
DENNIS GUNAWAN



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

IF470 COMPUTER SECURITY

01 INTRODUCTION TO COMPUTER SECURITY



COURSE SUB LEARNING OUTCOMES (SUB-CLO)

- Sub-CLO I
 - Students are able to relate threat-vulnerability-countermeasure paradigm and security properties to real case in their daily life (C3)

OUTLINE

- How Dependent Are We on Computers?
- What Is Computer Security?
- Threats
- Harm
- Vulnerabilities
- Controls

IMAGINE, ON A SINGLE DAY...

First, 20 million U.S. smart phones stop working. Next follow outages in wireline telephone service, problems with air traffic control, disruptions to the New York Stock Exchange, and eventually severe loss of power on America's East Coast.

- Isolated events, just coincidentally occurring on the same day?
- Dependencies in one sector trigger actions that cause the initial failure to cascade into other sectors?

INTRODUCTION

- It is difficult – sometimes impossible – to distinguish between an accident and an attack

An online gambling site that received a flood of blank incoming email messages that overwhelmed servers and slowed customer traffic to a crawl. Blank messages could easily come from a software or hardware problem: a mail handler caught in a loop with one malformed message that it dispatches over and over. Shortly thereafter, the company received email written in broken English. It told the company to wire \$40,000 to ten different accounts in Eastern Europe if it wanted its computers to stay online.

INTRODUCTION

Are cyber security exercises designed to
CONFIRM OUR READINESS
or
EXACERBATE OUR WORRIES
?

INTRODUCTION

You are using your mobile phone to talk with your friend, and the connection drops. You redial repeatedly but never connect. You then try to call your friend on your land line, but again there is no connection.

- How long does it take you to realize that the problem affects far more people than just you and your friend?
- Do you contact the telephone company? (And how? You cannot phone, and your Internet connection may very well depend on your telephone carrier!)
- By the time the power goes out, how do you know the power failure is related to your phone problems?
- When do you take any action? And what do you do?

INTRODUCTION

You are using your mobile phone to call your stockbroker because your company's initial public offering (IPO) is scheduled for today – so your company's viability depends on the resulting stock price and the volume of sales. As you begin your conversation with the stockbroker, the connection drops. You redial repeatedly, but never connect. You then try to call your broker on the land line, but again there is no connection.

- How long does it take you realize that the problem affects your company? Your broker? Others?
- Whom do you call to report a problem?
- And when the power goes out, what action do you take?

INTRODUCTION

You are a government official involved with air traffic control. All morning, you have heard rumors of telephone problems around the country. On your secure government line, you get a call confirming those problems and reporting widening problems with the air traffic control system.

- How do you determine what is wrong?
- To whom do you report problems?
- When you realize that problems with air traffic control may be dangerous to aircraft and their passengers, how do you react?
- Can you ground all aircraft until the sources of the problems are located and corrected?

INTRODUCTION

You are a government official involved with regulating the power grid. All morning, you have heard rumors of telephone problems around the country. Your web-based reporting system begins to report sporadic power outages on the East Coast. On your secure government line, you get a call confirming those problems and reporting widening problems with the air traffic control system.

- How do you determine what is wrong?
- To whom do you report problems?
- When you realize that problems with the power grid may threaten the viability of the entire nation's power system, how do you react?
- The power grid is owned by the private sector. Does the government have authority to shut down the grid until the sources of the problems are located and corrected?

INTRODUCTION

World War I

- The U.S. government took over the railroads and the telephone-telegraph system by presidential proclamations

World War II

- The U.S. government encouraged the automotive industry to redirect production toward jeeps, trucks, and airplane parts



INTRODUCTION

- Possible reactions
 - Inaction
 - Private sector coordination
 - Government intervention
- How do you determine cause and effect, severity of impact, and over what time period?
 - The answers are important in suggesting appropriate actions

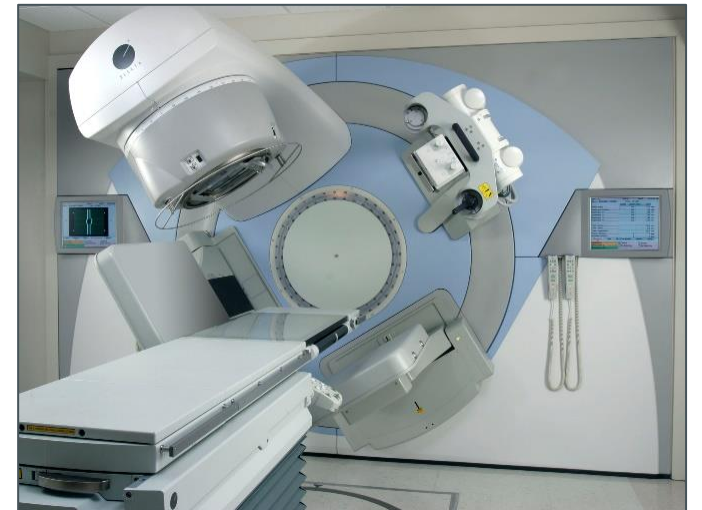
HOW DEPENDENT ARE WE ON COMPUTERS?

- You drive down the road and suddenly your car brakes to a stop or accelerates uncontrollably
- You try to withdraw money from your bank and find that your account is overdrawn, even though you think it should contain plenty of money
- Your doctor phones to tell you a recent test showed that your usually normal vitamin D level is a fraction of what it should be
- Your favorite candidate loses an election that should have been a sure victory

Should you be worried?

