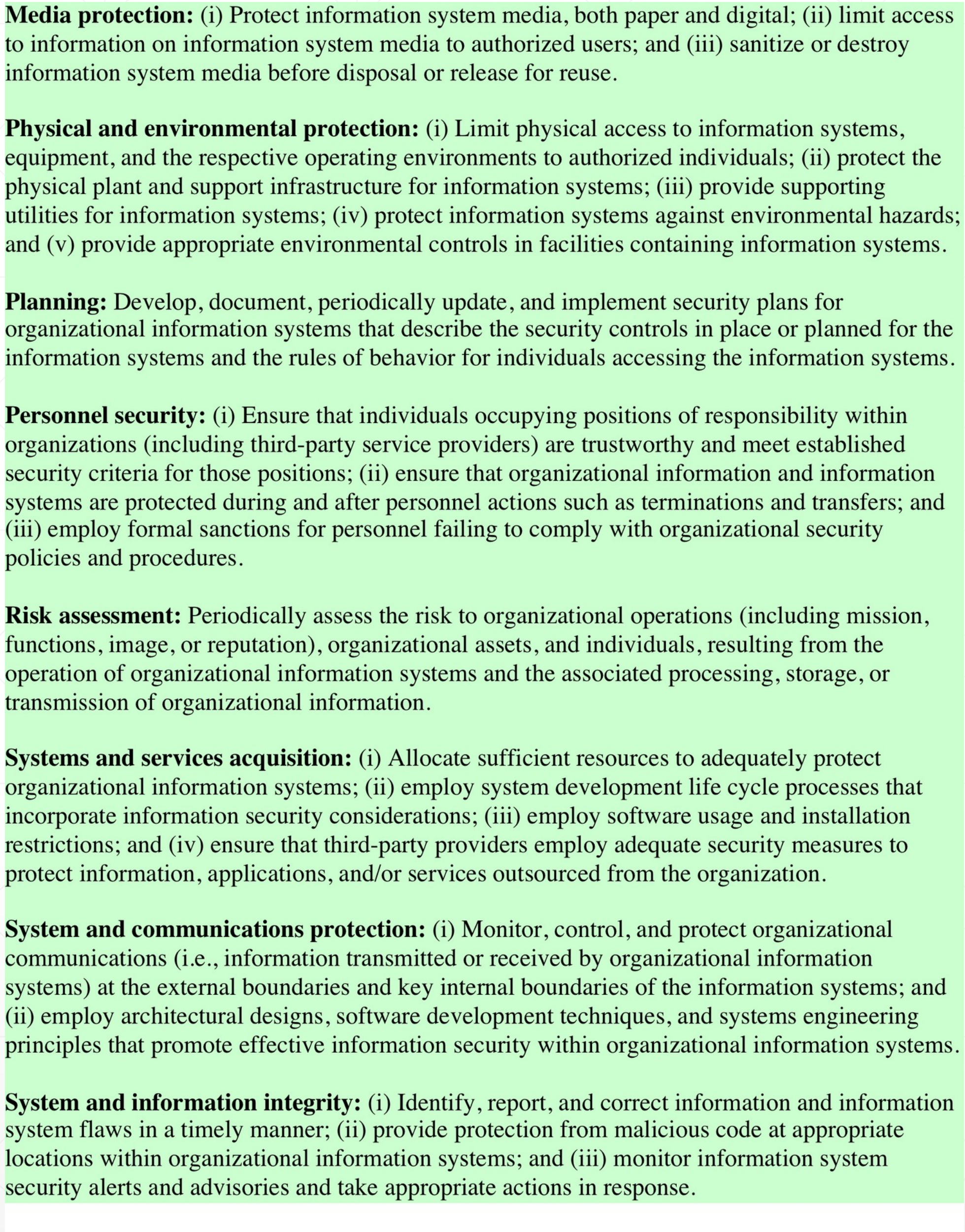
Configuration management: (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency planning: Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and authentication: Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident response: (i) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance: (i) Perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.



