Chapter One: Introduction to Information Security

School of Computer Engineering

Vahid Amin-Ghafari
Vahidaming@ustc.edu.cn

Index

Vulnerabilities: آسیب پذیری ها

A. Introduction

- What is Information Security?
  - The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or accidental (unintended) unauthorized access , damage, disclosure, manipulation, modification, loss, or use.
  - Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption (interruption/disorder), modification or destruction (damage).

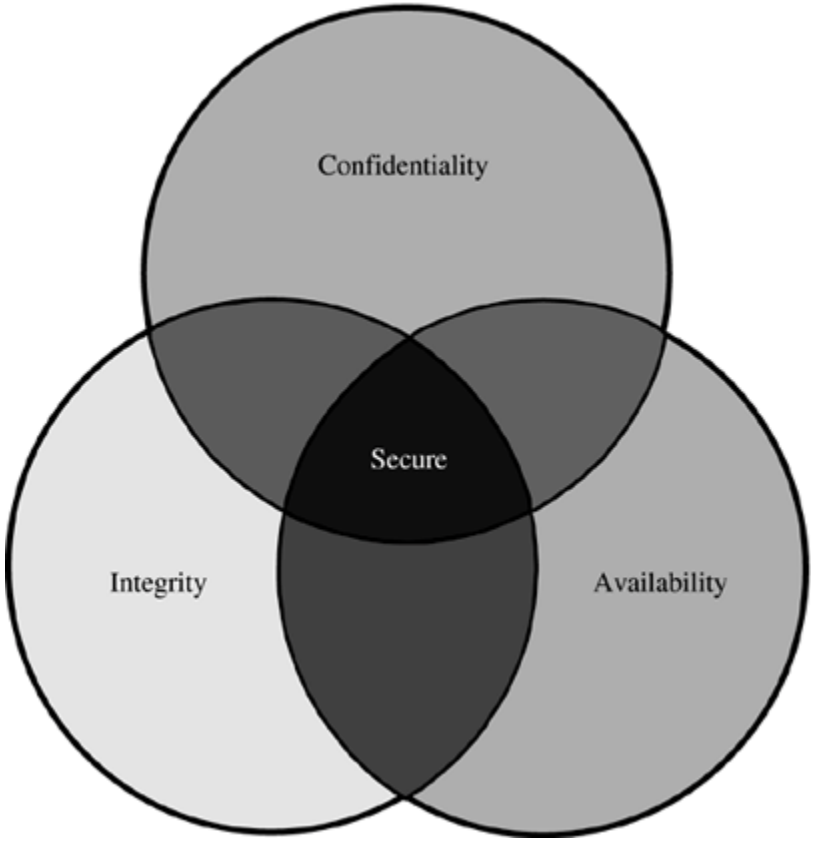
technical measures: اقدامات فنی

administrative measures: اقدامات اداری

IT Security

- **IT security** is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection (اختلال) of the services they provide.
- IT security performs four important functions for an organization:
  - Protects the organization's ability to function
  - Enables the safe operation of applications implemented on the organization's IT systems
  - Protects the data the organization collects and uses
  - Safeguards the technology assets in use at the organization

B. Security Goals:
When is any System Secure?



B. Security Goals:
When is any System Secure?

- **B.1. Confidentiality:** computer-related assets are accessed only by authorized parties. Confidentiality is sometimes called secrecy or privacy

- **B.2. Integrity:** assets can be modified only by authorized parties or only in authorized ways

- **B.3. Availability:** assets are accessible to authorized parties at appropriate times

B. Security Goals:

Confidentiality	Ensuring that information is accessible only to those authorised to have access.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Availability	Ensuring that authorised users have access to information and associated assets when required.

In some organisations, integrity and / or availability may be more important than confidentiality (Hospital).

B.1. Confidentiality (محرمانگی)

- It is not trivial to ensure confidentiality. For example,
  - Who determines which people or systems are authorized to access the current system?
  - By "accessing" data, do we mean that an authorized party can access a single bit? pieces of data out of context?
  - Can someone who is authorized disclose those data to other parties?

B.2. Integrity (یکپارچگی)

- It is much harder to ensure integrity. One reason is that integrity means different things in different context
- For example, if we say that we have preserved the integrity of an item, we may mean that the item is:
  - accurate
  - unmodified
  - modified only in acceptable ways
  - modified only by authorized people and processes
  - consistent

Accurate : (صحت) دقیق , Consistent: سازگار

B.3. Availability (دسترسی)

- Availability applies both to data and to services (i.e., to information and to information processing), and it is similarly complex
- We say a data item, service, or system is available if
  - There is a timely response to our request
  - There is a fair allocation of resources, so that some requesters are not favored over others
  - The service or system involved are fault tolerant - hardware or software faults lead to graceful stopping (cessation) of service or to work-a rounds rather than to crashes and sudden (abrupt) loss of information (تاب آوری)
  - The service or system can be used easily and in the way it was intended to be used

B.3. Availability

- The security community is just beginning to understand what availability implies and how to ensure it
- A small, centralized control of access is fundamental to preserving confidentiality and integrity, but it is not clear that a single access control point can enforce availability
- Much of computer security's past success has focused on confidentiality and integrity; full implementation of availability is security's next great challenge

Vulnerabilities (آسیب پذیری ها)

- A **vulnerability** is a weakness which can be exploited by a threat actor, such as an attacker, to cross benefit (privilege) boundaries (i.e. perform unauthorized actions) within a computer system.
- Vulnerabilities are classified according to the asset class they are related to:-
  - **Hardware:** Susceptibility to humidity/dust ; Unprotected storage; Over-heating.
  - **Software:** Insufficient testing; insecure coding; lack of audit trail; Design flaw.
  - **Network:** Unprotected communication lines; Insecure network architecture.
  - **Personnel:** Inadequate recruiting process; Inadequate security awareness; insider threat
  - **Physical site:** Area subject to natural disasters (e.g. flood, earthquake); interruption to power source
  - **Organizational:** Lack of regular audits; lack of continuity plans;

Threats (تهدیدها)

- **A threat** is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.
- *Any circumstance or event with the potential to adversely impact an IS (Information Systems) through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.*
- A countermeasure is any step you take to ward off a threat to protect user, data, or computer from harm.
- Various Security threats:
  - **Users:** Identity Theft; Loss of Privacy; Exposure to Spam; Physical Injuries.
  - **Hardware:** Power-related problems; theft; vandalism; and natural disasters.
  - **Data:** Malwares; Hacking; Cybercrime; and Cyber-terrorism.