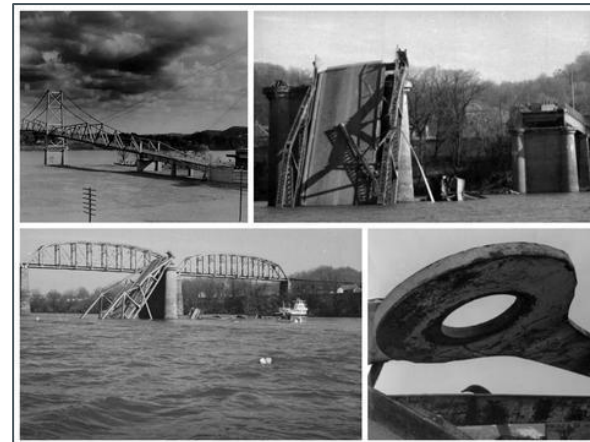
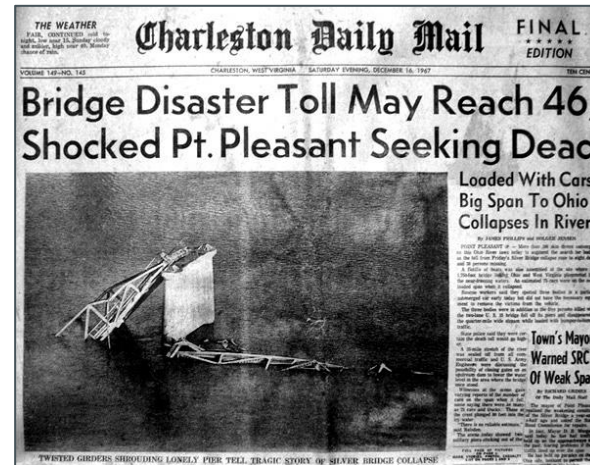
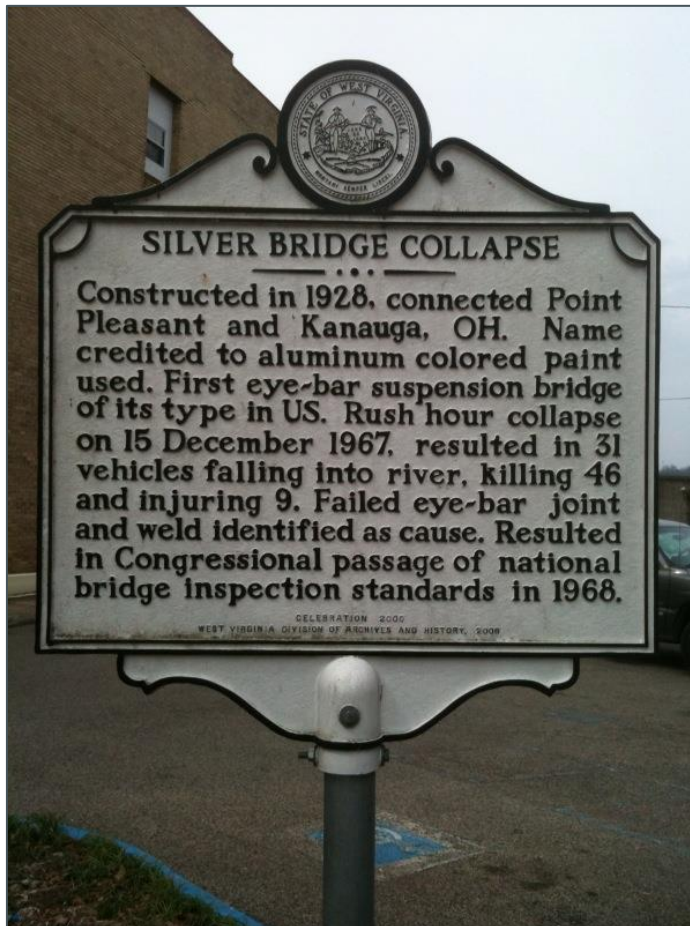
There may be other explanations for these events, but any of them may be the result of a **computer security** problem

HOW DEPENDENT ARE WE ON COMPUTERS?



- Can we – and should we – depend on computers to perform these tasks?
- How much can we entrust to them, and how will we determine their dependability, safety, and security?

HOW DEPENDENT ARE WE ON COMPUTERS?



- Some bridge component has been made of defective materials
- Design plans were not followed
- The bridge has been subjected to more strain than was anticipated

HOW DEPENDENT ARE WE ON COMPUTERS?

- Engineers are trained to deal with and learn from past failures
 - Well qualified to build large structures on which many of us depend
- Not all engineers appreciate the differences or implement software appropriately to address a wide variety of security risks

HOW DEPENDENT ARE WE ON COMPUTERS?

Failures

- Benign users
 - Small and harmless
 - A “click here” button that does nothing
 - The effects can be readily apparent
 - A screen goes blank
- Malicious attackers
 - Catastrophic
 - A faulty program that destroys a file or even erases an entire disk
 - Stealthy and difficult to find
 - A program that covertly records every key pressed on the keyboard

HOW DEPENDENT ARE WE ON COMPUTERS?

Computer security

addresses all these types of failures,
including the ones we cannot yet see or even anticipate

WHAT IS COMPUTER SECURITY?

- Computer security is the protection of the items you value, called the **assets** of a computer or computer system
 - Hardware
 - Software
 - Data
 - People
 - Processes
 - Access to data
 - Quality of service
 - Network connectivity

WHAT IS COMPUTER SECURITY?

- The thing that makes your computer unique and important to you is your content
 - Photos
 - Tunes
 - Papers
 - Email messages
 - Projects
 - Calendar information
 - E-books (with your annotations)
 - Contact information
 - Code you created

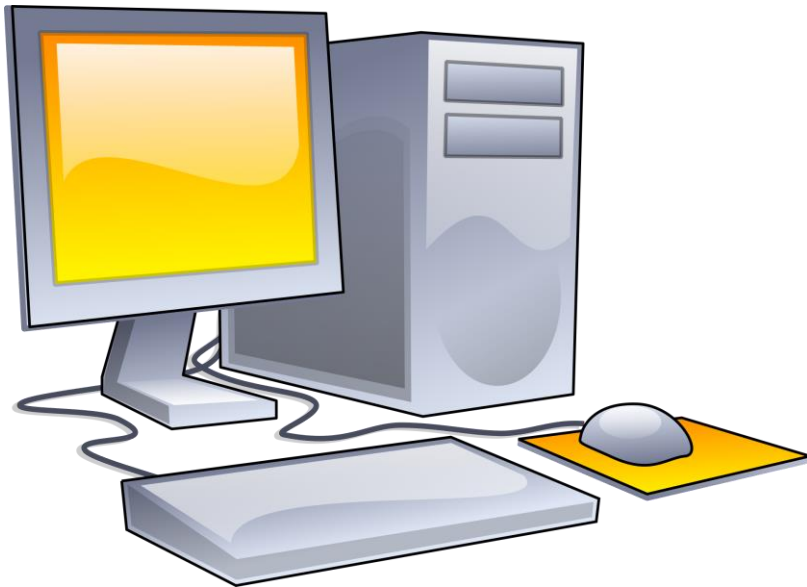
The design for your next new product

The photos from your recent vacation

The chapters of your new book

- All of these things represent intellectual endeavor or property
- They have value that differs from one person or organization to another

WHAT IS COMPUTER SECURITY?



Hardware


- Computer
- Devices
 - Disk drives
 - Memory
 - Printer
- Network gear

Software

- Operating system
- Utilities
 - Antivirus
- Commercial applications
 - Word processing
 - Photo editing
- Individual applications

Data

- Documents
- Photos
- Music
- Videos
- Email
- Class projects

 Off the shelf;
easily replaceable

 Unique;
irreplaceable

WHAT IS COMPUTER SECURITY?

When you go for a swim
you can leave a bottle of water on a towel on the beach,
but not your wallet or cell phone

WHAT IS COMPUTER SECURITY?

- The value of an asset depends on
 - The asset owner's or user's perspective, independent of monetary cost
 - Your photo of your sister, worth only a few cents in terms of paper and ink, may have high value to you and no value to your roommate
 - Replacement cost
 - The photo of you and your friends at a party may have cost you nothing, but it is invaluable because it can never be replaced
 - The DVD of your favorite film may have cost a significant portion of your take-home pay, but you can buy another one if the DVD is stolen or corrupted
 - Timing
 - The value of the plans for a company's new product line

