COMP 4384 Software Security

Module 2: *Security Blanket or Security Theater*

Ahmed Tamrawi

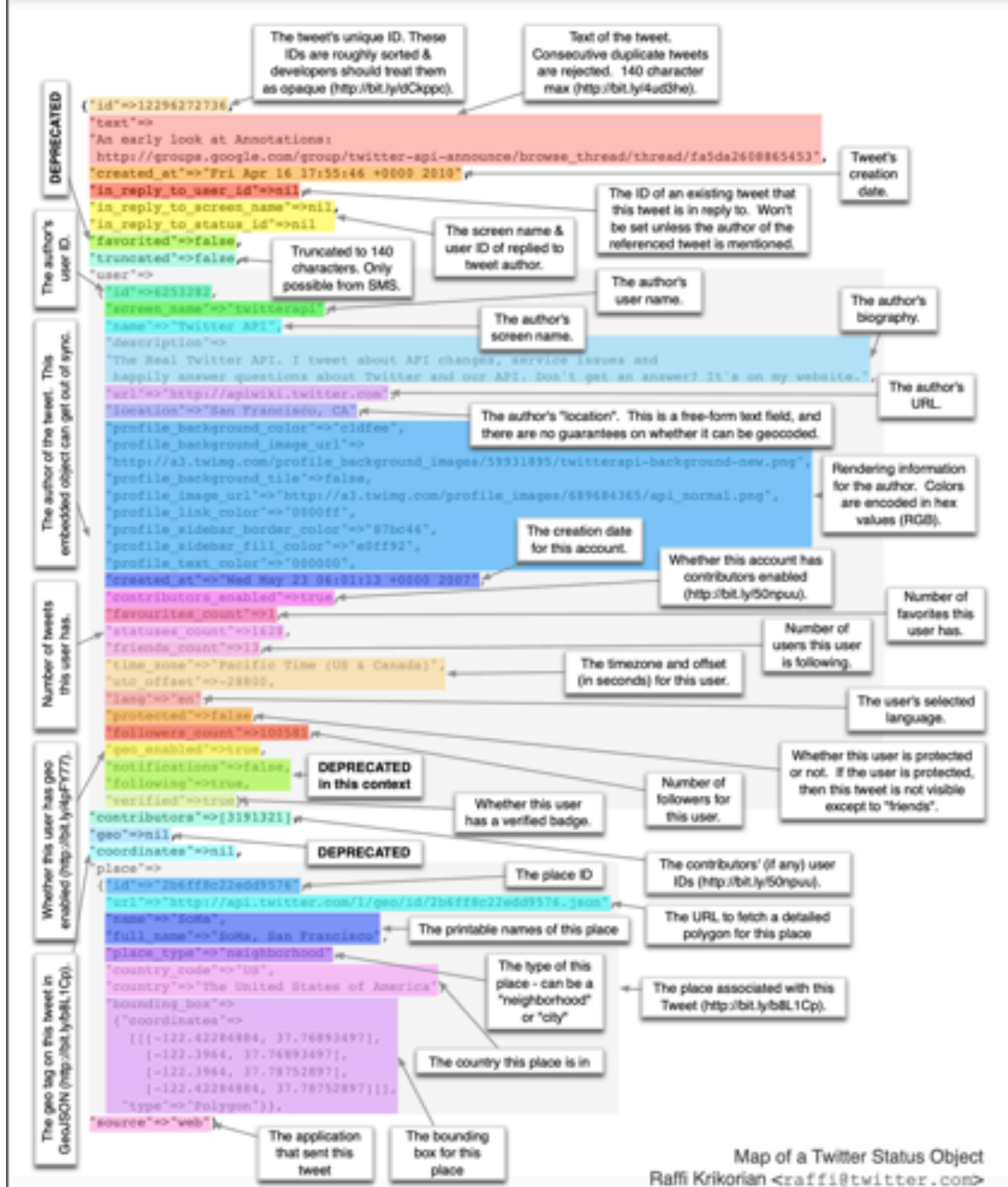
 atamrawi  atamrawi.github.io  ahmedtamrawi@gmail.com

```java
import java.util.Random;

public class Puzzle1 {

	public static void main(String[] args) {
		Random rnd = new Random();
		int odds = 0;
		int runs = 1000;
		for(int i=0; i<runs; i++) {
			int num = rnd.nextInt();
			if(isOdd(num)) {
				odds++;
			}
		}
		double oddPercentage = ((double) odds / (double) runs) * 100.0;
		System.out.println("Odd: " + String.format("%.2f", oddPercentage) + "%");
	}

	private static boolean isOdd(int num) {
		return num % 2 == 1;
	}

}
```

https://gist.github.com/atamrawi/3d279096091205ad02b0882d2382b221

Objectives

- Define **computer security** as well as basic computer security terms
- Introduce the **C-I-A Triad**
- Introduce **basic access control terminology**
- Explain basic **threats**, **vulnerabilities**, and **attacks**
- Show how controls map to threats



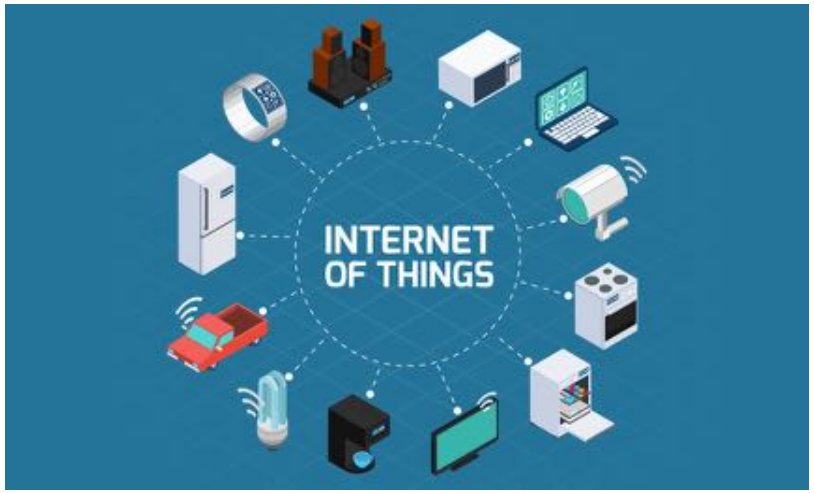
Map of a Twitter Status Object

Raffi Krikorian <raffi@twitter.com>

18 April 2010

What Is Computer Security?

- **Computer security** is the *protection* of the items you value, called the **assets** of a computer or computer system.
- There are many types of assets, involving *hardware*, *software*, *data*, *people*, *processes*, or combinations of these.



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

The Internet of Things (IoT)

- IoT refers to the **connection of everyday devices** to the Internet, making a world of so-called smart devices
- Examples:
  - Smart appliances, such as refrigerators and dishwashers
  - Smart home, such as thermostats and alarm systems
  - Smart health, such as fitness monitors and insulin pumps
  - Smart transportation, such as driverless cars
  - Smart entertainment, such as video recorders
- Potential downsides:
  - Loss of privacy and control of data
  - Potential for subversion
  - Mistaken identification
  - Uncontrolled access

Smartphones

- Smartphones are the control hub of the IoT.
- In 2013, Kaspersky Labs identified 143,211 distinct new forms of malware against mobile devices.
- 98% targeted Android devices, far in excess of its market share
  - Android, unlike its competitors, **does not limit** the software users can install and is thus an easier target
- Apple, in contrast, only allows **apps from its app store** to be installed on its smartphones
  - All apps go through an **approval** process, which includes some **security review.**
  - Once approved, apps are **signed**, using a **certificate approach**.