Media protection: (i) Protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and environmental protection: (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel security: (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) 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, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Systems and services acquisition: (i) Allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and communications protection: (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and information integrity: (i) Identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Fundamental Security Design Principles

- 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

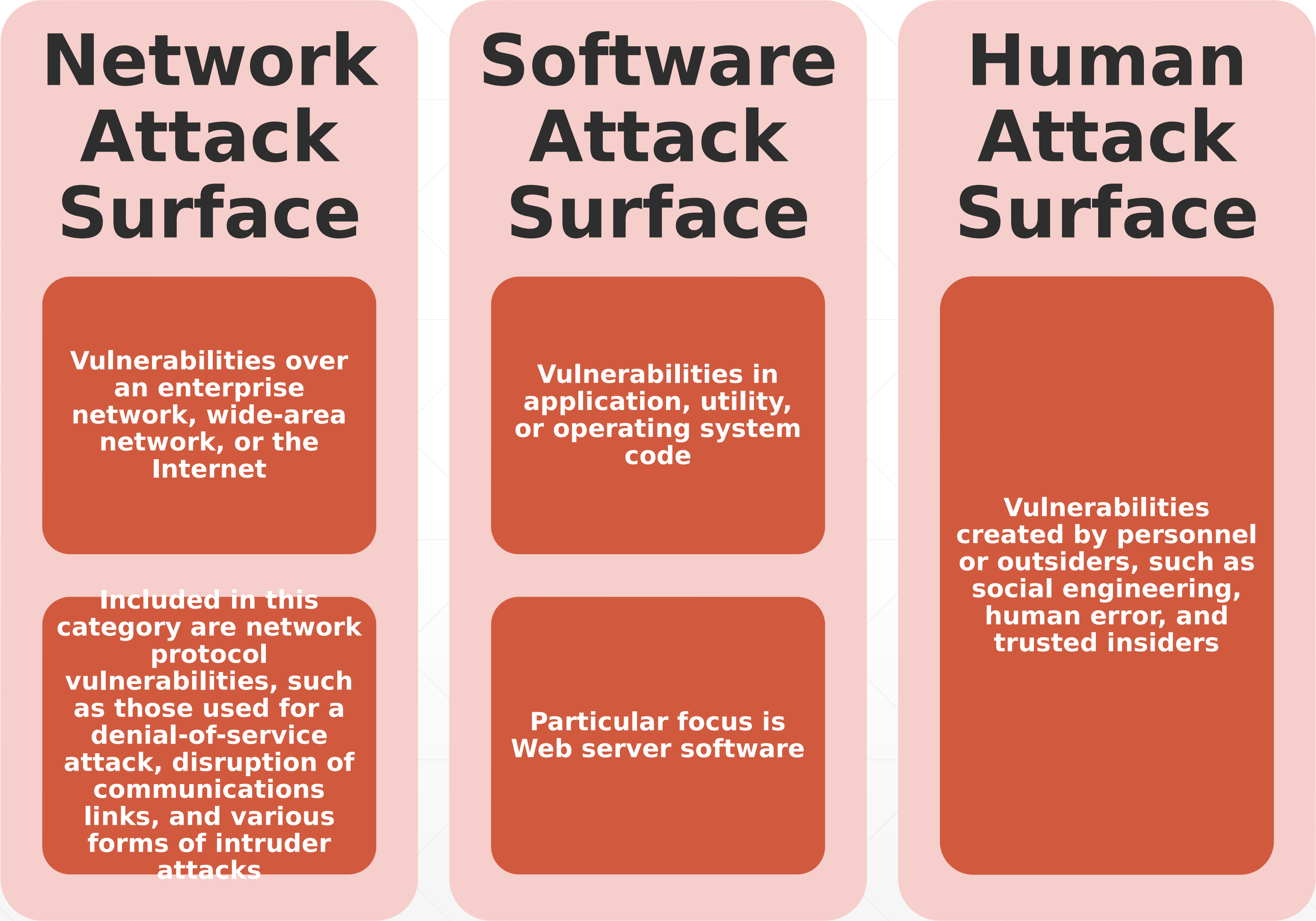
Attack Surfaces

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

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

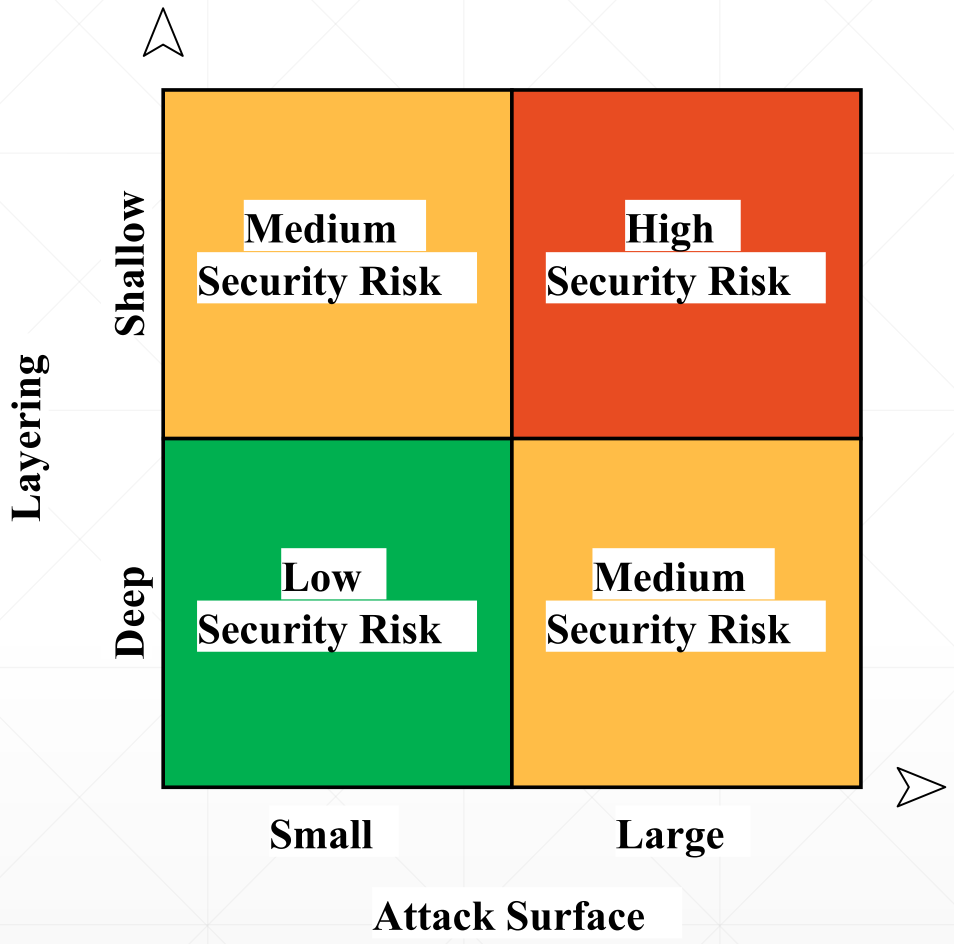
Vulnerabilities in application, utility, or operating system code