Exposure to Spam: قرار گرفتن در معرض هرزنامه, vandalism: خرابکاری

B. Security Goals: Relationship of Security Goals

- A secure system must meet all three requirements.
- The challenge is how to find the right balance among the goals, which often conflict:
  - For example, it is easy to preserve a particular object's confidentiality in a secure system simply by preventing everyone from reading that object
  - However, this system is not secure, because it does not meet the requirement of availability for proper access
  - => There must be a balance between confidentiality and availability

Disposition of Period and Assessment

- **Class hour：(48 hours)**
- **Assessment： (20 points)**
  - **process assessment（40%）**
    - **Class attendance 5% (only 1 session absence)**
    - **Oral questions 10%**
    - **Homework assignment 5%**
    - **You should choose a topic in information security area and get my approve (20%):**
      - ✓**A presentation for 15 minutes as a recorded file or voiced. Try to innovate in this field.**
      - ✓**A report at least 10 page size: 12 pt, line spacing 1**
  - **(final + midterm) exam 65%, 5% extra points**
  - **Students will be fired with more than 6 absences.**
- I can't verify your problems.
- Rules are the same for all students.

Review Questions

1.What are the three basic principles of information security. Define each one?

2. Among the fundamental challenges in information security are confidentiality, integrity, and availability, or CIA. Give an example where confidentiality is required, but not integrity. Give an example where integrity is required, but not confidentiality. Give an example where availability is the overriding concern.

3. From a bank's perspective, which is usually more important, the integrity of its customer's data or the confidentiality of the data? From the perspective of the bank's customer, which is more important?

4. Some authors distinguish between secrecy, privacy, and confidentiality. In this usage, secrecy is equivalent to our use of the term confidentiality, whereas privacy is secrecy applied to personal data and confidentiality refers to an obligation not to divulge certain information. Discuss an example where privacy is required. Discuss an example where confidentiality (in this sense) is required

5. What is the difference between confidentiality and privacy?

C. Threats, Vulnerabilities and Controls

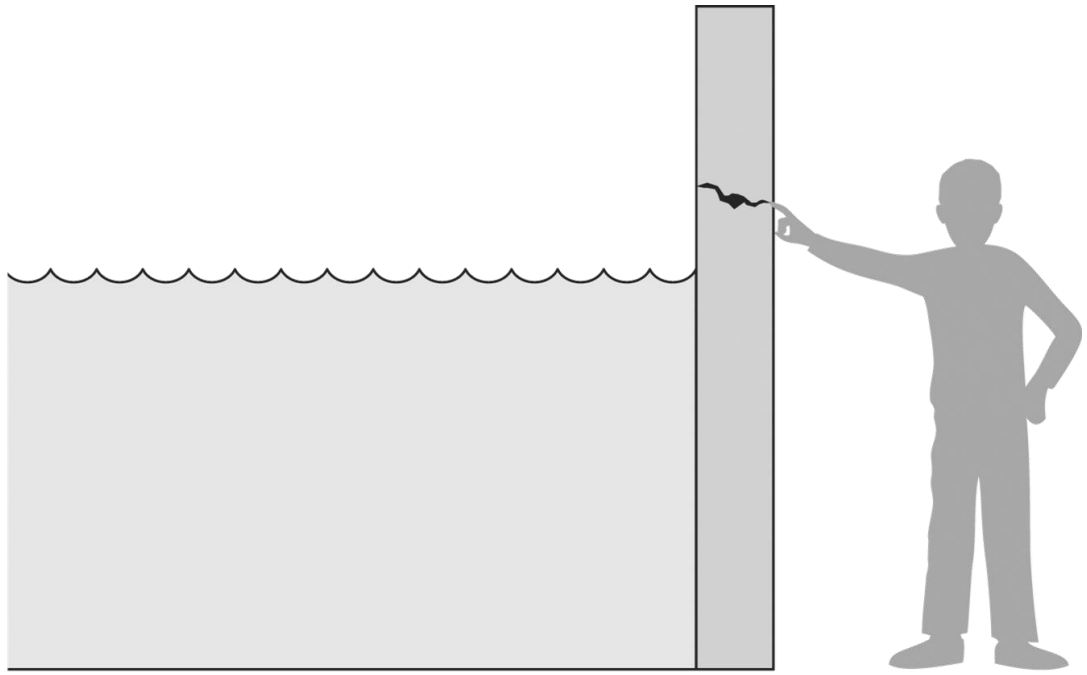
- **C.1. Threats:** Something that can potentially cause damage to information assets.

- **C.2. Vulnerabilities:** A weakness in the organization, computer system, or network that can be exploited by threat.

- **C.3. Control:** an action, device, procedure, or technique that remove or reduce a vulnerabilities.

Potentially: به طور بالقوه

C. Threats, Vulnerabilities and Controls



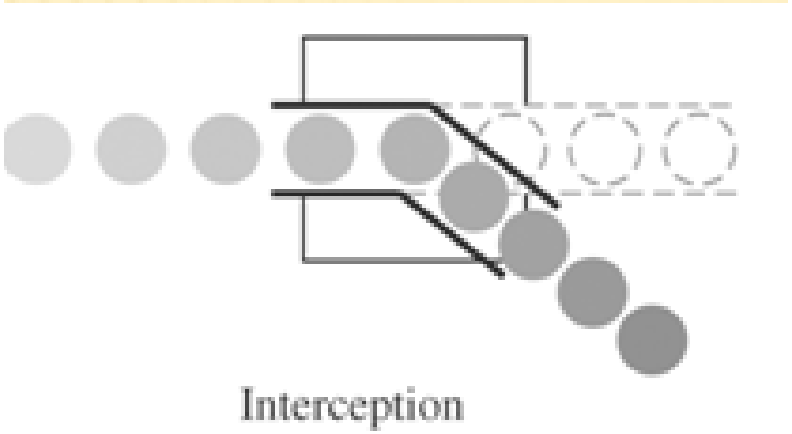
A threat is blocked by control of a vulnerability

C.1. Threats

- Definition: Something that can potentially cause damage to information assets.
- A malicious attacker must have three things:
  - Method: the skills, knowledge, tools, and other things with which to be able to succeed the attack.
  - Opportunity: the time and the access to accomplish the attack.
  - Motive: a reason to want to perform this attack against this system.