THE VULNERABILITY – THREAT – CONTROL PARADIGM

- **VULNERABILITY**

- A weakness in the system that might be exploited to cause loss or harm

- **THREAT**

- A set of circumstances that has the potential to cause loss or harm

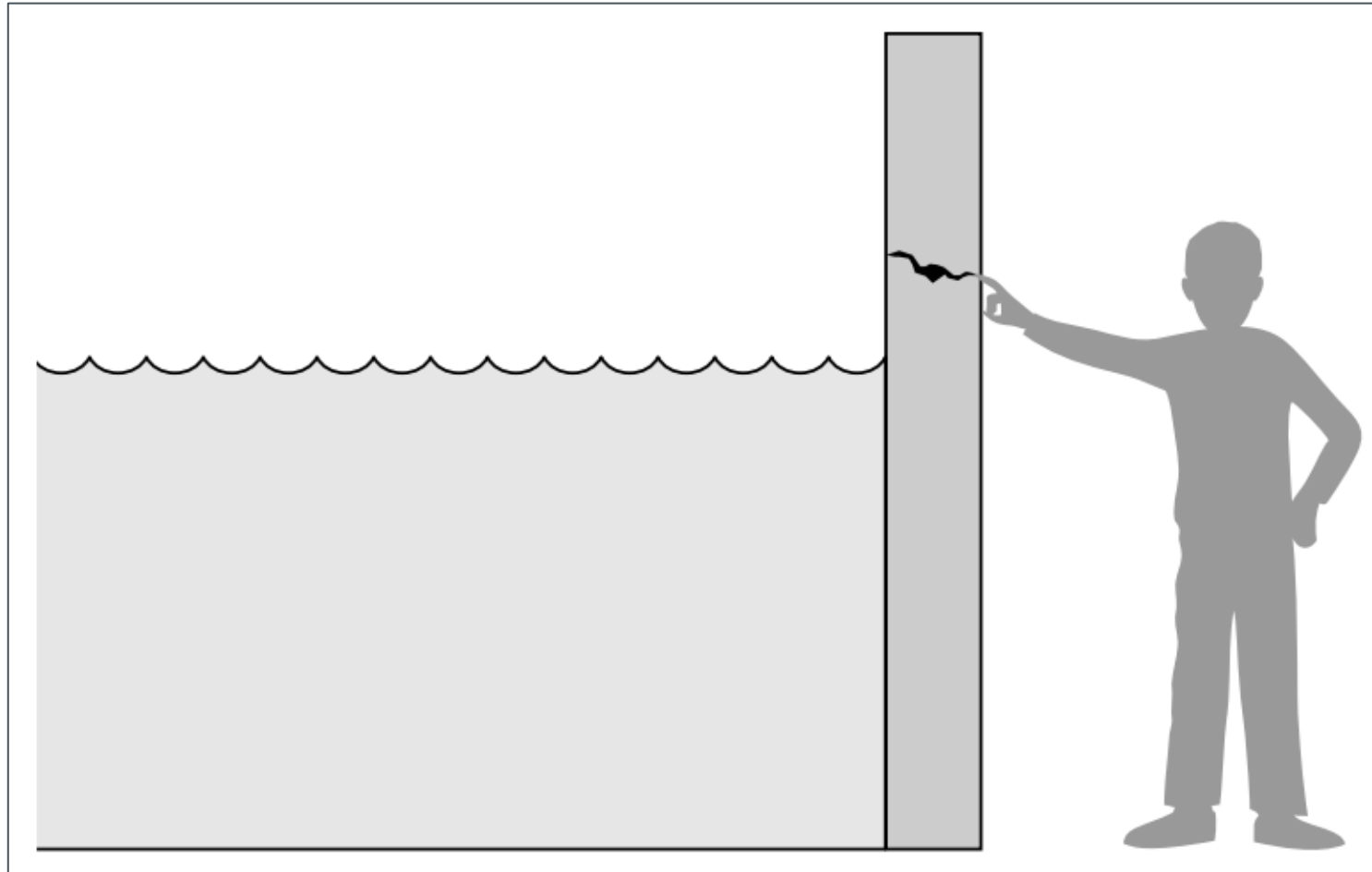
- **CONTROL** or **COUNTERMEASURE**

- An action, device, procedure, or technique that removes or reduces a vulnerability

Relationship among
threats, controls, and vulnerabilities

A **threat** is blocked by
control of a **vulnerability**

THE VULNERABILITY – THREAT – CONTROL PARADIGM



THE VULNERABILITY – THREAT – CONTROL PARADIGM

A human who exploits a vulnerability
perpetrates an **attack** on the system

SECURITY PROPERTIES

- What makes your computer valuable to you: C-I-A Triad or security triad
 - **CONFIDENTIALITY**
 - The ability of a system to ensure that an asset is viewed only by authorized parties
 - **INTEGRITY**
 - The ability of a system to ensure that an asset is modified only by authorized parties
 - **AVAILABILITY**
 - The ability of a system to ensure that an asset can be used by any authorized parties
- These characteristics are both basic security properties and the objects of security threats

SECURITY PROPERTIES

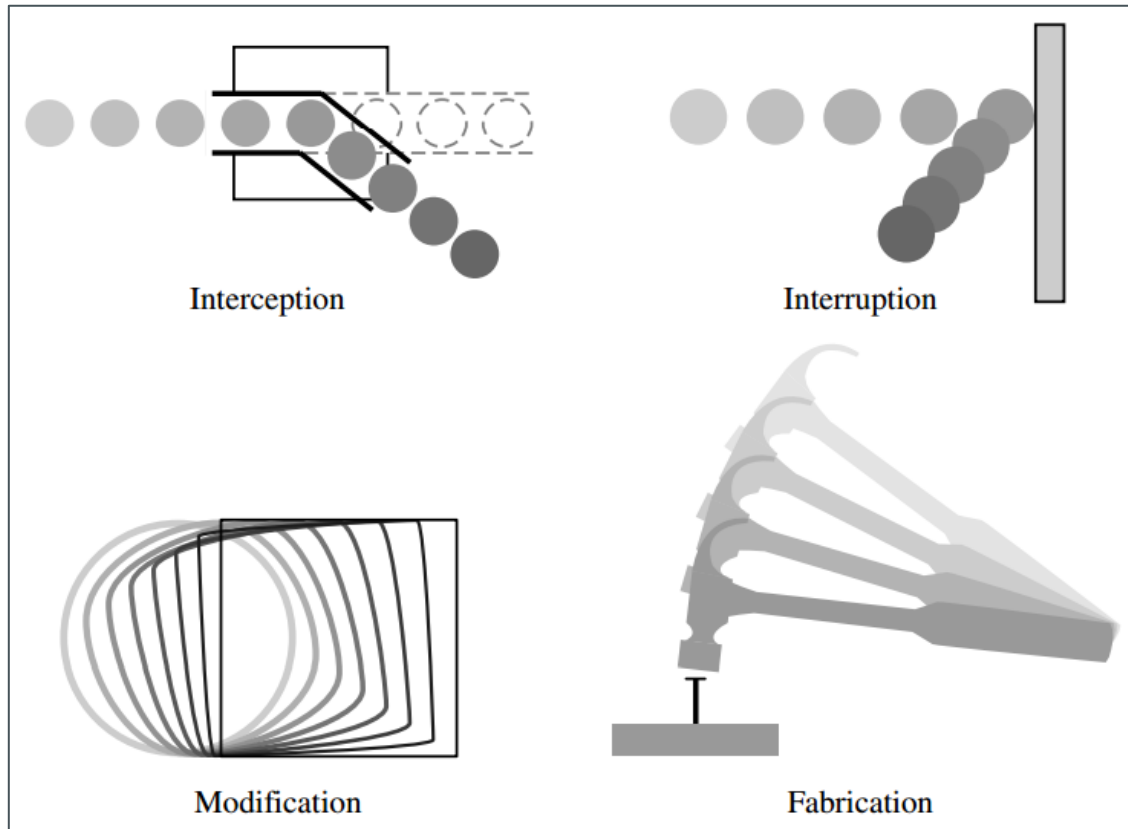
- ISO 7498-2 adds to them 2 more properties that are desirable, particularly in communication networks
 - **AUTHENTICATION**
 - The ability of a system to **confirm the identity** of a sender
 - **NONREPUDIATION** or **ACCOUNTABILITY**
 - The ability of a system to confirm that a sender **cannot convincingly deny** having sent something
- The U.S. Department of Defense adds
 - **AUDITABILITY**
 - The ability of a system to **trace** all actions related to a given asset