Values of Assets

Off the shelf;
easily replaceable

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

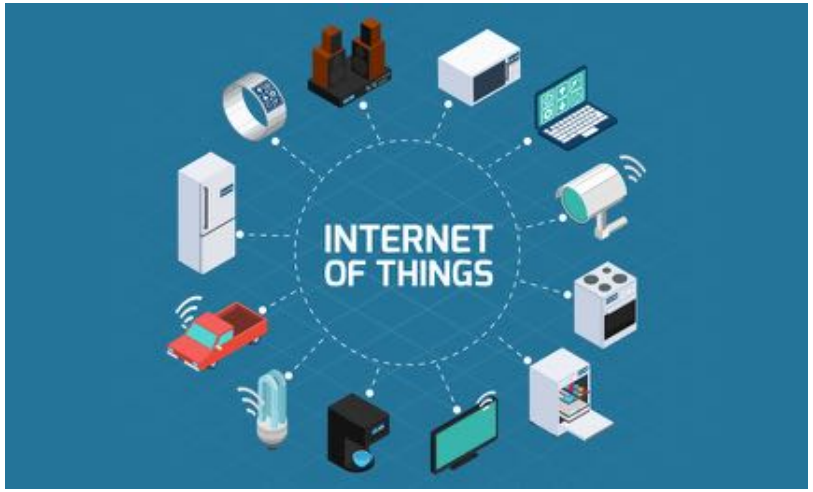
Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)

Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

- Individual applications

Unique; irreplaceable

mmh! Catastrophic?!



Disastrous?!

The Vulnerability–Threat–Control Paradigm

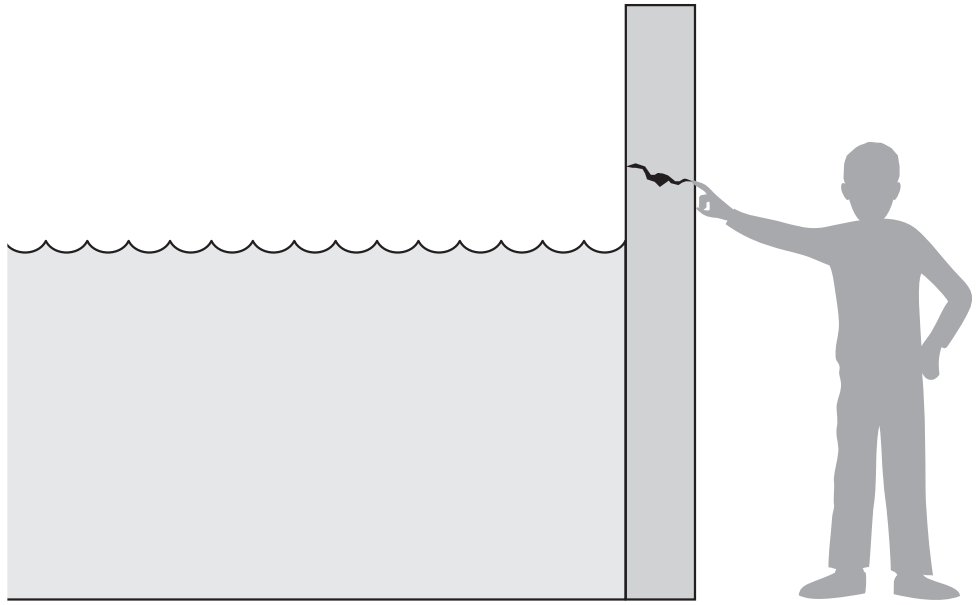
- A **vulnerability** is a *weakness in the system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm*.
  - For instance, a particular system may be vulnerable to **unauthorized data manipulation** because the system *does not verify a user's identity before allowing data access*.
- **Threat** to a computing system is *a set of circumstances that has the potential to cause loss or harm*.
- A human (criminal) who *exploits a **vulnerability*** perpetrates an ***attack*** on the system.

The Vulnerability–Threat–Control Paradigm

- An attack can also be launched **by another system**, as when one system sends an overwhelming flood of messages to another, **virtually shutting down** the second system's ability to function.
  - Unfortunately, we have seen this type of attack frequently, as **denial-of-service attacks** deluge servers with more messages than they can handle.
- How do we address these problems?
  - We use a **control** or **countermeasure** as **protection**.
  - A **control** is an *action, device, procedure, or technique that removes or reduces a vulnerability*.

Threat and Vulnerability

- Relationship among **threats**, **controls**, and **vulnerabilities**:
  - A **threat** is **blocked by control** of a **vulnerability**.
  - To devise **controls**, we must *know as much about **threats** as possible*.
- The fact that the violation might occur means that the ***actions that might cause it should be guarder against***.



The water is the **threat**, the crack the **vulnerability**, and the **finger** the control (for now).

Before we can protect **assets**, we need to **know the kinds of harm** we have to **protect** them against, so now we **explore threats to valuable assets**.

Threats

- We can consider **potential harm to assets** in two ways:
  - We can look at **what** bad things can happen to assets, and
  - We can look at **who** or **what** can cause or allow those bad things to happen.
- These two perspectives enable us to determine how to protect assets.

What makes your computer valuable to you?

- First, you use it as a tool for sending and receiving email, searching the web, writing papers, and performing many other tasks, and you expect it to be **available** for use when you want it.
  - Without your computer these tasks would be harder, if not impossible.
- Second, you rely heavily on your computer's **integrity**.
  - When you write a paper and save it, you trust that the paper will reload exactly as you saved it. Similarly, you expect that the photo a friend passes you on a flash drive will appear the same when you load it into your computer as when you saw it on your friend's computer.
- Finally, you expect the "personal" aspect of a **personal computer to stay personal**, meaning you want it to protect your **confidentiality**.
  - For example, you want your email messages to be just between you and your listed recipients; you don't want them broadcast to other people. And when you write an essay, you expect that no one can copy it without your permission.

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 three properties, **hallmarks of solid security**, appear in the literature as early as James P. Anderson's essay on computer security (we discussed Anderson's report on first lecture).

C-I-A Triad or Security Triad

- ISO 7498-2 adds to them two more properties that are desirable, particularly in communication networks:
  - **Authentication:** *the process or action of proving or showing something to be true, genuine, or valid.*
  - **Nonrepudiation:** *is the assurance that someone cannot deny something.*
    - **Nonrepudiation** refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated
- The U.S. Department of Defense adds **auditability**: *the ability of a system to trace all actions related to a given asset*.