C.1. Threats: Types

1. Interception: some unauthorized party has gained access to an asset, the outside party can be a person, a program, or computing system.
   - Example: illicit (forbidden) copying of program or data files, or wiretapping to obtain data in a network

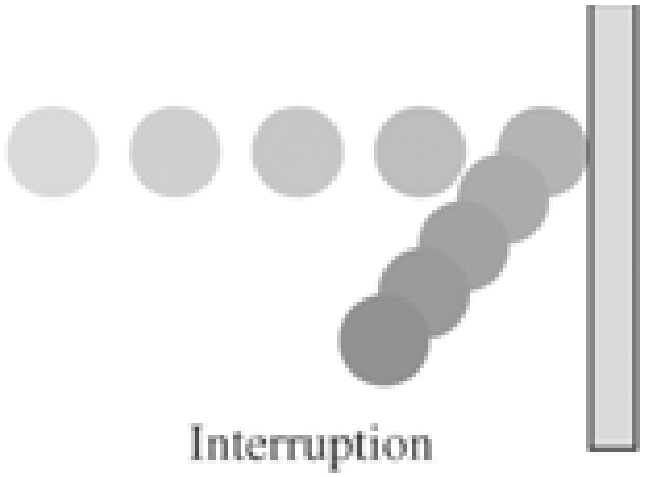


Interception

~ an attack on confidentiality

C.1. Threats: Types

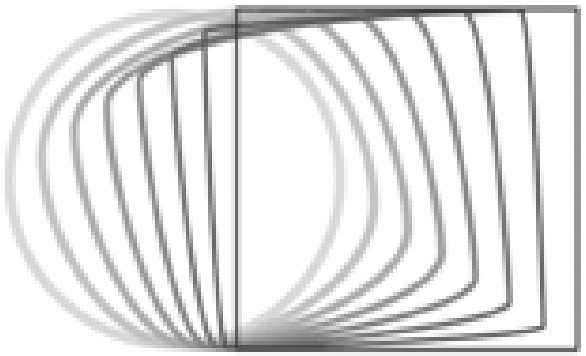
2. Interruption: an asset of the system becomes lost, unavailable, or unusable.
   - Example: malicious destruction of a hardware device, deletion (erasure) of a program or data file, denial of service attacks



~ an attack on availability

C.1. Threats: Types

3. Modification: alteration the values in a database, or programs to perform additional computation, or modify data being transmitted electronically.
   - Example: someone might change the values in a database, alter a program so that it performs an additional computation

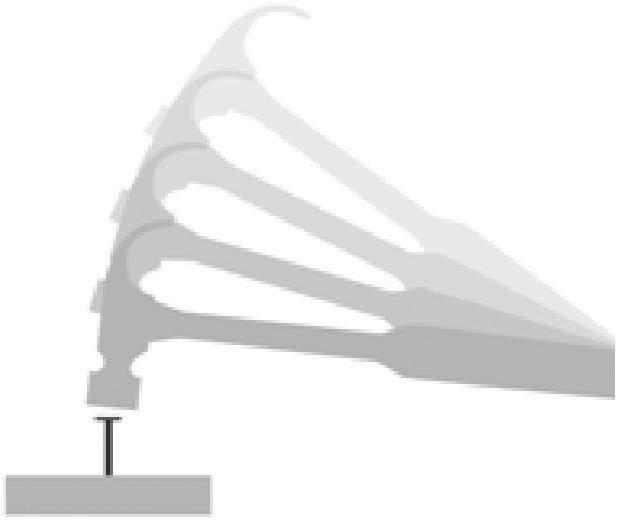


Modification

~ an attack on integrity

C.1. Threats: Types

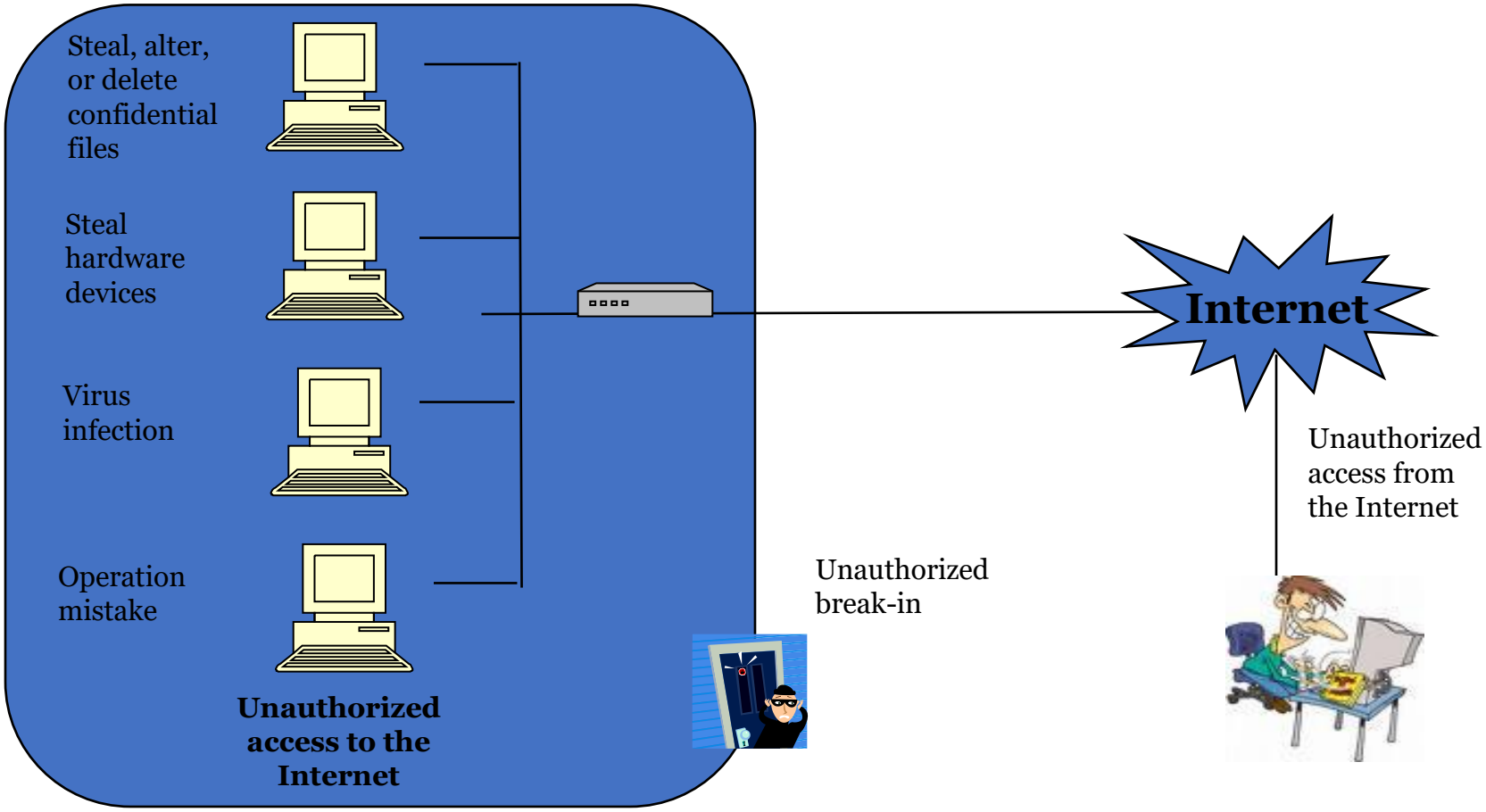
4. Fabrication: An unauthorized party might create a fabrication of fake (counterfeit) objects on a computing system.
   - Example: the intruder may insert false (spurious) transactions to a network communication system, or add records to an existing database



