ECCS 3411: Computer Security

LECTURE 2

COMPUTER SECURITY CONCEPTS

A Business Trip to South America Goes South

- **SCENARIO:**

A 10-person consulting firm sent a small team to South America to complete a client project. During their stay, an employee used a business debit card at a local ATM. A month after returning to the US, the firm received overdraft notices from their bank. They identified fraudulent withdrawals of $13,000, all originating from South America. There was an additional $1,000 overdraft fee.

Source: Small Business Cybersecurity Case Study Series
https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/case-study-series

A Business Trip to South America Goes South

- **ATTACK:** The criminals installed an ATM skimmer device to record card account credentials. Many false debit cards were manufactured and used at ATMs in different cities across South America.

- **RESPONSE:**

Realizing they had been defrauded, the firm contacted their bank and closed the impacted account immediately. Their attempts to pursue reimbursement from the bank were unsuccessful. The commercial account used at the ATM for local currency had different protections from consumer accounts and the bank was not required to reimburse them for their losses. The bank went on to deduct the $1,000 overdraft fee from the firm owner's account.

- **IMPACT:** The entire cash reserve for the small business was wiped out, netting losses of almost $15,000.

Source: Small Business Cybersecurity Case Study Series
https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/case-study-series

Key Security Concepts

- **Loss of Confidentiality:**

The unauthorized use of a stolen debit card can be considered a loss of confidentiality. In the context of information security, confidentiality refers to the protection of sensitive information from unauthorized access or disclosure. In the case of a stolen debit card, the cardholder's financial information is considered sensitive, and if it is accessed or used by someone without authorization, it can be seen as a breach of confidentiality.

- **Loss of Integrity:**

Integrity involves ensuring that data remains accurate, unaltered, and trustworthy. When a debit card is stolen and used without authorization, it can result in unauthorized transactions that compromise the integrity of the financial data associated with the card. The information may be altered or used in a way that was not intended by the legitimate cardholder.

- **Loss of Availability:**

Availability in information security refers to ensuring that authorized users have timely and reliable access to data and resources. In the case of a stolen debit card, the legitimate cardholder may face difficulties accessing their own funds due to unauthorized transactions or potential account freezes initiated by the bank to prevent further misuse. This can be considered a temporary loss of availability for the rightful owner.