C-I-A Triad

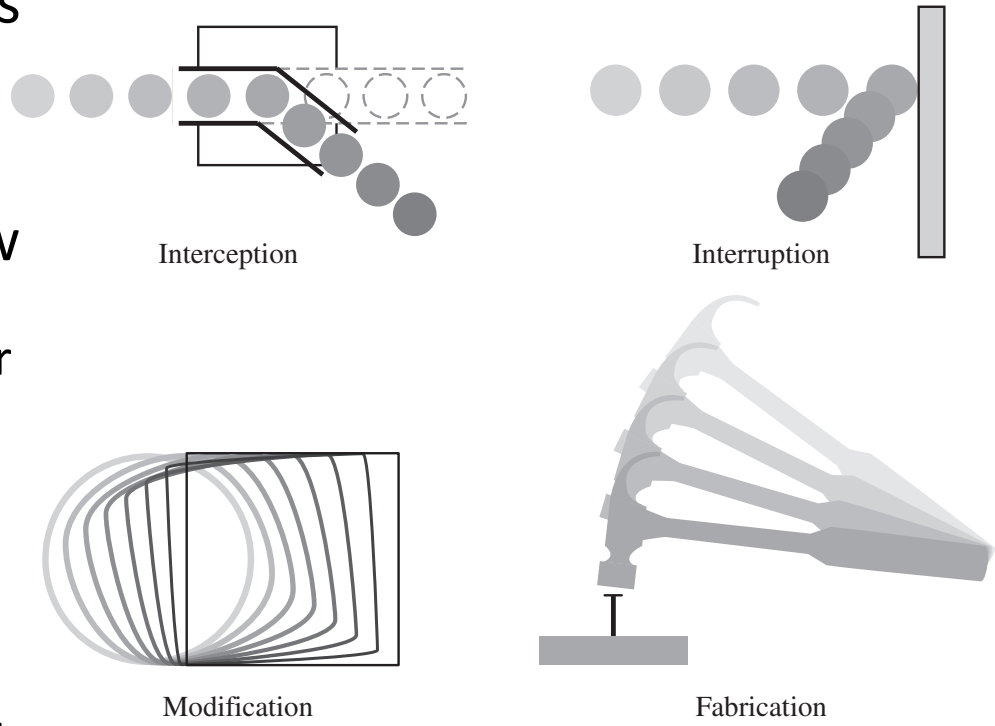
- What can happen to harm the *confidentiality*, *integrity*, or *availability* of computer assets?
  - If a thief steals your computer, you no longer have access, so you have lost **availability**.
  - If the thief looks at the pictures or documents you have stored, your **confidentiality** is compromised.
  - If the thief changes the content of your music files but then gives them back with your computer, the **integrity** of your data has been harmed.

C-I-A Triad: Nature of Harm

- The C-I-A triad can be viewed from a different perspective: **the nature of the harm caused to assets.**
- Harm can also be characterized by four acts: **interception**, **interruption**, **modification**, and **fabrication**.

C-I-A Triad: Nature of Harm

- Confidentiality can suffer if someone intercepts data
  - some unauthorized party has gained access to an asset.
- Availability is lost if something interrupts a flow of data or access to a computer
  - an asset of the system becomes lost, unavailable, or unusable.
- Integrity can fail if something modifies data or fabricates false data.
  - an unauthorized party not only accesses but **tampers** (forges) with an asset, the threat is a **modification**.
  - an unauthorized party might create a **fabrication** of **counterfeit** objects on a computing system.



Confidentiality

- Some things obviously need **confidentiality protection**.
  - Students' grades, financial transactions, medical records, and tax returns are sensitive.
  - A proud student may run out of a classroom screaming "I got an A!" but the student should be the one to choose whether to reveal that grade to others.
  - Diplomatic and military secrets, companies' marketing and product development plans, and educators' tests, also must be carefully controlled.
- Sometimes, however, it is not so **obvious** that something is sensitive.
  - For example, a military food order may seem like innocuous information, but a **sudden increase** in the order could be a sign of incipient engagement in conflict. (*Side-Channel Attacks*)

Confidentiality

- Purchases of food, hourly changes in location, and access to books are not things you would ordinarily consider confidential, but they **can reveal something that someone wants to be kept confidential**.
- The definition of confidentiality is straightforward: *Only authorized people or systems can access protected data*. However, **ensuring confidentiality can be difficult**.

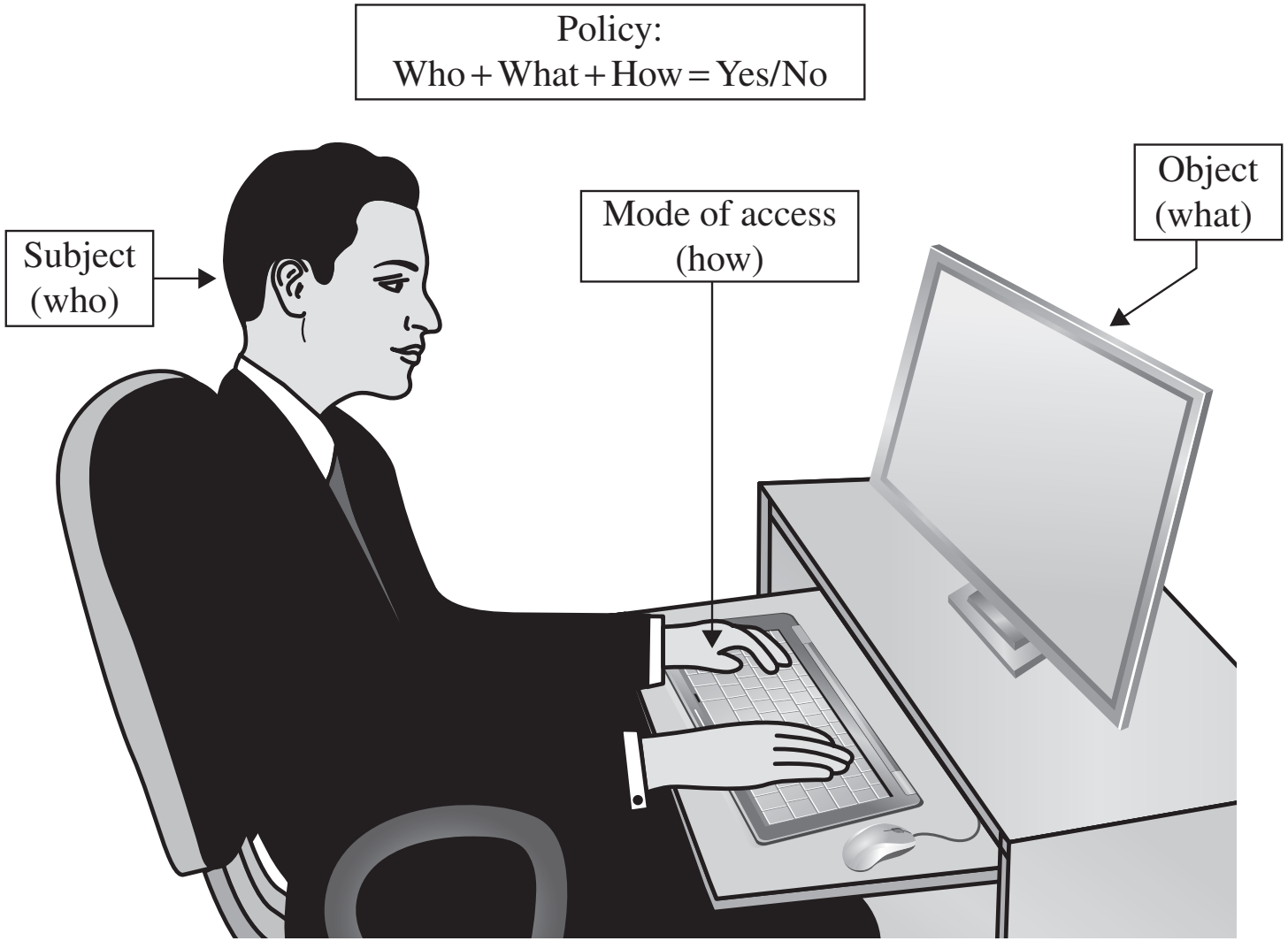
Confidentiality can be Difficult

- 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? the whole collection? pieces of data out of con- text? Can someone who is authorized disclose data to other parties?
  - Sometimes there is even a question of who owns the data: If you visit a web page, do you own the fact that you clicked on a link, or does the web page owner, the Internet provider, someone else, or all of you?