Fabrication

~ an attack on authenticity

C.1. Threats: Examples



Computer and Network Assets
Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
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	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.

C.2. Vulnerabilities

- Definition: A weakness in the organization, computer system, or network that can be exploited by threat.
- Examples:
  - Security policy is not set.
  - Roles and responsibilities are vague (unclear).
  - Security training of employees are inadequate (insufficient).
  - Building entrance are not checked thoroughly.
  - There is not protection against computer viruses.
  - A software bug exists in the server OS.
  - No password rules are set.
  - Confidential data are sent over the network.

Organization

Computer System

Network

C.2. Vulnerabilities: Example 1: Building

Threats of building break-ins:

1. Theft of keys, ID cards, passwords, etc.
2. Following an authorized person.
3. Pretending to be a sweeper or deliveryman.

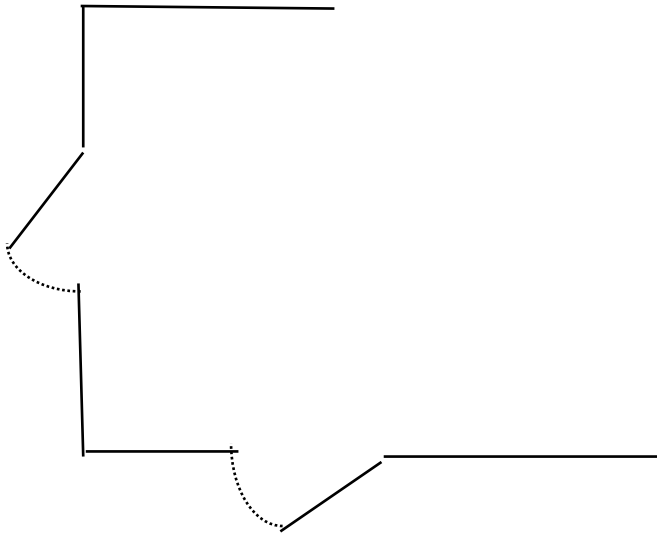
Vulnerabilities:

1. Lost ID cards are not reported.
2. No guards to check entry.
3. Sweeper's ID is not checked.

1. Entering with stolen ID cards

2. Following a person who unlocks the door

3. Entering with a stolen uniform of a deliveryman



C.2. Vulnerabilities: Example 2: Within the Office

Threats in the Office:

1. Theft of documents or disks, and/or making copies.
2. Theft of hardware.
3. Theft of discarded documents

Vulnerabilities:

1. Sensitive documents are not stored in locked cabinet.
2. Computers are not locked to desks.
3. Sensitive documents are not shredded (tear into small pieces)

1. Theft of documents or disks

2. Theft of computers

3. Picking up documents from a trash box

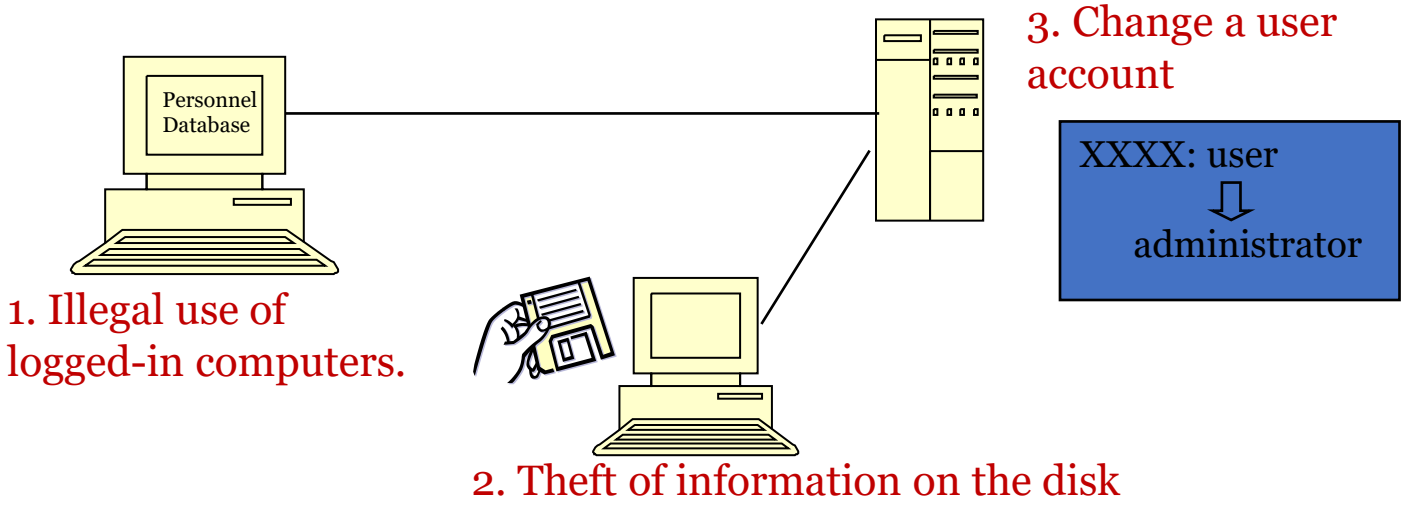
C.2. Vulnerabilities: Example 3: Computer System