Particular focus is Web server software

Human Attack Surface

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

Defense in Depth and Attack Surface



Layering

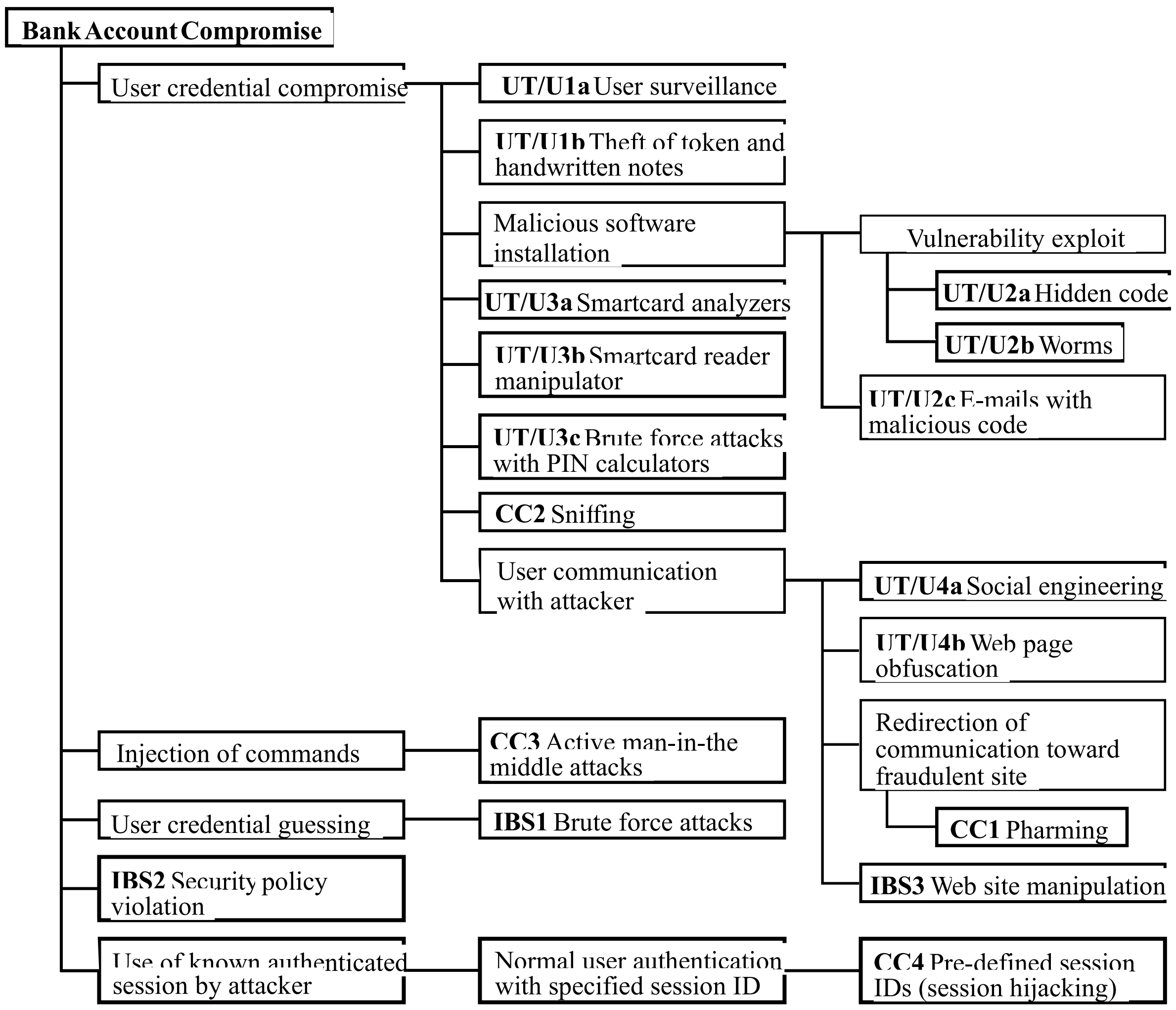
	Small	Large
Shallow	Medium Security Risk	High Security Risk
Deep	Low Security Risk	Medium Security Risk

Attack Surface

Figure 1.4 Defense in Depth and Attack Surface

Attack Trees

Branching, hierarchical data structures that represent a set of potential techniques for exploiting security vulnerabilities



- **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)

Figure 1.5 An Attack Tree for Internet BankingAuthentication

Computer Security Strategy

- Security Policy – A formal statement of rules and practices that specify or regulate how a system of organization provides security services to protect sensitive and critical system resources.
- Security Implementation – Involves four complementary courses of action
  - Prevention
  - Detection
  - Response
  - Recovery
- Assurance – 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. It can involve testing and formal analytic or mathematical techniques

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