Key Security Concepts

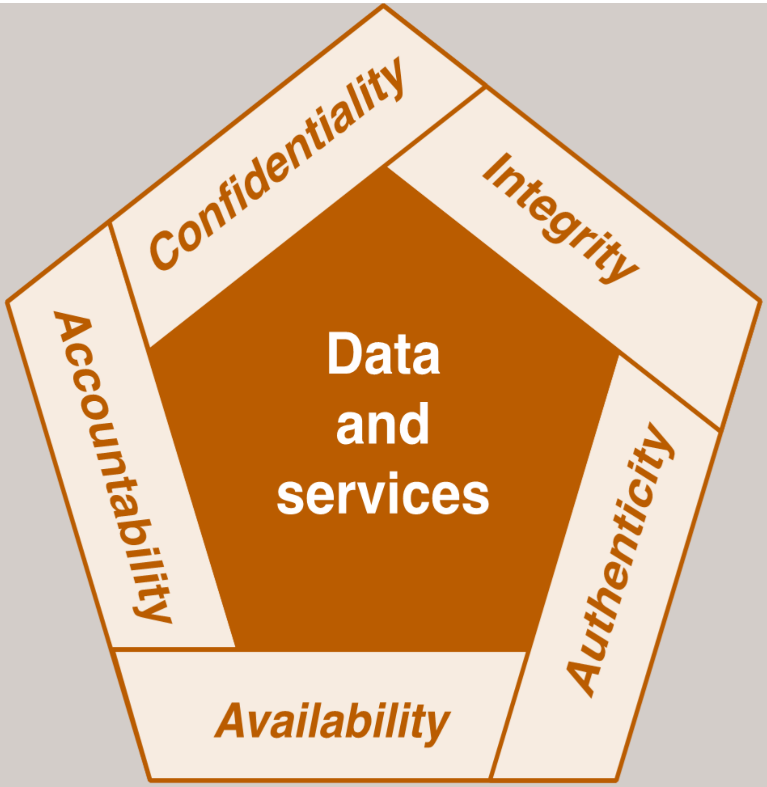


Figure 1.1 Essential Network and Computer Security Requirements

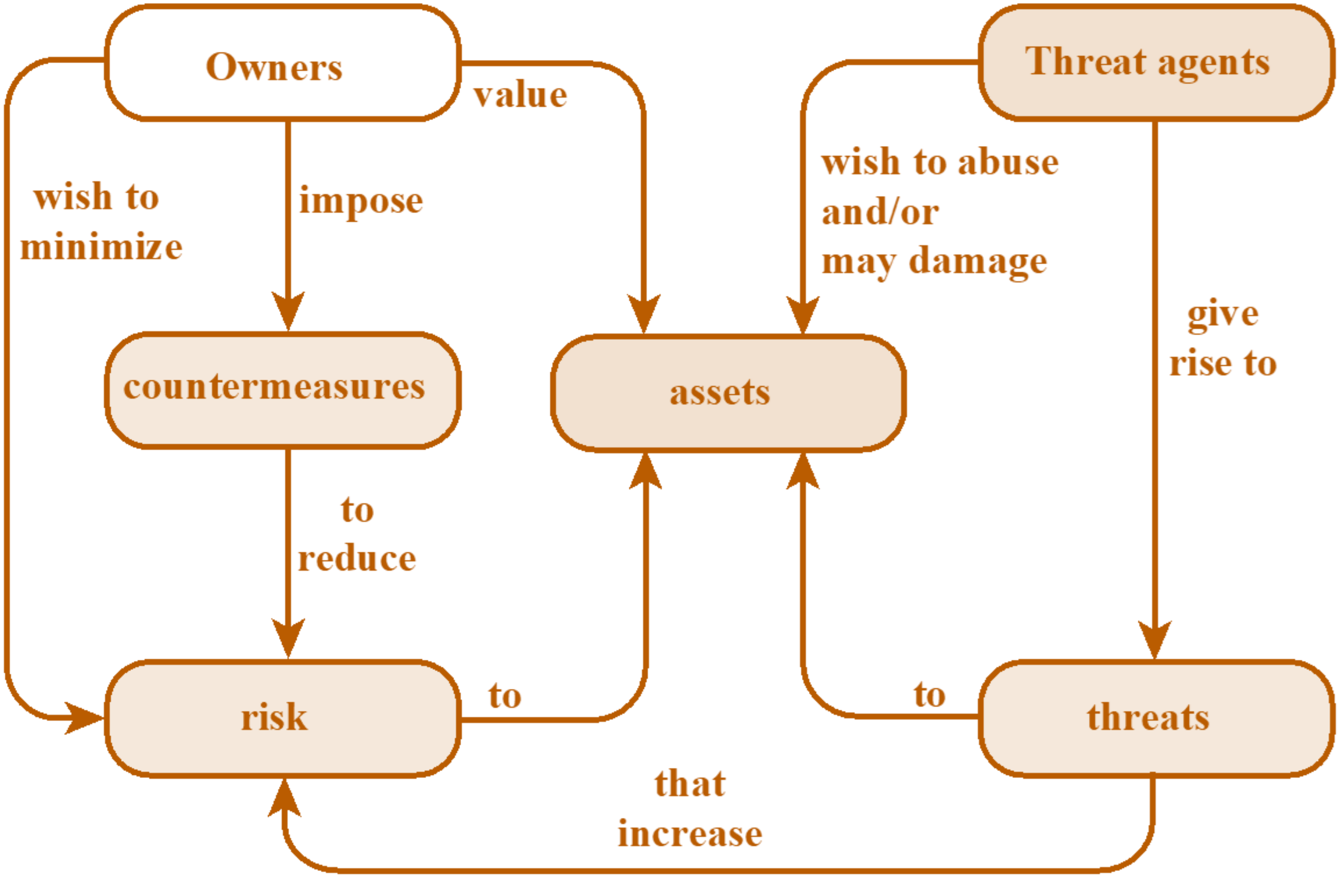


Figure 1.2 Security Concepts and Relationships

A Business Trip to South America Goes South

The three fundamental questions from this case study:

1. What assets do we need to protect?
2. How are those assets threatened?
3. What can we do to counter those threats?

A Business Trip to South America Goes South

The three fundamental questions from this case study:

1. What assets do we need to protect? – Cash Reserve
2. How are those assets threatened? – account breach
3. What can we do to counter those threats? –

The firm created two business accounts:

- one for receiving funds and making small transfers
- one for small expense payments

The firm updated travel protocols, banning the use of company-provided debit cards. Employees now prepay expenses electronically, pay cash, or use a major credit card, as necessary.