Confidentiality

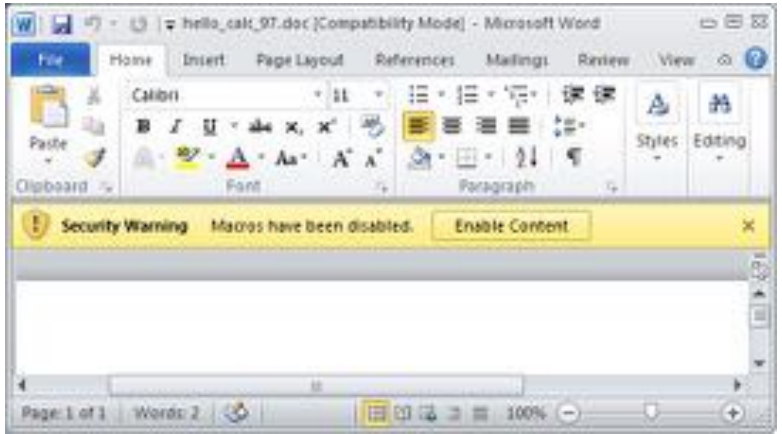
- Confidentiality relates most obviously to **data**, although we can think of the confidentiality of a **piece of hardware** (a novel invention) or a **person** (the whereabouts of a wanted criminal).
- Here are some properties that could mean a failure of data confidentiality:
  - An unauthorized person accesses a data item.
  - An unauthorized process or program accesses a data item.
  - A person authorized to access certain data accesses other data not authorized
  - An unauthorized person accesses an approximate data value (for example, not knowing someone's exact salary but knowing that the salary falls in a particular range or exceeds a particular amount).
  - An unauthorized person learns the existence of a piece of data (for example, knowing that a company is developing a certain new product or that talks are underway about the merger of two companies).

Access Control



Integrity

- Several years ago a malicious macro in a Word document inserted the word “not” after some random instances of the word “is;” you can imagine the havoc that ensued. **Because the document was generally syntactically correct**, people did not immediately **detect the change**.
- A model of the Pentium computer chip produced an incorrect result in certain circumstances of floating-point arithmetic. Although the circumstances of failure were rare, Intel decided to manufacture and replace the chips.



Integrity

- Integrity is **harder to pin down than confidentiality**.
- For example, if we say that we have preserved the integrity of an item, we may mean that the item is
  - Precise
  - Accurate
  - Unmodified
  - modified only in acceptable ways
  - modified only by authorized people
  - modified only by authorized processes
  - consistent
  - internally consistent
  - meaningful and usable
- Integrity can be enforced in much the same way as can confidentiality: by rigorous control of **who** or **what** can access which resources in what ways.

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. Fortunately, few of us experience that failure.
  - Many of us do experience overload, however: access gets slower and slower; the computer responds but not in a way we consider normal or acceptable.

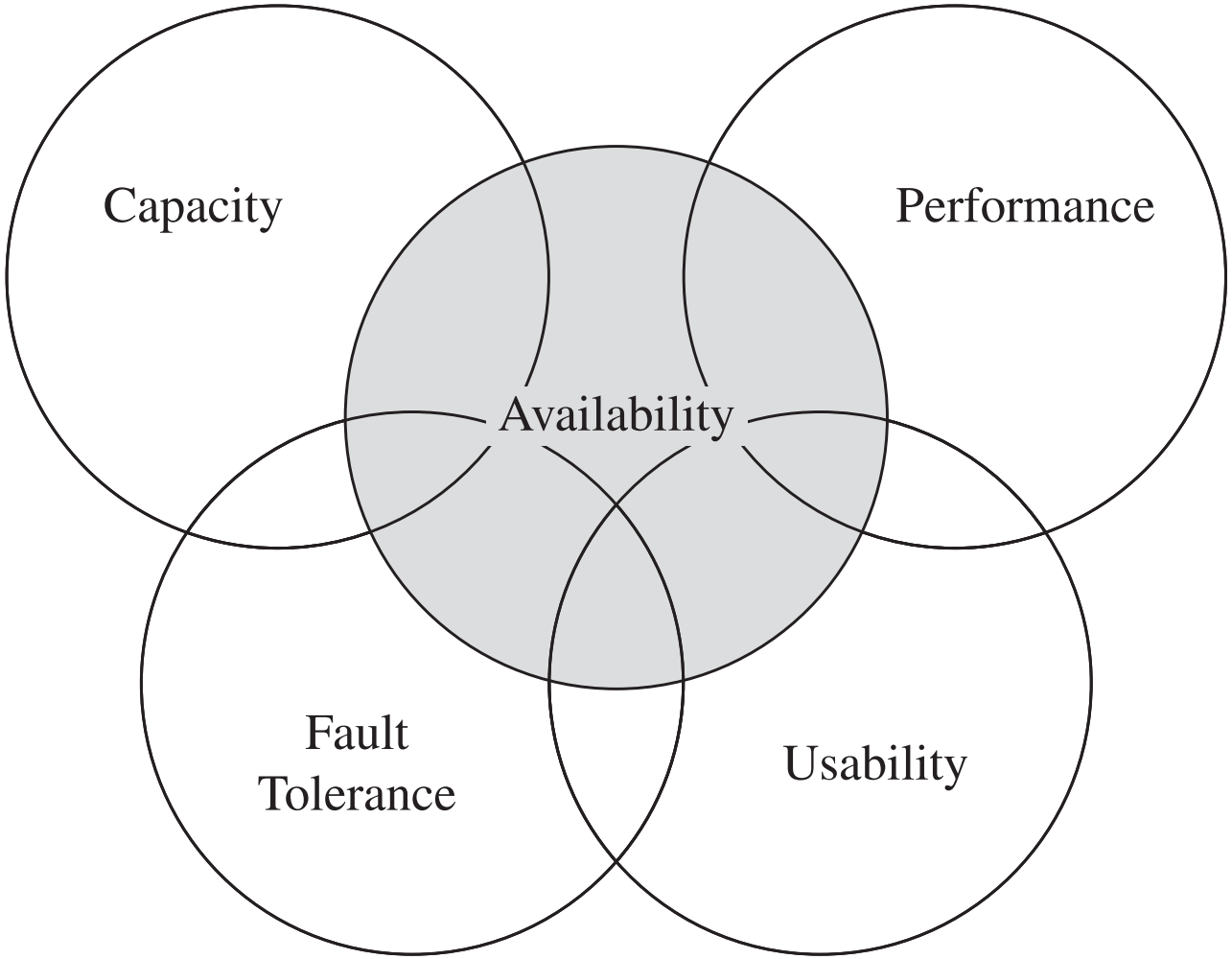
Availability

- Availability applies both to **data** and to **services** (that is, to information and to information processing), and it is similarly complex.
- For example, an object or service is thought to be available if the following are true:
  - It is present in a usable form.
  - It has enough capacity to meet the service's needs.
  - It is making clear progress, and, if in wait mode, it has a bounded waiting time.
  - The service is completed in an acceptable period of time.