THREATS

- If a thief steals your computer, you no longer have access
 - ~~AVAILABILITY~~
- If the thief looks at the pictures or documents you have stored
 - ~~CONFIDENTIALITY~~
- If the thief changes the content of your music files but then gives them back with your computer
 - ~~INTEGRITY~~

THREATS

- Harm can be characterized by 4 acts



- **Confidentiality** can suffer if someone **intercepts** data
- **Availability** is lost if someone or something **interrupts** a flow of data or access to a computer
- **Integrity** can fail if someone or something **modifies** data or **fabricates** false data

CONFIDENTIALITY

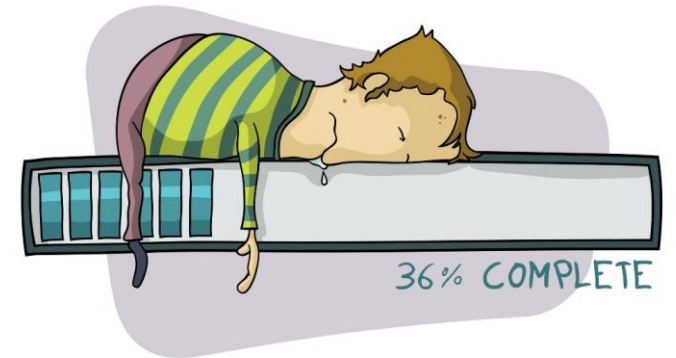
- Some things obviously need confidentiality protection
 - Students' grades
 - Financial transactions
 - Medical records
 - Tax returns
 - Diplomatic and military secrets
 - Companies' marketing and product development plans
- Sometimes, it is not so obvious that something is sensitive
 - Purchases of food
 - Hourly changes in location
 - Access to books

INTEGRITY

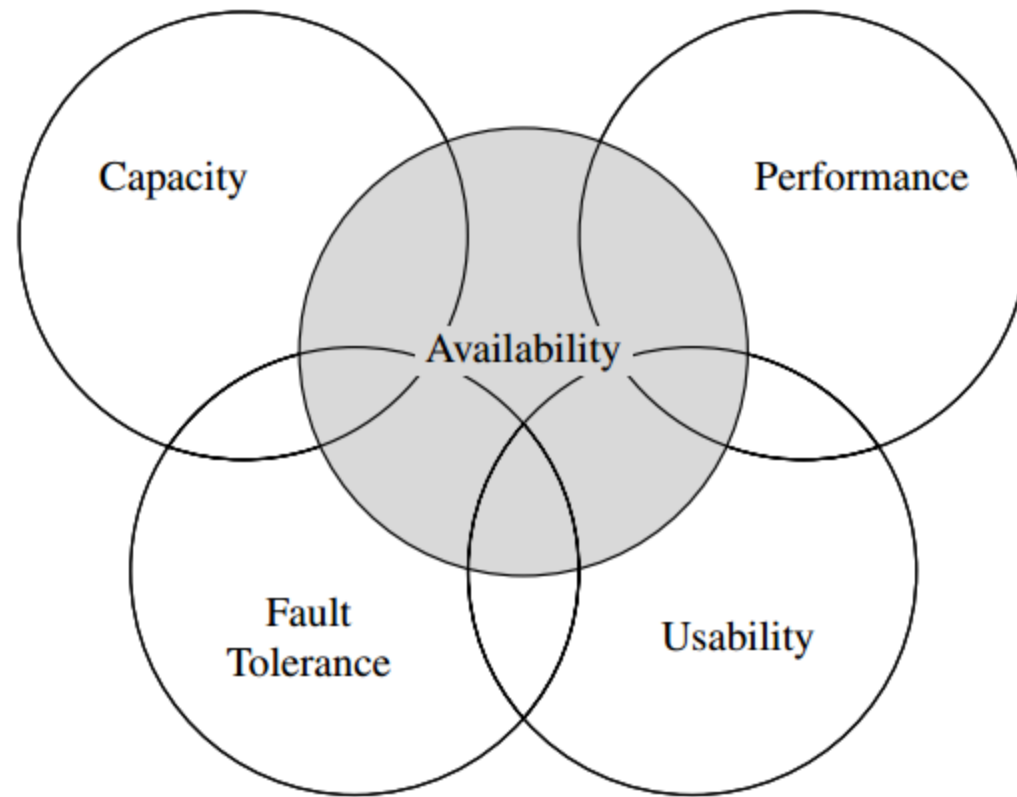
- A number of years ago a malicious macro in a Word document inserted the word “not” after some random instances of the word “is”
- A model of the Pentium computer chip produced an incorrect result in certain circumstances of floating-point arithmetic

AVAILABILITY

- A computer user's worst nightmare
 - You turn on the switch and the computer does nothing
 - Your data and programs are presumably still there, but you cannot get at them
- Many of us do experience overload
 - Access gets slower and slower
 - The computer responds but not in a way we consider normal or acceptable

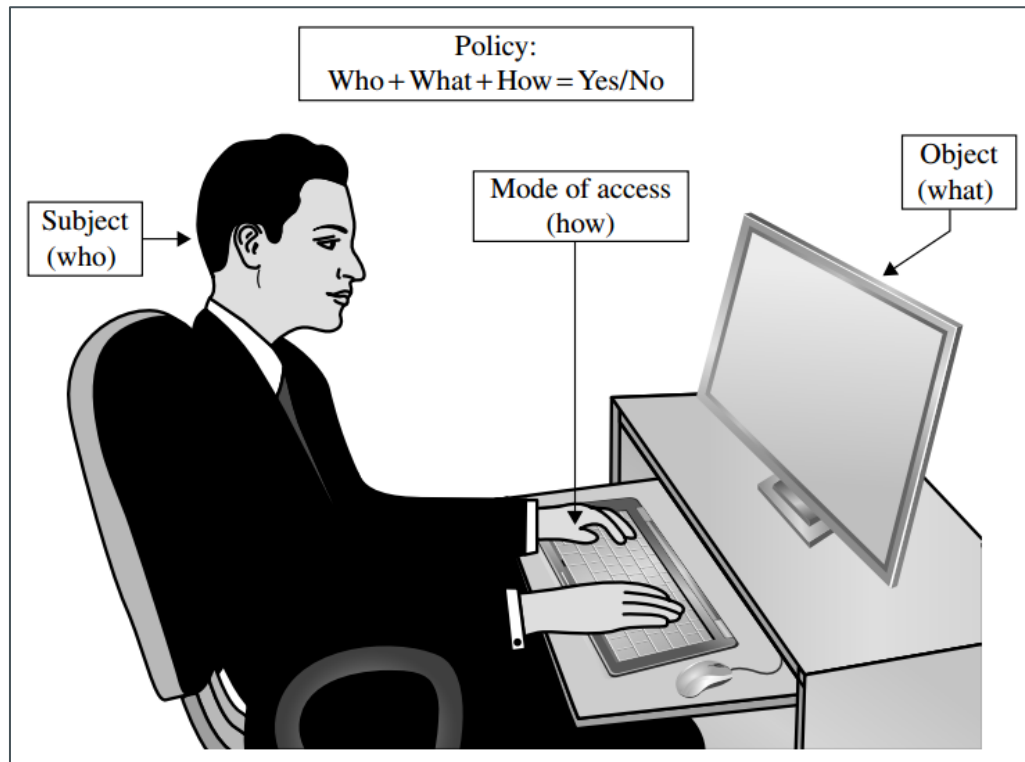


AVAILABILITY



ACCESS CONTROL

- A person, process, or program is (or is not) authorized to access a data item in a particular way