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

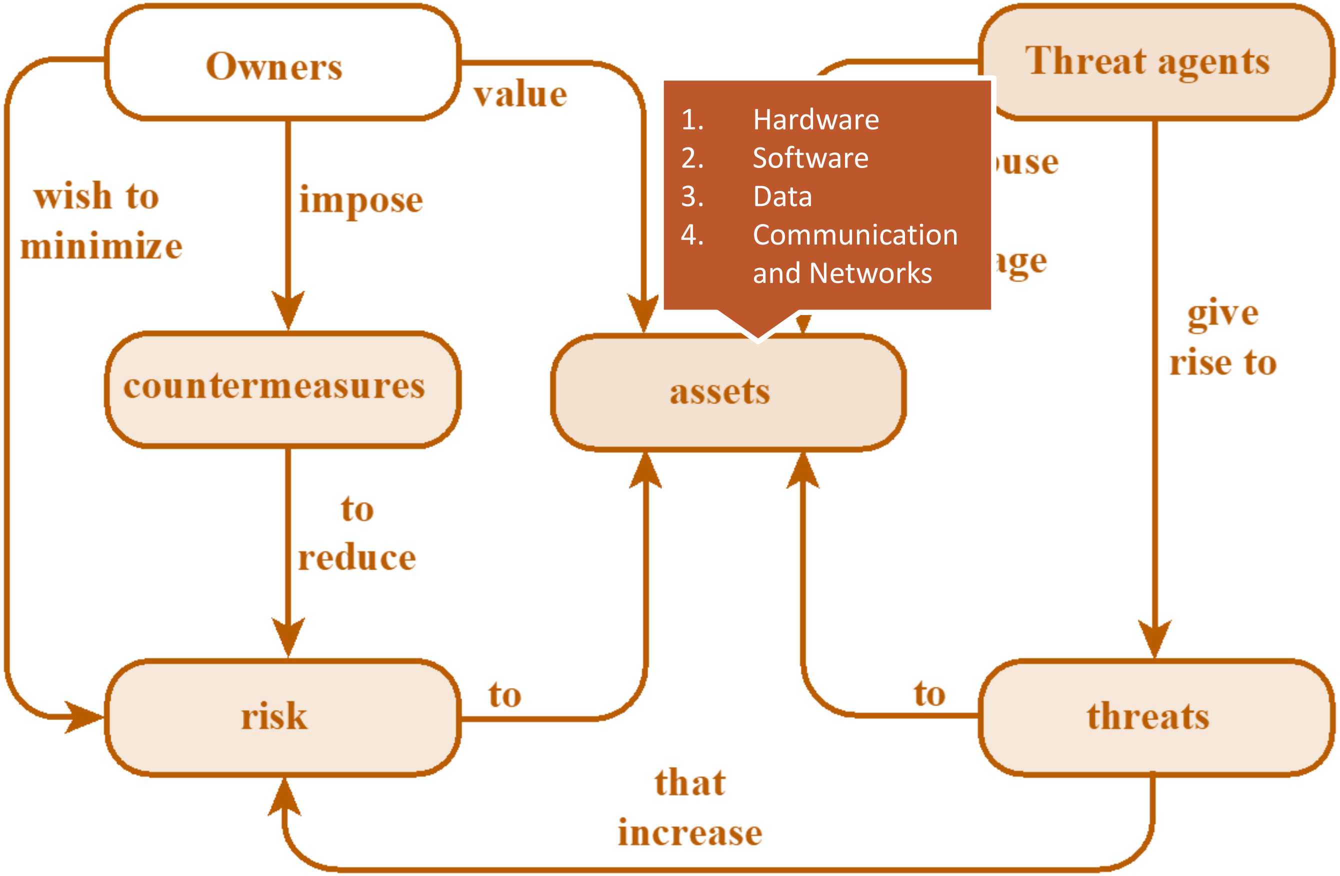
The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Computer Security Challenges

Some of the challenges:

1. Is it simple?
2. Potential attacks on security features
3. Physical and logical placement of these features
4. Proper functioning of the security mechanism
5. Attacker needs to find a single weakness
6. Security should be included in the design process
7. It requires regular and constant monitoring
8. Security as an impediment to efficient and user-friendly operations