Availability – Different Perspective

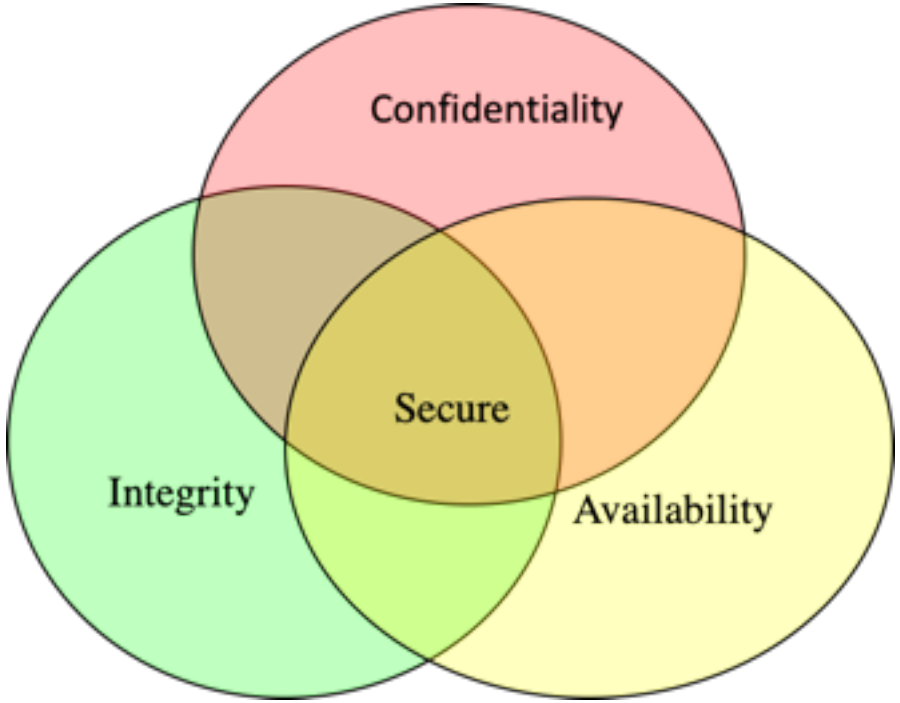
- There is a **timely response** to our request.
  - Resources are allocated so that some requesters are not favored over others.
- **Concurrency is controlled**; that is, simultaneous access, deadlock management, and exclusive access are supported as required.
- The service or system involved follows a philosophy of **fault tolerance**, whereby hardware or software faults lead to graceful cessation of service or to workarounds rather than to crashes and abrupt loss of information.
- The service or system can be used **easily** and in the way it was **intended** to be used. (This is a characteristic of **usability**, but an unusable system may also cause an availability failure.)

Availability



Relationship between Confidentiality, Integrity, and Availability

- In fact, these three characteristics can be independent, can overlap, and can even be mutually exclusive.



Goals of Security

- **Prevention**
  - Prevent attackers from violating security policy
- **Detection**
  - Detect attackers' violation of security policy
- **Recovery**
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

Access Control

- Computer security seeks to *prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability)*.
- A paradigm of computer security is **access control**:
  - To implement a **policy**, computer security controls all accesses by all subjects to all protected objects in all modes of access.
  - 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**.
    - Indeed, experts on dependability will note that single points of control can become **single points of failure**, making it easy for an attacker to destroy availability by disabling the single control point.

Security Models

- Much of computer security's past success has focused on **confidentiality** and **integrity**; Can you tell why?
  - There are models of confidentiality and integrity, for example, see Bell La Padula model and Biba model

https://youtu.be/r1pnyxgWD38

https://youtu.be/SEV110BkOfQ

- Availability is security's next great challenge.

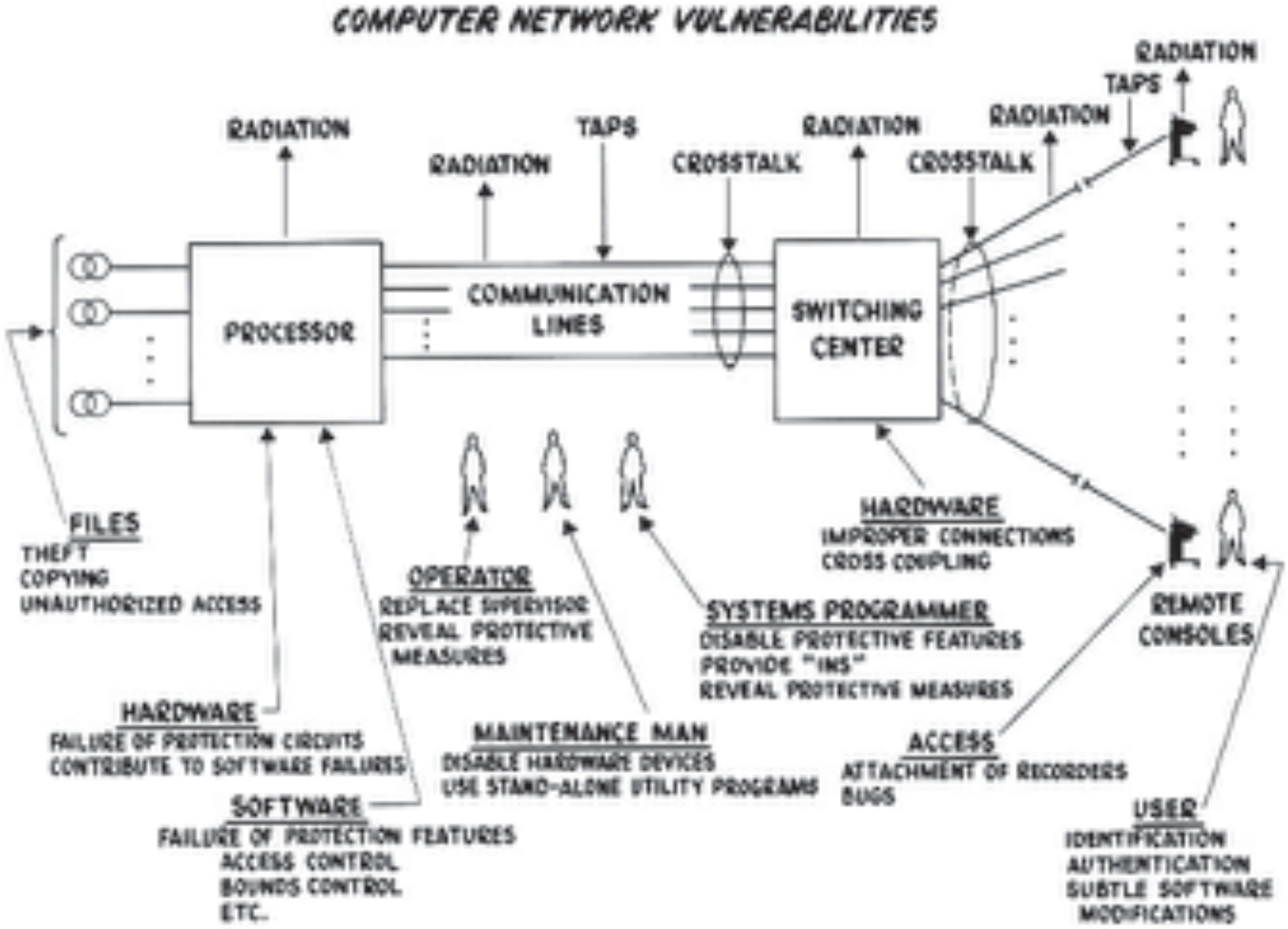


Figure taken from Willis Ware's report. Ware was concerned primarily with the protection of classified data, that is, preserving confidentiality.