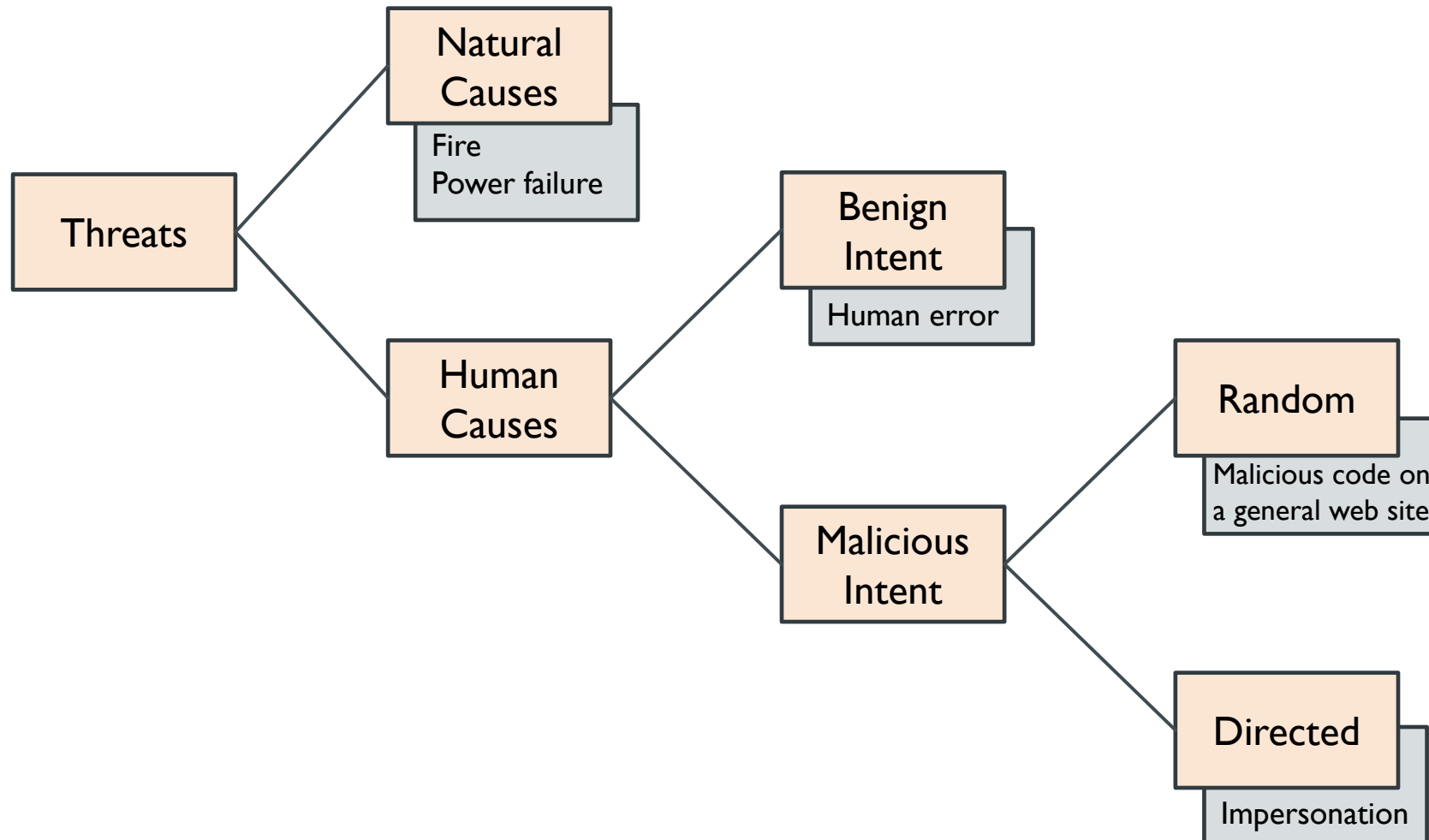


- **Subject**
 - Person, process, or program
- **Object**
 - Data item
- **Access mode**
 - The kind of access
- **Policy**
 - Authorization

ACCESS CONTROL

To implement a **policy**,
computer security controls all accesses
by **all subjects** to **all protected objects**
in **all modes of access**

TYPES OF THREATS



TYPES OF ATTACKERS

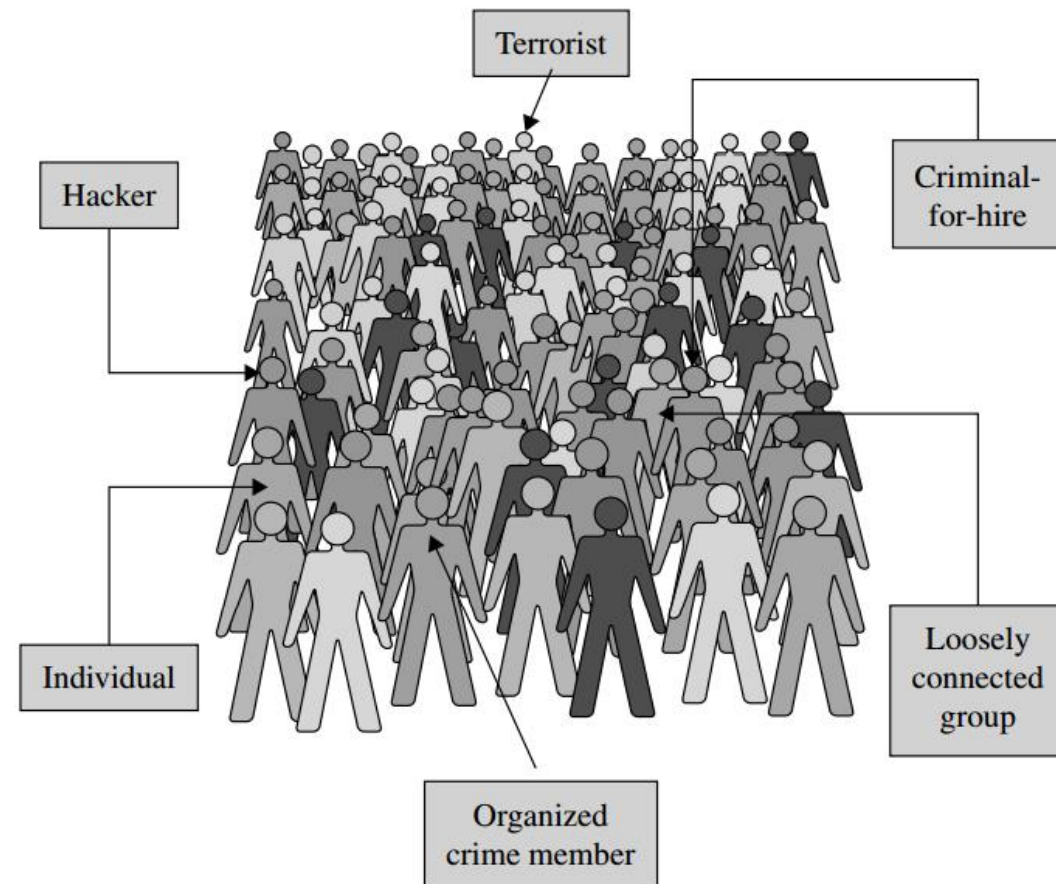
What does a cyber criminal look like?