Security Jargons



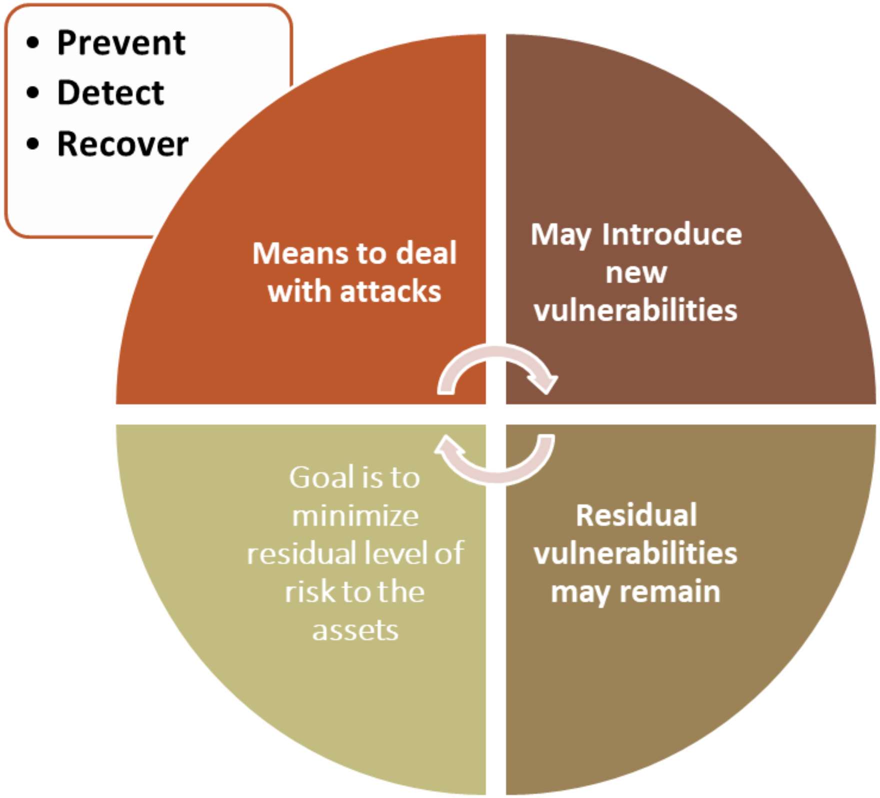
1. Hardware
2. Software
3. Data
4. Communication and Networks

Figure 1.2 Security Concepts and Relationships

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.”

Countermeasure



- Prevent
- Detect
- Recover

Means to deal with attacks

May Introduce new vulnerabilities

Residual vulnerabilities may remain

Goal is to minimize residual level of risk to the assets

Vulnerability

A vulnerability is a weakness or flaw in a system's design, implementation, operation, or management. Ex: A router with a default password is a vulnerability resulting from poor implementation.

A threat is any event that can potentially impact a system negatively through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

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

A threat actor is a person or group who exploits a vulnerability.

An attack is any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

A data breach is the exposure of data to an unauthorized user.

Data loss is the loss of access to data.

Data exfiltration is the unauthorized transfer of data.

An attack vector, or threat vector, is a path or means by which an attack is realized.

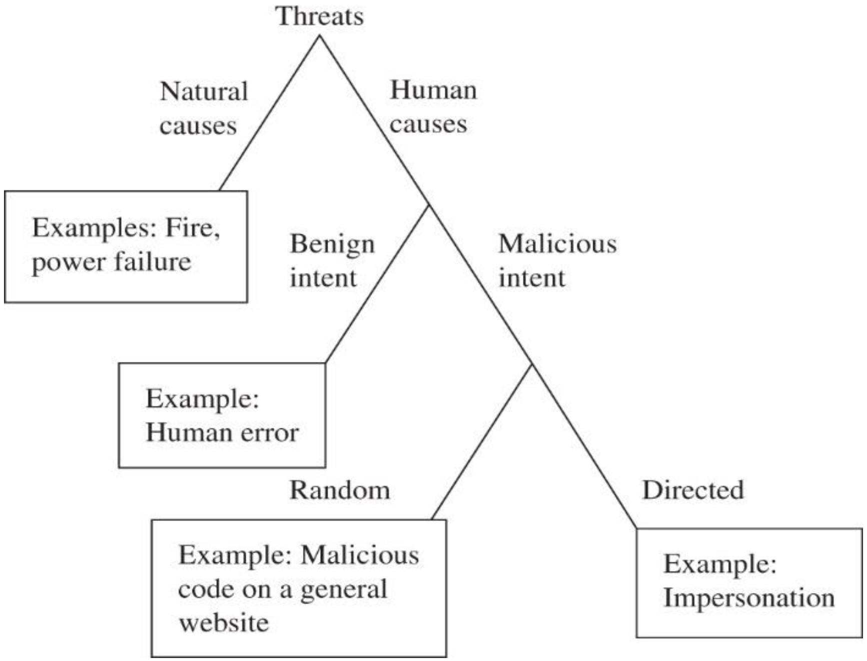
Vulnerability

1. An attacker sends an employee an email with an attachment containing a virus. The employee opens the email attachment and infects the computer.