Threats to a computer system:

1. Illegally operate on an already logged-in computers.
2. Information theft from a client or server.
3. Change a system setting or account

Vulnerabilities:

1. Computers are left unattended in a logged-in state.
2. No password is set.
3. Easy passwords are set on server.



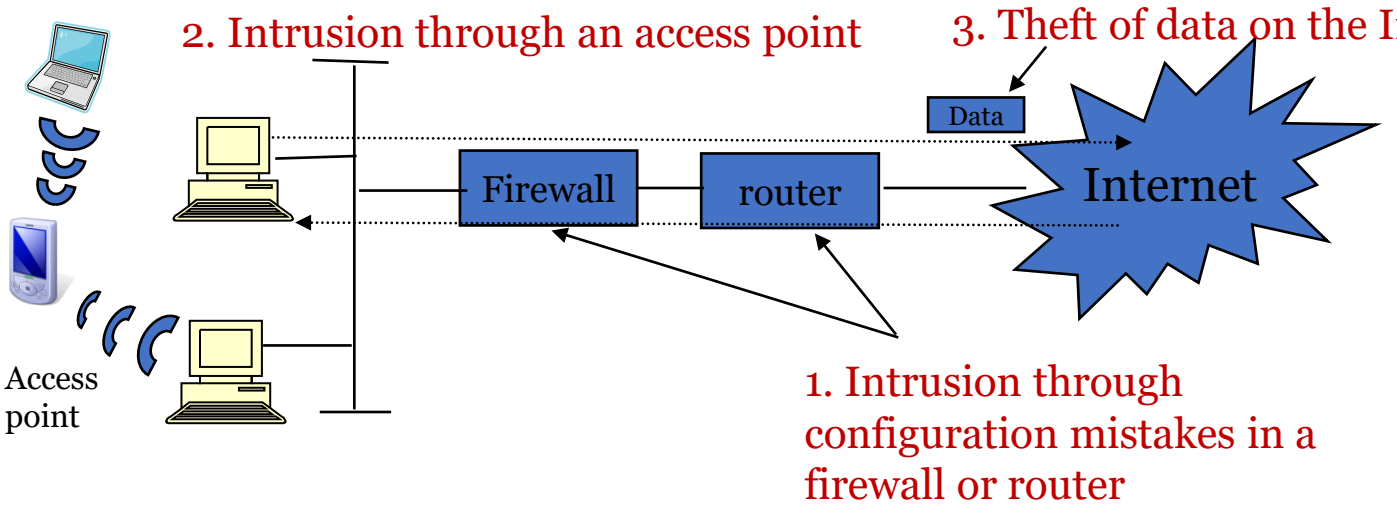
C.2. Vulnerabilities: Example 4: Network

Threats using networks:

1. Intrusion through security holes in a router or firewall.
2. Intrusion through wireless LAN's access point.
3. Theft or alteration of data during transmission on the network

Vulnerabilities:

1. Router's and firewall's access list is improperly configured..
2. Access point is not configured to prevent illegal access..
3. Transmitted data are not encrypted.



C.2. Vulnerabilities: Example 5: Software

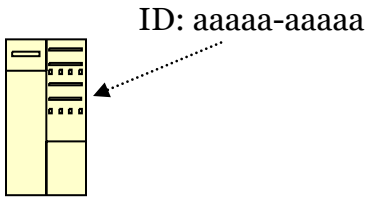
Software threats:

1. Buffer overflow attacks.
2. Malicious code
3. Denial of Service (DoS) attack

Vulnerabilities:

1. Bugs in OSs or applications.
2. No protection against computer viruses.
3. Security hole exists in the server.

1. When receiving IDs that are too long, the system stops. (overflow)

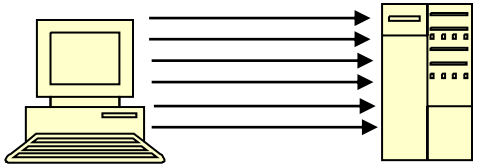


2. When a mail infected with a computer virus is opened

To: %%%
From: $$$

Attach: xxx
virus

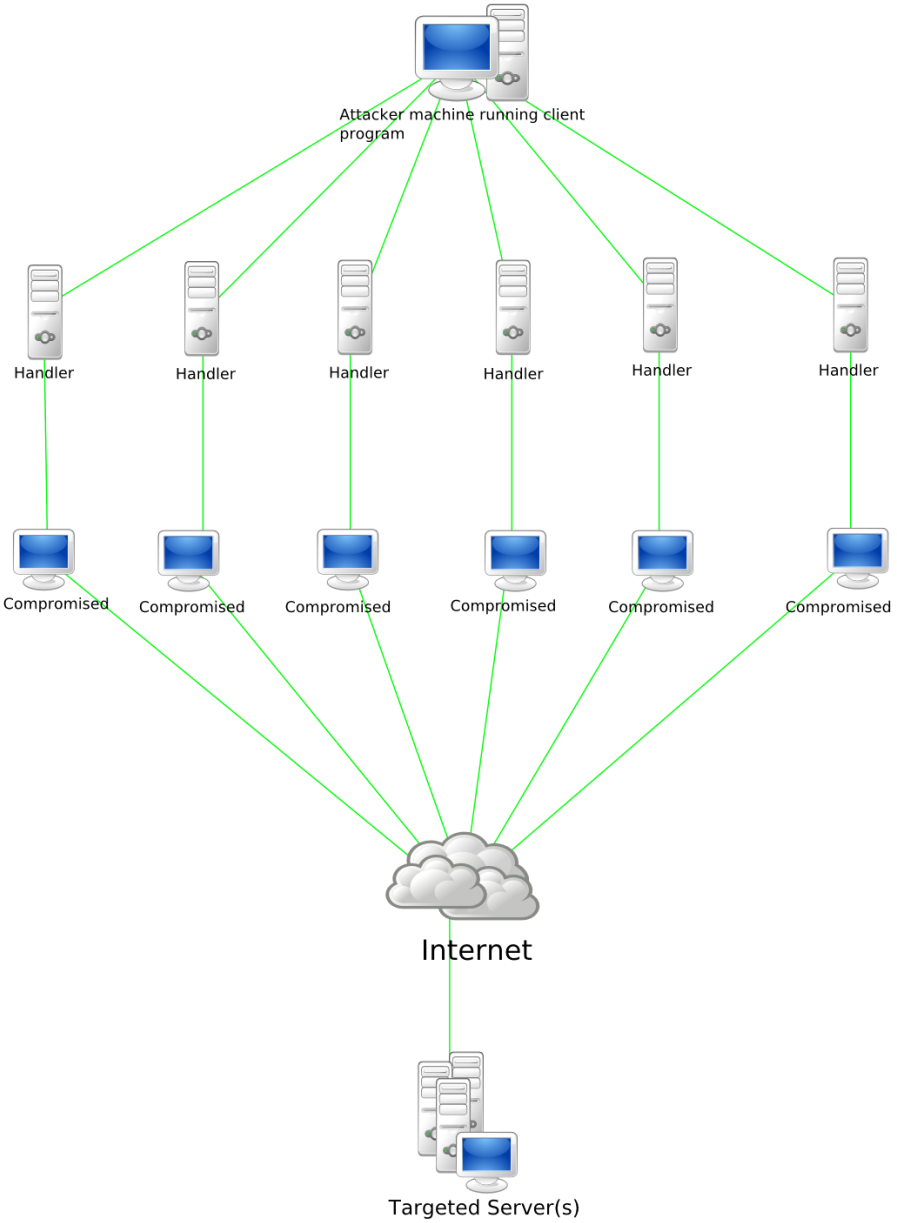
3. With too much access, the server stops

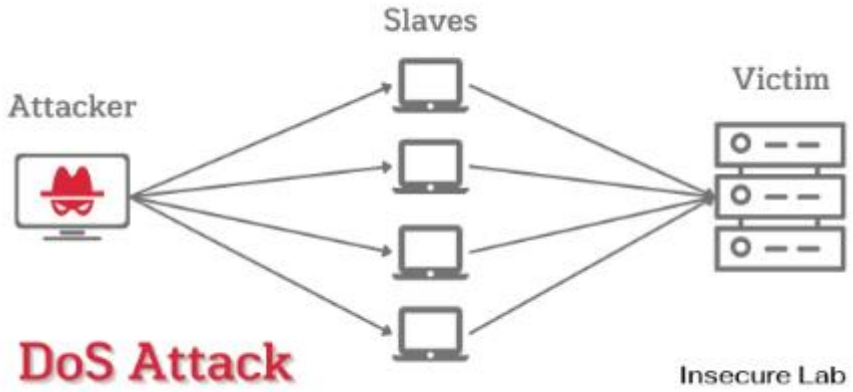


Buffer overflow attacks

- Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.
- A buffer overflow attack works when an attacker manipulates coding errors to overwrite computing memory. They can then carry out malicious actions like stealing data and compromising systems.