TYPES OF ATTACKERS

- Mean and sinister types
- Wear business suits
- Have university degrees
- High school or university students
- Middle-aged business executives
- Mentally deranged
- Overtly hostile
- Ordinary people tempted by personal profit, revenge, challenge, advancement, or job security

No single profile captures
the characteristics of
a “typical” computer attacker

TYPES OF ATTACKERS



DARK WEB



- Credit card numbers, \$0.85 to \$30.00 each
- Bank account credentials, \$15 to \$850
- Email accounts, \$1 to \$20
- Lists of email addresses, \$1.70 to \$15.00 per thousand
- Web site administration credentials, \$2 to \$30

HARM

The negative consequence of
an actualized threat

- The causes of harm are limitless and largely unpredictable
- The possibility for harm to occur is called **risk**
- Because our resources are limited, we must prioritize our protection
- Choosing the threats we try to mitigate involves a process called **risk management**

RISK & COMMON SENSE

Simplistic Model of Risk Management

- Calculating the value of all assets
- Determining the amount of harm from all possible threats
- Computing the costs of protection
- Selecting safeguards (controls or countermeasures) based on the degree of risk and on limited resources
- Applying the safeguards to optimize harm averted

In Reality

- It is difficult to assess the value of each asset
- Even harder is determining the impact of all possible threats
- The range of possible threats is effectively limitless
- It is difficult (if not impossible in some situations) to know the short- and long-term impacts of an action

RISK & COMMON SENSE

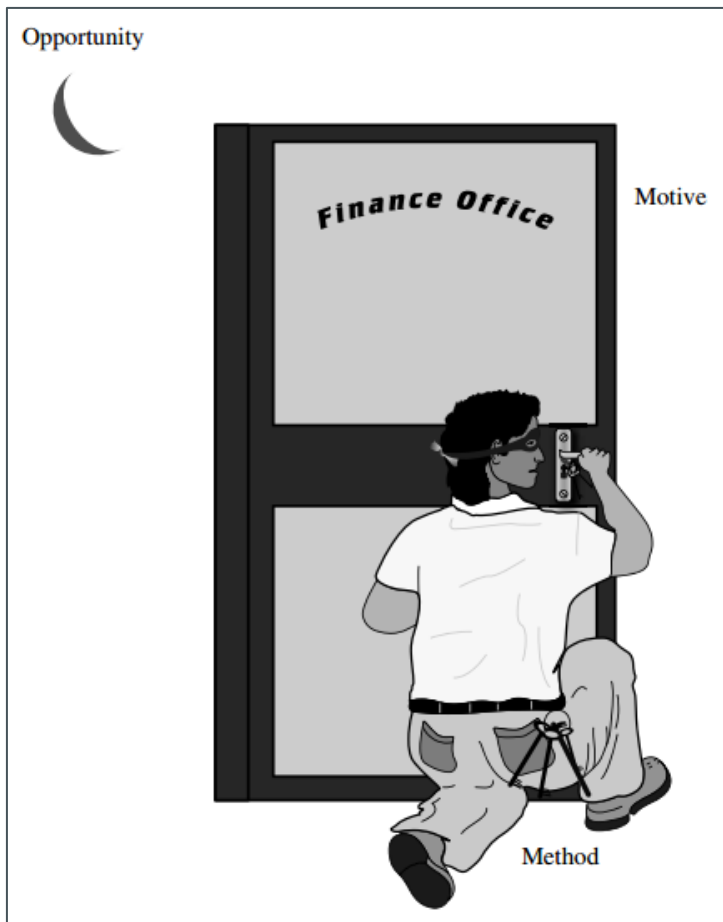
- We will necessarily protect against threats we consider **most likely** or **most damaging**
- We also consider how great is the threat's **likelihood**
- A **likely threat** is not just one that someone might want to pull off but rather **one that could actually occur**

RISK & COMMON SENSE

Some people might daydream about getting rich by robbing a bank; most, however, would reject that idea because of its difficulty (if not its immorality or risk)

- One aspect of likelihood is **feasibility**
 - Is it even possible to accomplish the attack?
 - If the answer is no, then the likelihood is zero, and therefore so is the risk
- 3 factors determine feasibility
 - **Method**
 - **Opportunity**
 - **Motive**

METHOD – OPPORTUNITY – MOTIVE



- A malicious attacker must have 3 things to ensure success
 - **Method**
 - The skills, knowledge, tools, and other things with which to perpetrate the attack
 - **Opportunity**
 - The time and access to execute an attack
 - **Motive**
 - An attacker must have a reason to want to attack

VULNERABILITIES

Think of a bank, with an armed guard at the front door, bulletproof glass protecting the tellers, and a heavy metal vault requiring multiple keys for entry

- To rob a bank, you would have to think of how to exploit a weakness not covered by these defenses
- You might bribe a teller or pose as a maintenance worker

VULNERABILITIES

- Weak authentication
- Lack of access control
- Errors in programs
- Finite or insufficient resources
- Inadequate physical protection

Paired with a credible attack,
each of these vulnerabilities can allow
**harm to confidentiality, integrity, or
availability**