Computer Vulnerabilities

- Weak Authentication
- Lack of Access Control
- Errors in Programs
- Finite or insufficient resources
- Inadequate Physical Protection

Kinds of Threats



From Security in Computing, Fifth Edition, by Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies (ISBN-13: 978-0-13-13408504-3)

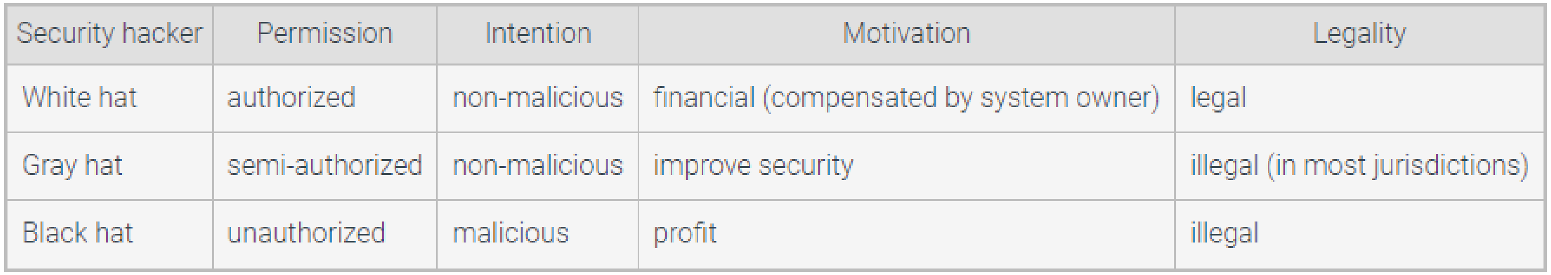
Attacks

Types of Attacks

1. Active Attacks
2. Passive Attacks
3. Insider Attack
4. Outsider Attack

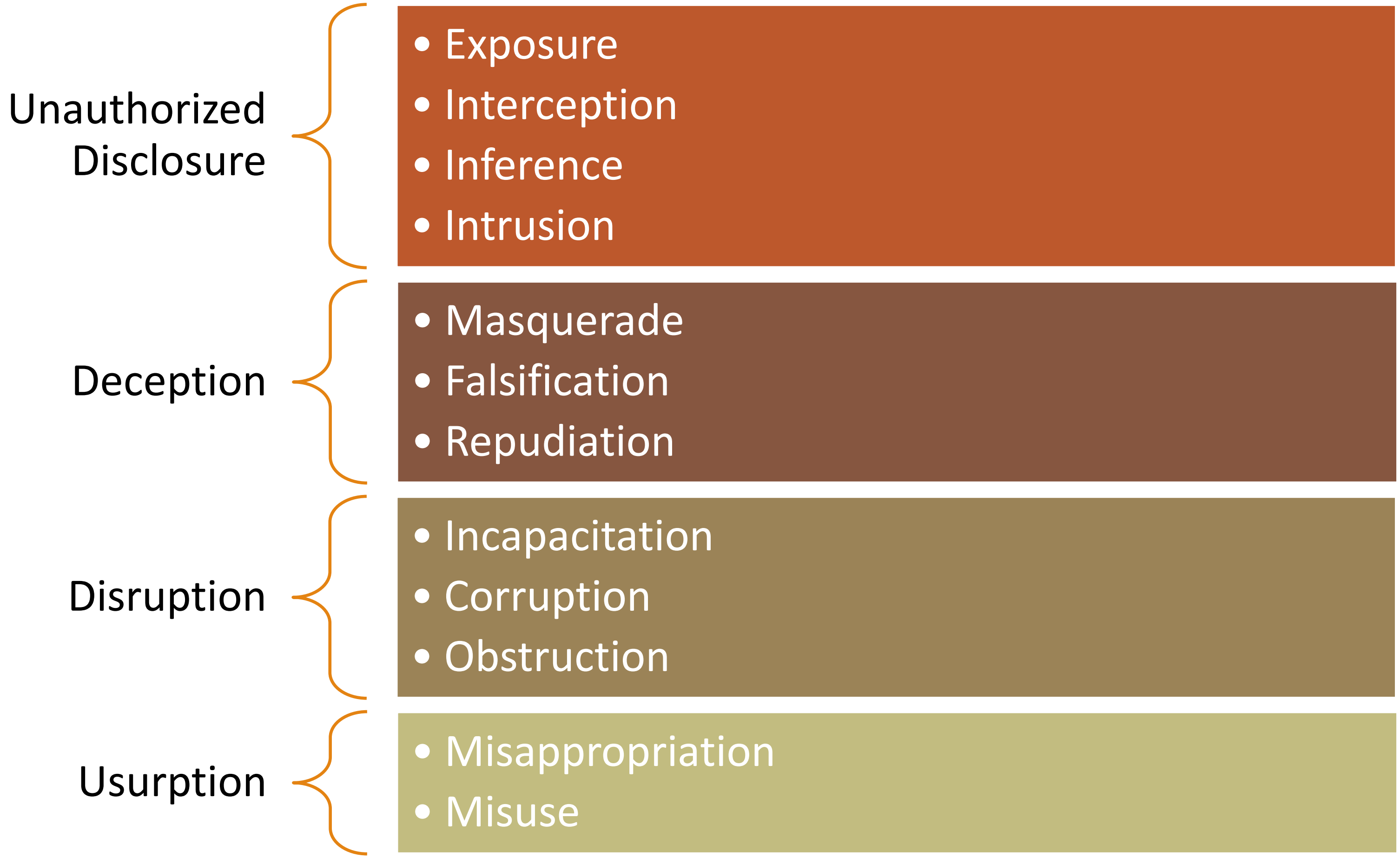
Types of Attackers

1. Hacker
2. State Actor
3. Advanced Persistent Threat (APT)
4. Hacktivist
5. Phishers and Malware Developers



Security hacker	Permission	Intention	Motivation	Legality
White hat	authorized	non-malicious	financial (compensated by system owner)	legal
Gray hat	semi-authorized	non-malicious	improve security	illegal (in most jurisdictions)
Black hat	unauthorized	malicious	profit	illegal