Denial of Service (DoS) attack

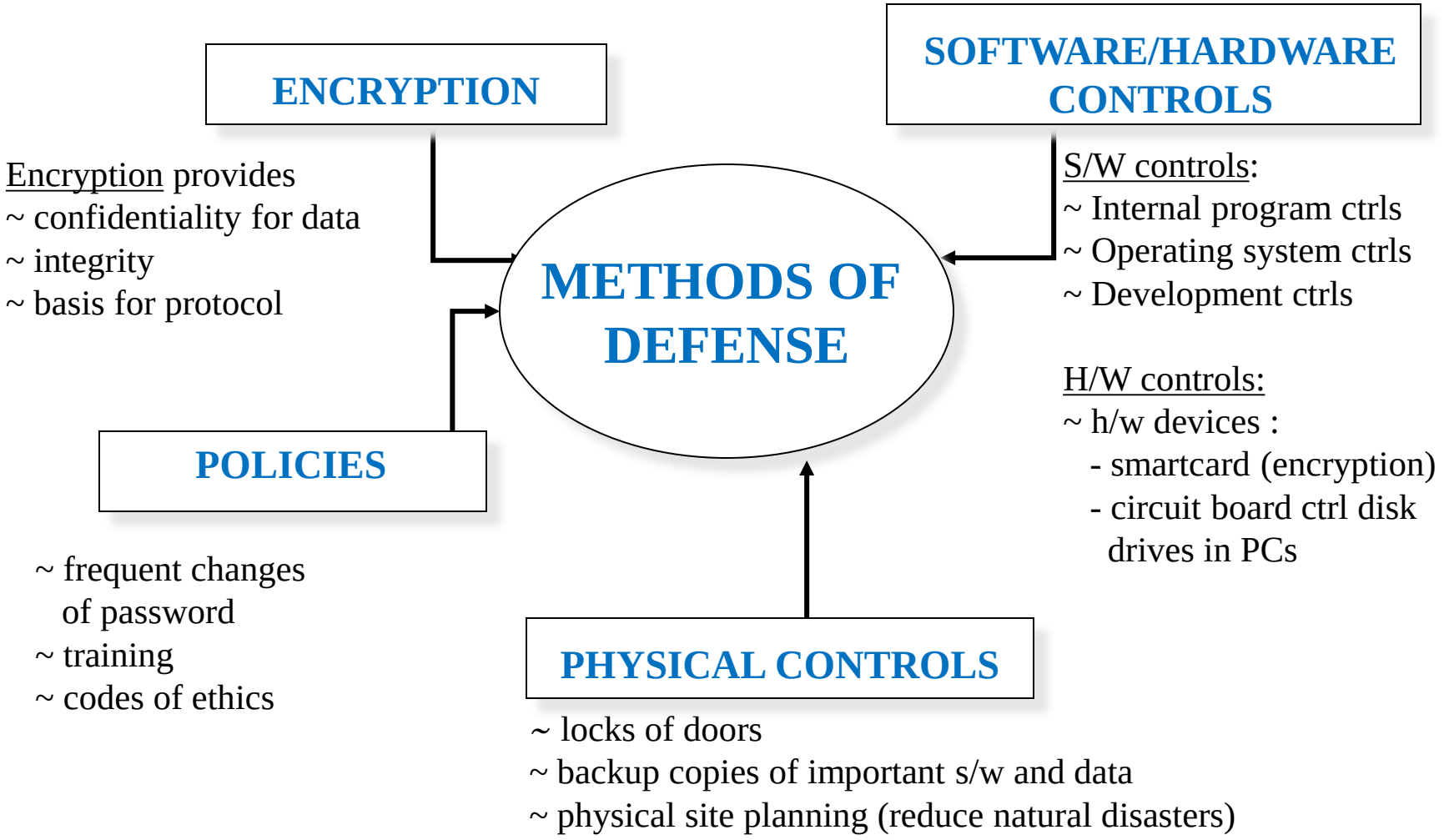




C.3. Controls

- Definition: an action, device, procedure, or technique that remove or reduce a vulnerabilities
- Harm occurs when a threat is realized against a vulnerability. To protect against harm, we can neutralize the threat, close the vulnerability, or both
- The possibility for harm to occur is called risk

C.3. Controls: Methods of Defense



C.3. Controls:
What makes a system secure?

1. System Access Control: Ensuring that unauthorized users don't get into the system.
2. Data Access Controls: Monitoring who can access what data, and for what purpose.
3. System and Security Administration: Performing the offline procedures that make or break a secure system
   ~ by clearly stated system administrator responsibilities,
   ~ by training users appropriately etc.
4. System Design: Taking advantage of basic h/w and s/w security characteristics.

Review Questions

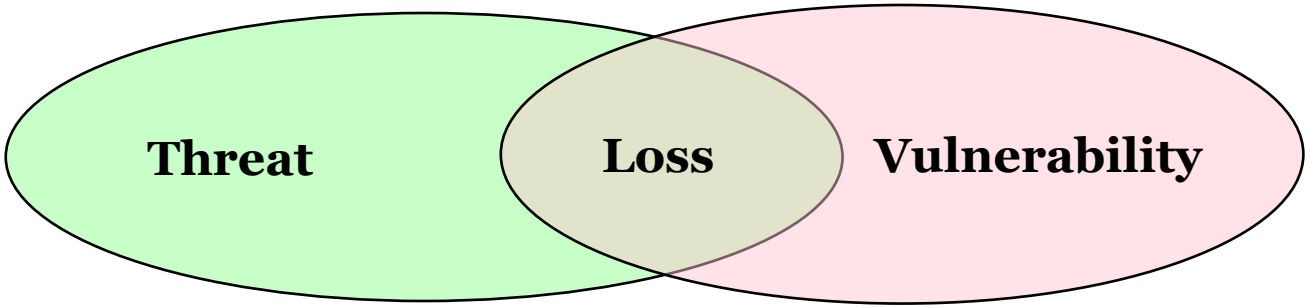
1. Define Threats, Vulnerabilities, Controls
2. What are the types of Threats?
3. What are the methods of defense from Threats
4. What questions should you ask when determining threats?
5. What is vulnerability threat and control?

D. Risk Management

- "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization." CISA Review Manual 2006

D.1. Risk Analysis

Relationship between threat, vulnerability, and loss



(threat)	**+**	**(vulnerability)**	**= (loss)**
computer virus	+	no anti-virus software installed	= data destruction

Risk: a possibility that a threat exploits a vulnerability in an asset and causes damage or loss to the asset.

D.1. Risk Analysis

- The figure explains the relation between threat, vulnerability and loss. A loss occurs when there is a threat and vulnerability. Threat and vulnerability alone does not result in a loss.

- For example, if a house has door that is unlocked, that door can be perceived as a vulnerability. But if that house is in a country where there are no security crimes (no thieves), that vulnerability does not result in a loss. In case of computers, presence of a computer virus (threat) may result in data destruction (loss), if no anti-virus software is installed (vulnerability).

D.1. Risk Analysis

- What may happen if you omit the analysis?
  - Cannot detect vulnerabilities.
  - Introduce countermeasures without specific reason.
  - Remake the whole system.
  - Take huge cost and time.
- Risk analysis leads you to ….
  - Identify threats to your system.
  - Estimate damages and possibility of occurrence.
  - Develop countermeasures to minimize threats.