2 RETROSPECTIVE LISTS OF KNOWN VULNERABILITIES

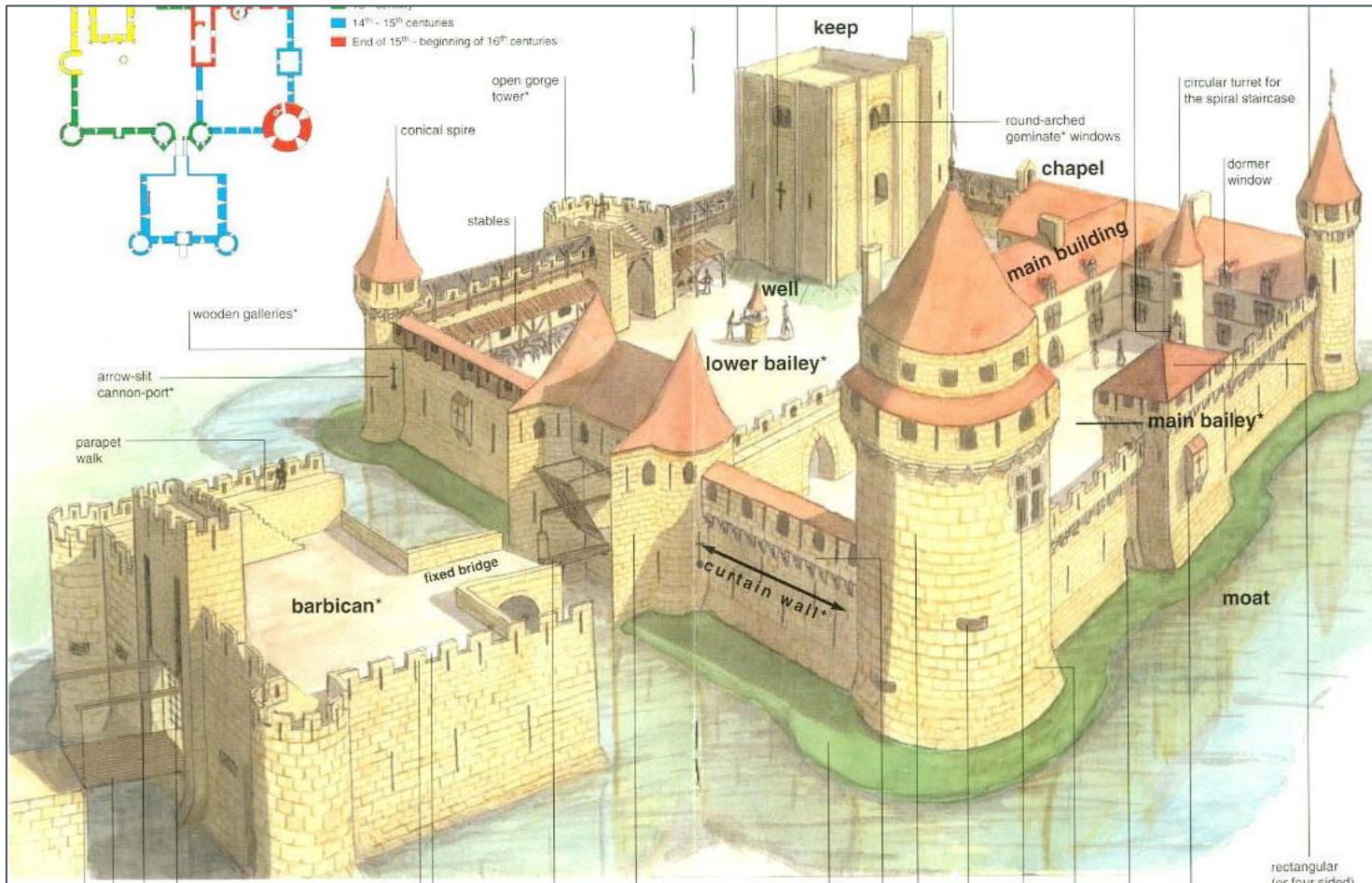
CVE

- Common Vulnerabilities and Exposures list
- <http://cve.mitre.org/>
- A dictionary of publicly known information security vulnerabilities and exposures

CVSS

- Common Vulnerability Scoring System
- <http://nvd.nist.gov/cvss.cfm>
- Provides a standard measurement system that allows accurate and consistent scoring of vulnerability impact

CONTROLS



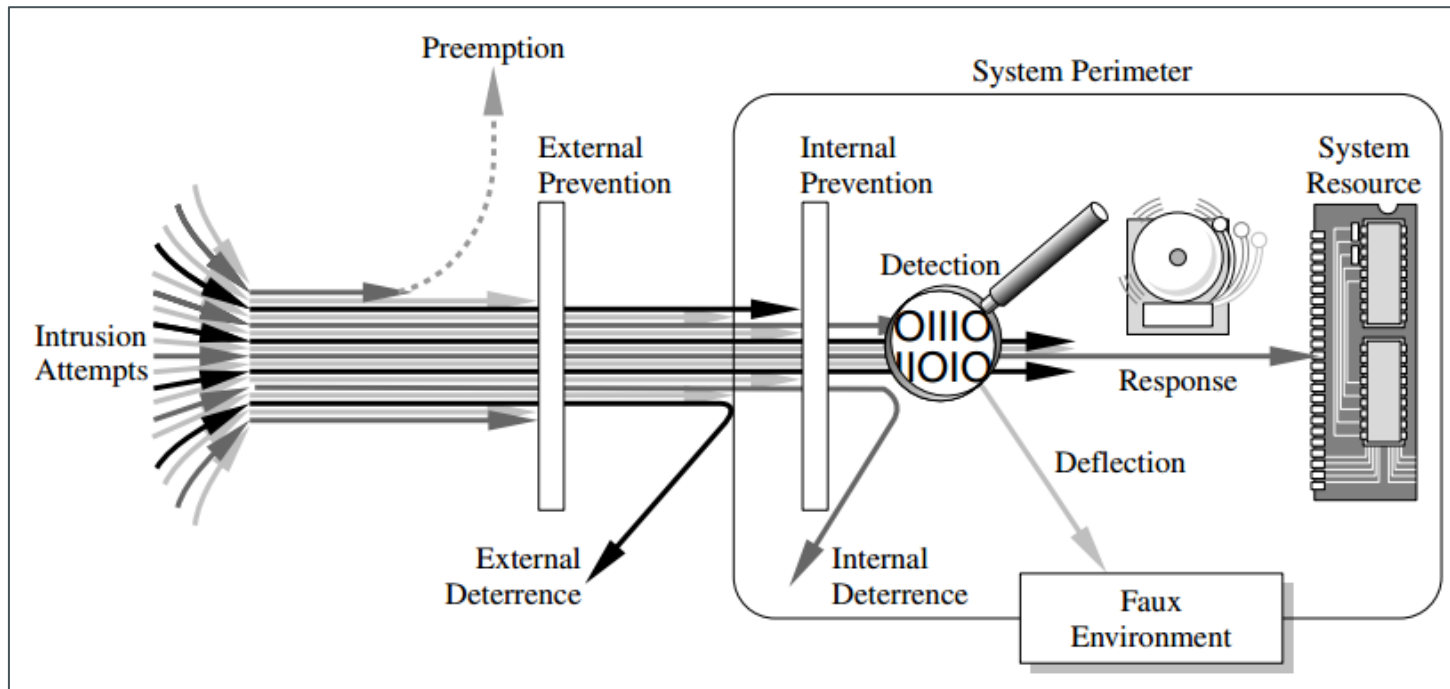
- Similarly, today we use a multipronged approach to protect out homes and offices
- We may combine strong locks on the doors with a burglar alarm, reinforced windows, and even a nosy neighbor to keep an eye on our valuables

CONTROLS

Dealing with Harm

- **Prevent**
 - Blocking the attack or closing the vulnerability
- **Deter**
 - Making the attack harder but not impossible
- **Deflect**
 - Making another target more attractive (or this one less so)
- **Mitigate**
 - Making its impact less severe
- **Detect**
 - Either as it happens or some time after the fact
- **Recover** from its effects

CONTROLS



We use one or more controls, according to what we are protecting, how the cost of protection compares with the risk of loss, and how hard we think intruders will work to get what they want

CONTROLS

Physical Controls

Stop or block an attack by using something tangible

- Walls and fences
- Locks
- (Human) Guards
- Sprinklers and other fire extinguishers

Procedural / Administrative Controls

Use a command or agreement that requires or advises people how to act

- Laws, regulations
- Policies, procedures, guidelines
- Copyrights, patents
- Contracts, agreements