Types of Threats

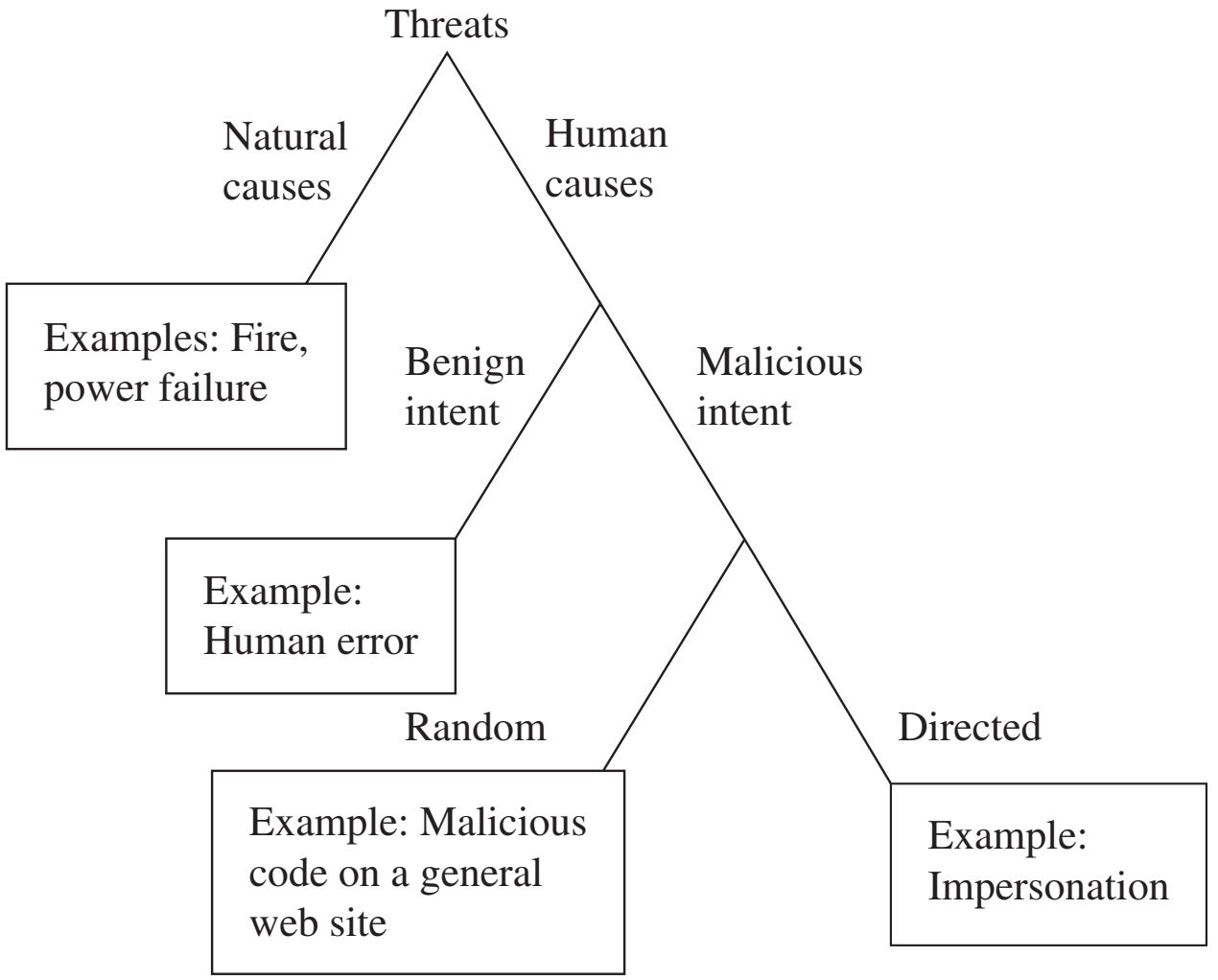
- One way to analyze harm is to consider the **cause or source**. We call a potential cause of harm a **threat**.
- Harm can be caused by either non-human events or humans.
  - Examples of **non-human threats** include natural disasters like fires or floods; loss of electrical power; failure of a component such as a communications cable, processor chip, or disk drive; or attack by a wild boar.
  - Human threats can be either benign (non-malicious) or malicious.
    - Non-malicious kinds of harm include someone's accidentally spilling a soft drink on a laptop, unintentionally deleting text, inadvertently sending an email message to the wrong person, and carelessly typing "12" instead of "21" when entering a phone number or clicking "yes" instead of "no" to overwrite a file.
    - These inadvertent, human errors happen to most people; we just hope that the seriousness of harm is not too great, or if it is, that we will not repeat the mistake.

Types of Threats

- Most computer security activity relates to **malicious**, **human-caused harm**:
  - A malicious person actually wants to cause harm, and so we often use the term ***attack*** for a malicious computer security event.
- Malicious attacks can be random or directed.
  - In a **random attack** the attacker wants to harm **any** computer or user; such an attack is analogous to accosting the next pedestrian who walks down the street.
    - For example, a malicious code posted on a website that could be visited by anybody.
  - In a **directed attack**, the attacker intends harm to **specific** computers, perhaps at one organization (think of attacks against a political organization) or belonging to a specific individual (think of trying to drain a specific person's bank account, for example, by impersonation).

Types of Threats

- This diagram shows threats categorized according to whether they are human-caused, malicious, or directed. These characteristics will affect security planning in important ways later.



Types of Threats

- Neither this book nor any checklist or method can show you *all* the kinds of harm that can happen to computer assets.
- There are too many ways to interfere with your use of these assets.
- The Common Vulnerabilities and Exposures (CVE) list (http://cve.mitre.org/) is a dictionary of publicly known security vulnerabilities and exposures.
  - CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of security tools and services.
  - To measure the extent of harm, the Common Vulnerability Scoring System (CVSS) (see http://nvd.nist.gov/cvss.cfm) provides a standard measurement system that allows accurate and consistent scoring of vulnerability impact.