Threats and Attacks



Unauthorized Disclosure

- Exposure
- Interception
- Inference
- Intrusion

Deception

- Masquerade
- Falsification
- Repudiation

Disruption

- Incapacitation
- Corruption
- Obstruction

Usurption

- Misappropriation
- Misuse

Threats and Assets

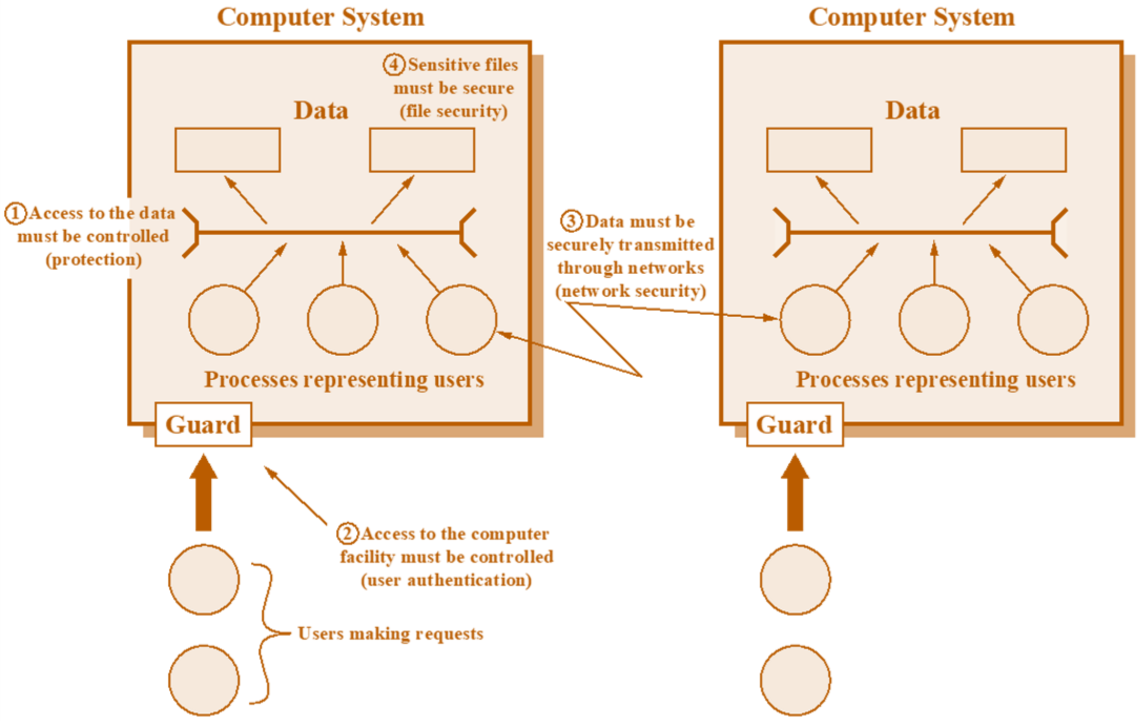
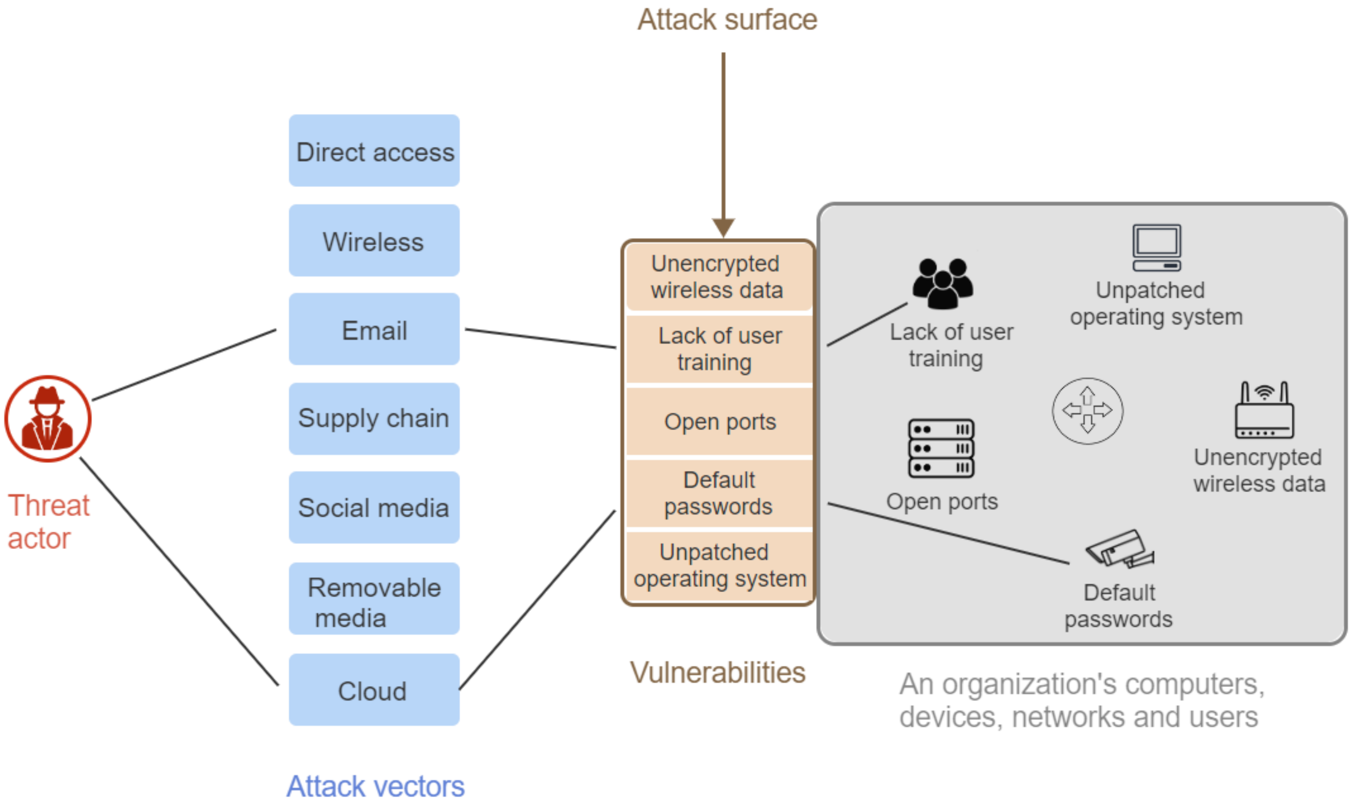

Computer System
Data
④Sensitive files must be secure (file security)
①Access to the data must be controlled (protection)
Processes representing users
Guard
③Data must be securely transmitted through networks (network security)
Computer System
Data
Processes representing users
Guard
②Access to the computer 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.