Technical Controls

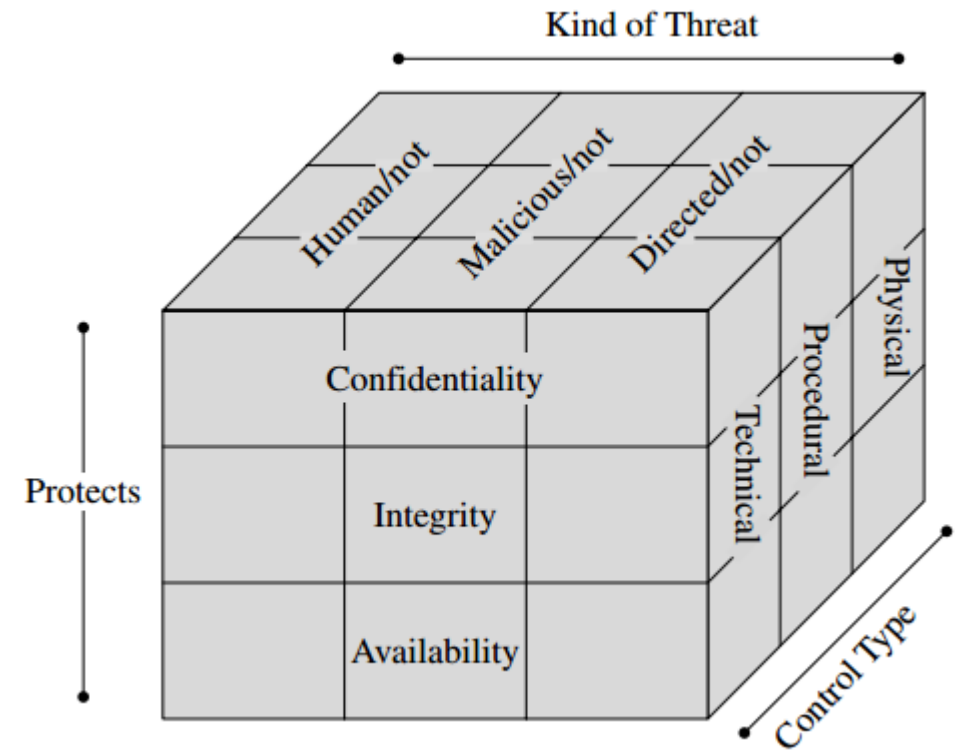
Counter threats with technology (hardware or software)

- Passwords
- Access controls enforced by an operating system or application
- Network protocols
- Firewalls, intrusion detection systems
- Encryption
- Network traffic flow regulators

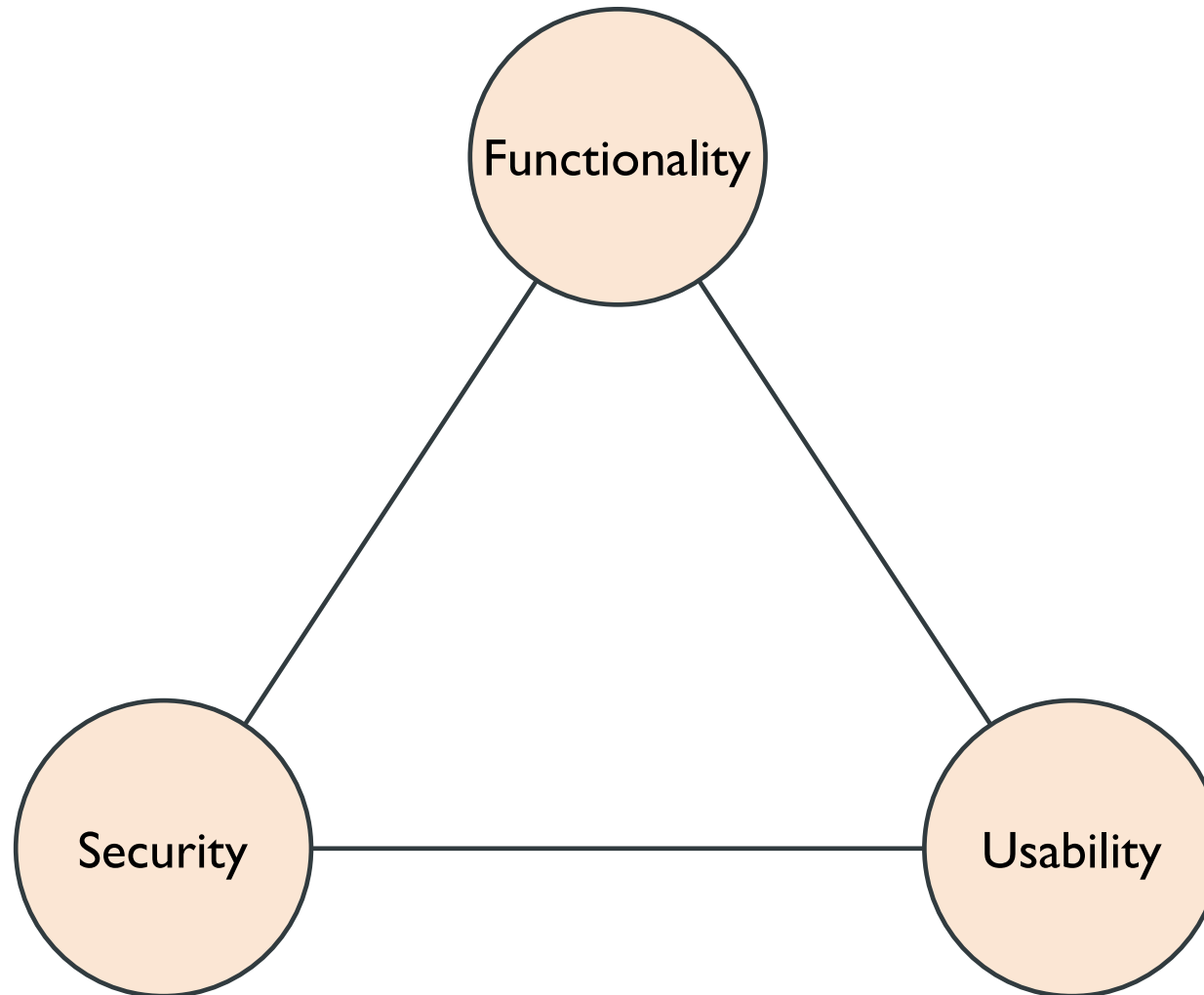
CONTROLS

Defense in depth

More than one control or
more than one class of control
to achieve protection



SECURITY, FUNCTIONALITY, & USABILITY TRIANGLE



REFERENCES

- Pfleeger, Charles P. and Shari Lawrence Pfleeger (2012), *Analyzing Computer Security*, 1st Edition, Prentice Hall.

NEXT WEEK: USER AUTHENTICATION

- Attack
 - Impersonation / Failed Authentication
- Vulnerability
 - Faulty or Incomplete Authentication
- Countermeasure
 - Strong Authentication



AS THE WORLD IS INCREASINGLY INTERCONNECTED,
EVERYONE SHARES THE RESPONSIBILITY OF
SECURING CYBERSPACE



Vision

To become an **outstanding** undergraduate Computer Science program that produces **international-minded** graduates who are **competent** in software engineering and have **entrepreneurial spirit** and **noble character**.



Mission

1. To conduct studies with the best technology and curriculum, supported by professional lecturer
2. To conduct research in Informatics to promote science and technology
3. To deliver science-and-technology-based society services to implement science and technology