Vuln ID	Summary	CVSS Severity
CVE-2020-15709	Versions of add-apt-repository before 0.98.9.2, 0.96.24.32.14, 0.96.20.10, and 0.92.37.8ubuntu0.1~esm1, printed a PPA (personal package archive) description to the terminal as-is, which allowed PPA owners to provide ANSI terminal escapes to modify terminal contents in unexpected ways. **Published:** September 05, 2020; 12:15:13 AM -0400	V3.x:(not available) V2.0:(not available)
CVE-2020-24987	Tenda AC18 Router through V15.03.05.05_EN and through V15.03.05.19(6318) CN devices could cause a remote code execution due to incorrect authentication handling of vulnerable logincheck() function in /usr/lib/lua/ngx_authserver/ngx_wdas.lua file if the administrator UI interface is set to "radius". **Published:** September 04, 2020; 4:15:13 PM -0400	V3.x:(not available) V2.0:(not available)
CVE-2020-24986	Concrete5 up to and including 8.5.2 allows Unrestricted Upload of File with Dangerous Type such as a .php file via File Manager. It is possible to modify site configuration to upload the PHP file and execute arbitrary commands. **Published:** September 04, 2020; 4:15:11 PM -0400	V3.x:(not available) V2.0:(not available)

Advanced Persistent Threat (APT)

- Security experts are becoming increasingly concerned about a type of threat called **advanced persistent threat**.
- APT Examples:
  - A lone attacker might create a **random attack** that snares a few, or a few million, individuals, but the resulting impact is limited to what that single attacker can organize and manage.
  - A collection of attackers—think, for example, of the cyber equivalent of a street gang or an organized crime squad—might work together to purloin credit card numbers or similar financial assets to fund other illegal activity. Such attackers tend to be opportunistic, picking unlucky victims' pockets and moving on to other activities.

Advanced Persistent Threat (APT)

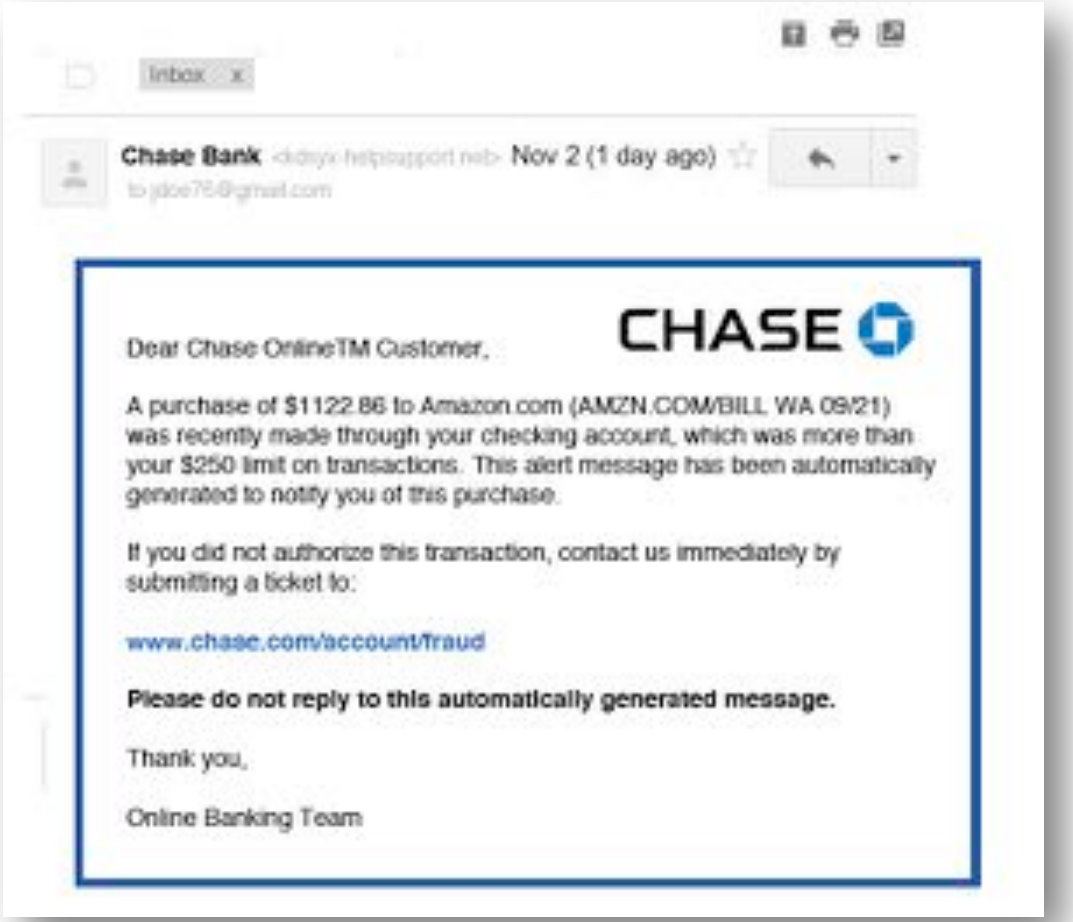
- Advanced persistent threat attacks come from **organized**, **well financed**, **patient assailants**.
  - Often affiliated with governments or quasi-governmental groups, these attackers engage in long term campaigns.
- They carefully select their **targets**, crafting **attacks** that appeal to specifically those targets; email messages called spear phishing are intended to seduce their recipients.
- Typically the attacks are **silent**, avoiding any **obvious impact** that would alert a victim, thereby allowing the attacker to exploit the victim's access rights over a **long time**.

Advanced Persistent Threat (APT)

- The motive of such attacks is sometimes unclear.
  - One popular objective is economic espionage.
- A series of attacks, apparently organized and supported by the Chinese government, was used in 2012 and 2013 to obtain product **designs from aerospace companies** in the United States.
  - There is evidence the stub of the attack code was loaded into victim machines long in advance of the attack; then, the attackers installed the more complex code and extracted the desired data.
  - In May 2014, the Justice Department indicted five Chinese hackers in absentia for these attacks.

Advanced Persistent Threat (APT)

- In the summer of 2014, a series of attacks against J.P. Morgan Chase bank and up to a dozen similar financial institutions allowed the assailants access to 76 million names, phone numbers, and email addresses.
  - The attackers—and even their country of origin— remain unknown, as does the motive.
  - Perhaps the attackers wanted more sensitive financial data, such as account numbers or passwords, but were only able to get the less valuable contact information.
  - It is also not known if this attack was related to an attack a year earlier that disrupted service to that bank and several others.