Attack Surface

- Consist of the reachable and exploitable vulnerabilities in a system



From zyBooks – Introduction to Computer Security with CompTIA Security+

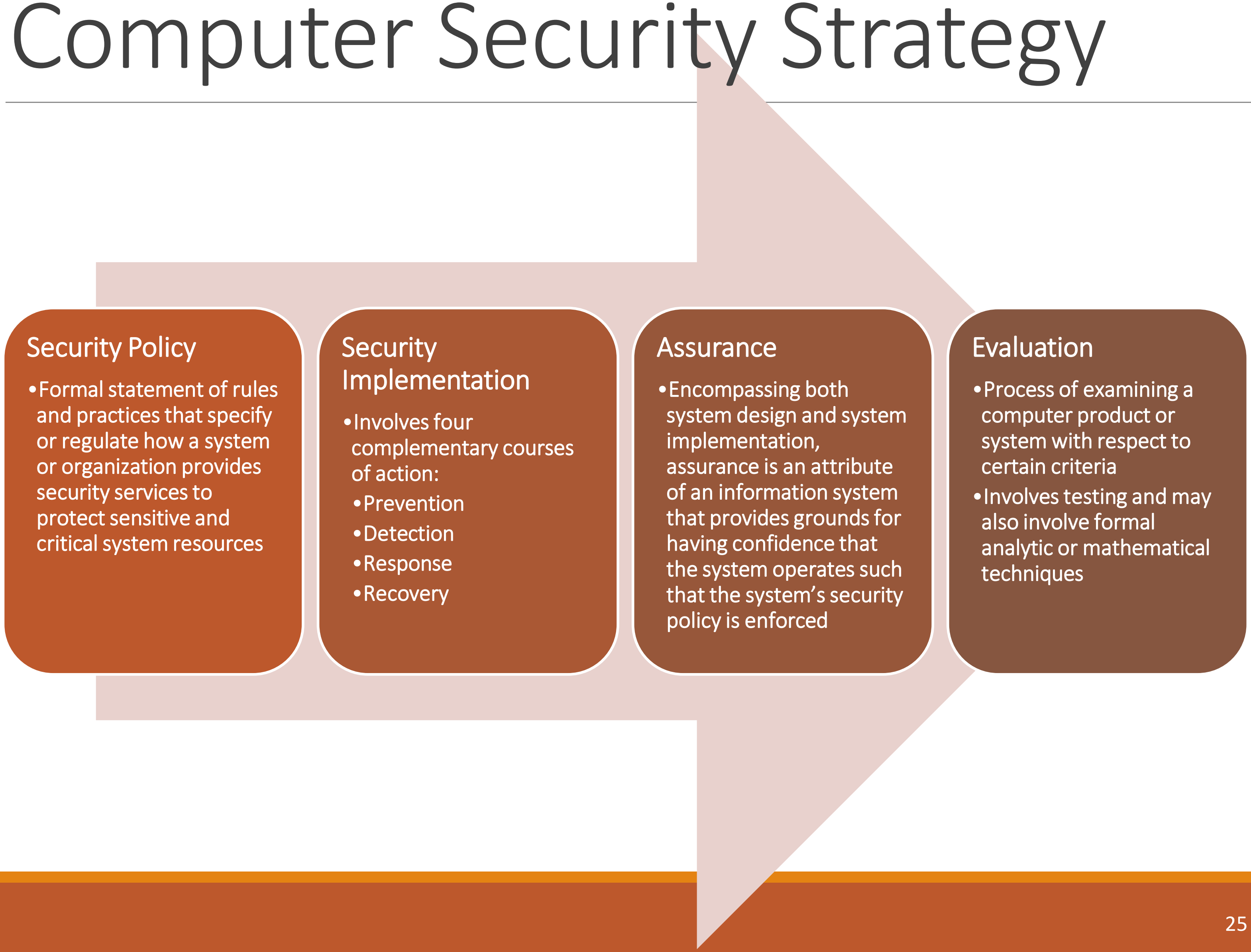
Security Requirements

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Certification, Accreditation and Security Assessments
5. Configuration Management
6. Contingency Planning
7. Identification and Authentication
8. Incident Response
9. Maintenance
10. Media Protection
11. Physical and Environmental Protection
12. Planning
13. Personnel Security
14. Risk Assessment
15. Systems and Services Acquisition
16. System and Communication Protection
17. System and Information Integrity

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 (Defense In Depth)
- Least astonishment

Computer Security Strategy



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

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

Standards

- Standards have been developed to cover management practices and the overall architecture of security mechanisms and services

National Institute of Standards and Technology (NIST)

US Federal Agency

- Deals with measurement science, standards and technology related to US government use
- Promotion of U.S. private sector innovation

Internet Society (ISOC)

Professional Membership Society

- Provides leadership in addressing issues that confront the future of the Internet
- Home for the groups responsible for Internet infrastructure standards

International Telecommunication Union (ITU-T)

United Nations Agency

- Governments and the private sector coordinate global telecom networks and services

International Organization for Standardization (ISO)

Nongovernmental Organization

- Work results in international agreements that are published as International Standards