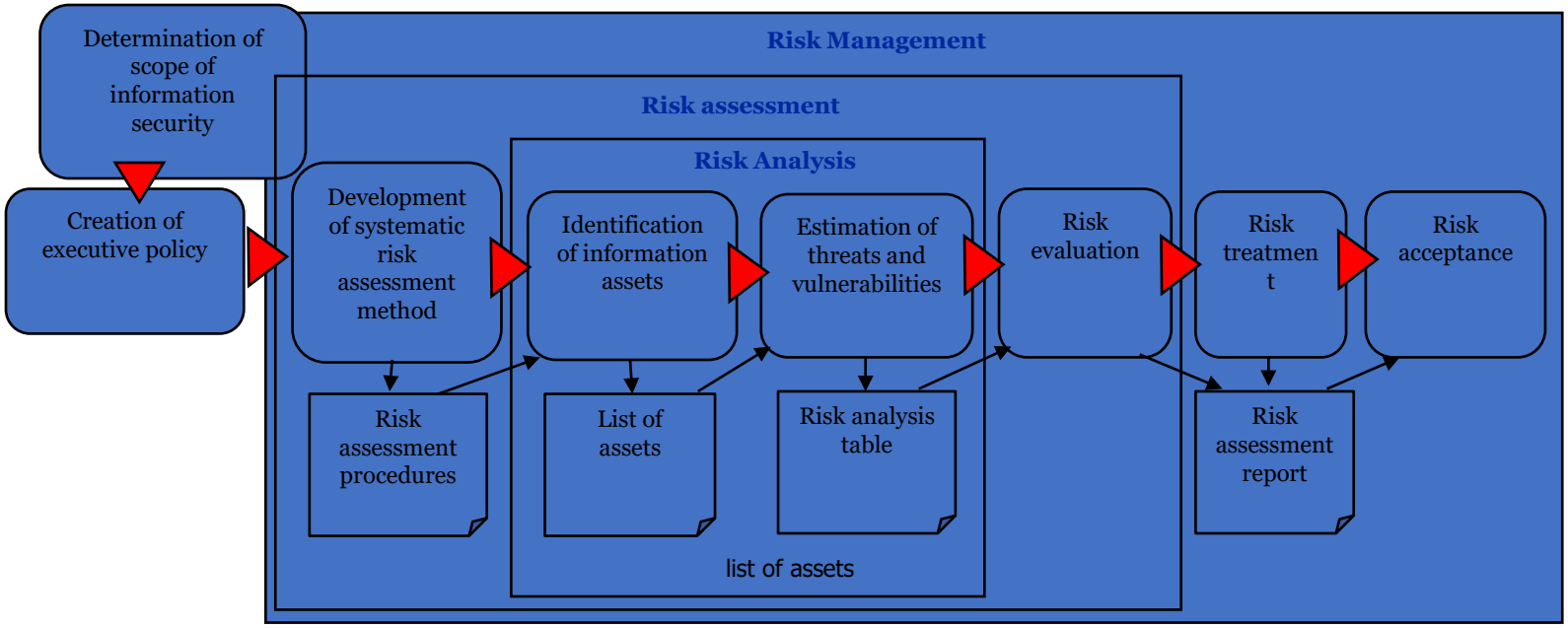
D.1. Risk Analysis

- Risk analysis is a time and cost consuming task. Adding to the fact that risk analysis does not directly lead to profit, some may choose to skip the analysis. However, there is also a risk in skipping the analysis. By not conducting the analysis, the organization might overlook the vulnerabilities in the system (many security holes may go unnoticed), introduce countermeasures without a specific reason (install firewall without any consideration), remake the whole system (because the overall security level was too low), and spend huge cost and time (to reinvest for countermeasures against overlooked vulnerabilities).

- One the other hand, risk analysis leads you to identify threats to your system (know who, when, why, and what would be the threat, and how to protect against them), estimate damages and possibility of occurrence of threats (be able to decide which risk should be reduced, removed, transferred, and retained), and develop appropriate countermeasures to minimize threats (be able to apply countermeasures with minimum cost).

D.2. Procedures

Risk analysis: Estimation of threats and vulnerabilities of information assets.
Risk assessment: Overall process of risk analysis and risk evaluation.
Risk management: Process of identifying, controlling, and minimizing or eliminating security risks that may affect information systems.



D.3. Executive Management

- Executive Management can choose to:
  - "Accept the risk"?
    - do nothing !

    based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business
  - "Mitigate the risk"?
    - Administrative Control
    - Logical Control
    - Physical Control

    by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be **transferred** to another business by buying insurance
  - "Deny the risk"?
    - Confidentiality
    - Integrity
    - Authenticity

Real Story

- **Government's Computer Security Report Card**

The U.S. Congress requires to supply annual reports to the Office of Management and Budget (OMB) on the state of computer security in the agencies. The agencies must report efforts to protect their computer networks against crackers, terrorists, and other attackers. In November 2001, two-thirds of the government agencies received a grade of F (the lowest possible) on the computer security report card based on the OMB data. The good news is that in 2005 only 8 of 24 agencies received grades of F and 7 agencies received a grade of A. The bad, and certainly sad, news is that the average grade was D+. Also disturbing is that the grades of 7 agencies fell from 2004 to 2005. Among the failing agencies were Defense, State, Homeland Security, and Veterans Affairs. The Treasury Department received a D-. A grades went to Labor, Social Security Administration, and the National Science Foundation, among others. (Source: U.S. House of Representatives Government Reform Committee.)111

Terms and Concepts

- Integrity
- Availability
- Risk
- Risk Management
- Risk Assessment
- Risk Analysis
- Information Assets
- Authorized
- Malware

Terms and Concepts

- Malicious
- Cybercrime
- Threats
- Vulnerabilities
- Control
- Confidentiality

Security Policies

- A security policy is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within the organization.
- A well designed policy addresses:
- What is being secured? - Typically an asset.
- Who is expected to comply with the policy? - Typically employees.
- Where is the vulnerability, threat or risk? Typically an issue of integrity or responsibility.

Types of Security Policies

- **Organizational**
  - Management establishes how a security program will be set up, lays out the program's goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out.
- **Issue-specific**
  - Addresses specific security issues that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply with these security issues
  - E.g.: An e-mail policy might state that management can read any employee's e-mail messages that reside on the mail server, but not when they reside on the user's workstation
- **System-specific**
  - Presents the management's decisions that are specific to the actual computers, networks, applications, and data.
  - This type of policy may provide an approved software list, which contains a list of applications that may be installed on individual workstations.

Standards

- Standards refer to mandatory activities, actions, rules, or regulations.
- Standards can give a policy its support and reinforcement in direction.
- Standards could be internal, or externally mandated (government laws and regulations)

Review Questions

1. One control against accidental software deletion is to save all old versions of a program. Of course, this control is prohibitively expensive in terms of cost of storage. Suggest a less costly control against accidental software deletion. Is your control effective against all possible causes of software deletion? If not, what threats does it not cover?

2. Suppose a program to print paychecks secretly leaks a list of names of employees earning more than a certain amount each month. What controls could be instituted to limit the vulnerability of this leakage?

3. Consider a program that allows a surgeon in one city to assist in an operation on a patient in another city via an Internet connection. Who might want to attack the program? What types of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?