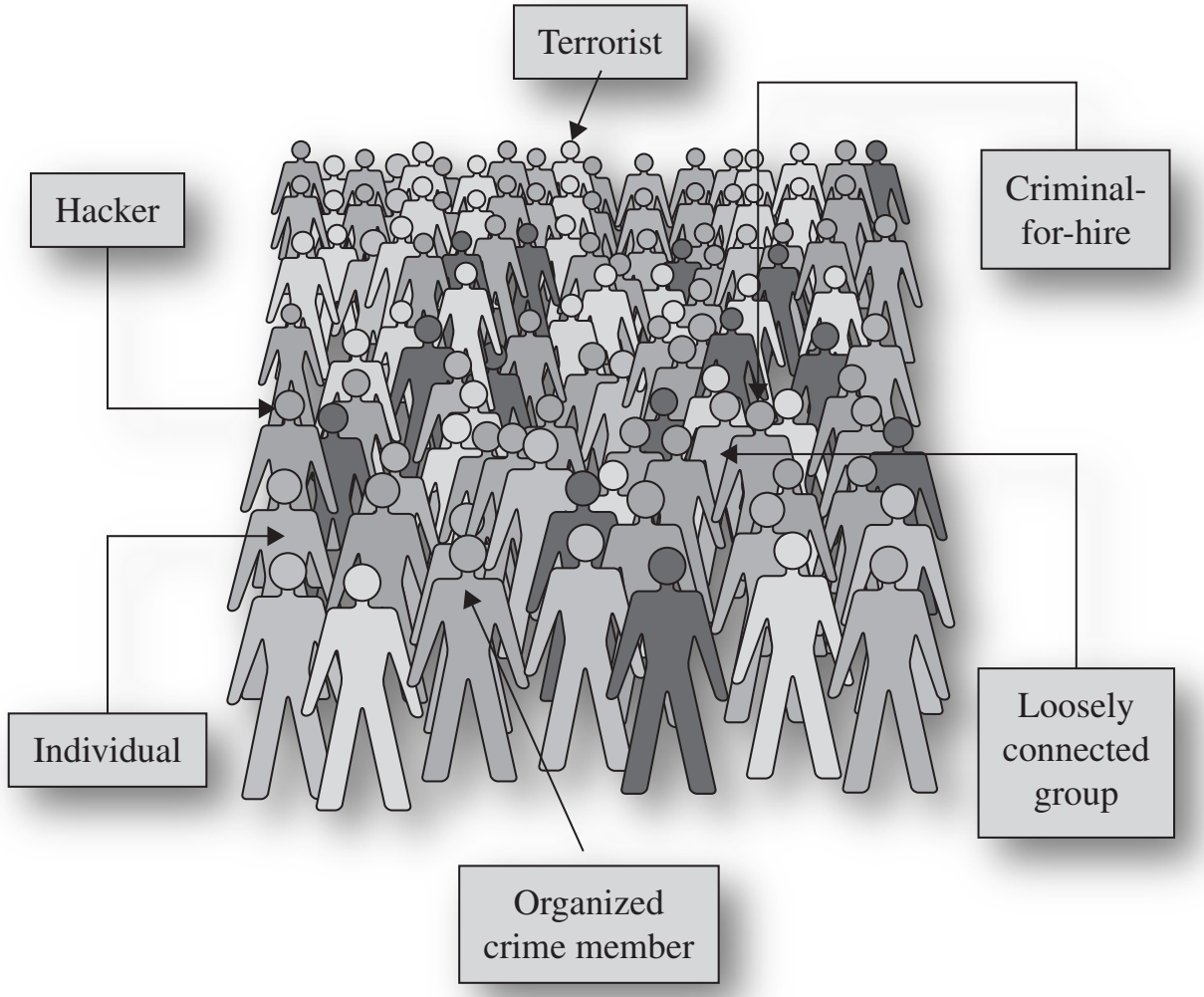



APT


Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

Types of Attackers

- **No one pattern matches all attackers**
- Each of these attacker types is associated with a different set of resources, capabilities, and motivations.
- Understanding the different types will help later in considering threats.



Types of Attackers: Individuals

- Originally, computer attackers were individuals, acting with motives of fun, challenge, or revenge.
- Early attackers acted alone; two of the most well-known are:
  - Robert Morris Jr., the Cornell University graduate student who brought down the Internet in 1988.
  - Kevin Mitnick, the man who broke into and stole data from dozens of computers, including the San Diego Supercomputer Center.

Types of Attackers: Organized Crime

- Attackers' goals include fraud, extortion, money laundering, and drug trafficking, areas in which organized crime has a well-established presence.
  - Evidence is growing that organized crime groups are engaging in computer crime.
- In fact, traditional criminals are recruiting hackers to join the lucrative world of cybercrime.
  - For example, Albert Gonzales was sentenced in March 2010 to 20 years in prison for working with a crime ring to steal 40 million credit card numbers from retailer TJMaxx and others, costing over $200 million (*Reuters*, 26 March 2010).

Types of Attackers: Organized, Worldwide Groups

- Whereas early motives for computer attackers such as Morris and Mitnick were personal, such as prestige or accomplishment, recent attacks have been heavily influenced by financial gain.
- Security firm McAfee reports "*Criminals have realized the huge financial gains to be made from the Internet with little risk. They bring the skills, knowledge, and connections needed for large scale, high-value criminal enterprise that, when combined with computer skills, expand the scope and risk of cybercrime.*"

Types of Attackers: Terrorists

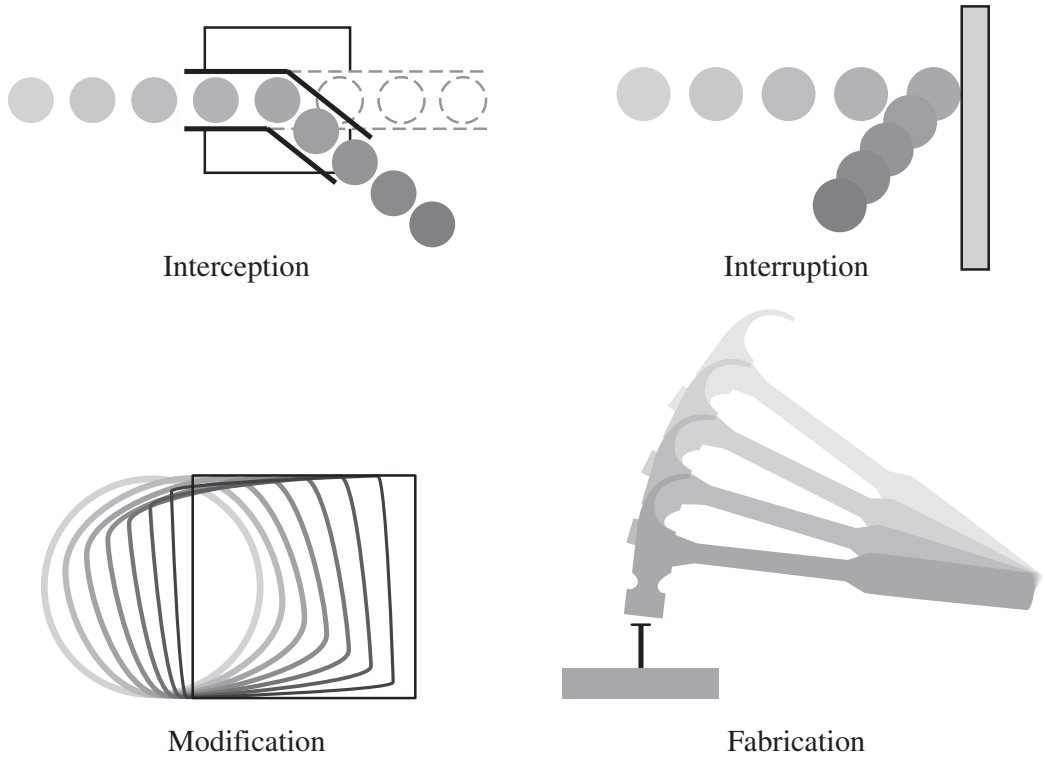
- The link between computer security and terrorism is quite evident. We see terrorists using computers in four ways:
  - *Computer as target of attack*:
    - Denial-of-service attacks and website defacements are popular activities for any political organization because they attract attention to the cause and bring undesired negative attention to the object of the attack.
    - Example: the massive denial-of-service attack launched against the country of Estonia
  - *Computer as method of attack*:
    - Launching offensive attacks requires the use of computers
    - Example: Stuxnet, a malicious computer code called a worm, is known to attack automated control systems, specifically a model of control system manufactured by Siemens. Experts say the code is designed to disable machinery used in the control of nuclear reactors in Iran.
    - The infection is believed to have spread through USB flash drives brought in by engineers maintaining the computer controllers.

Types of Attackers: Terrorists

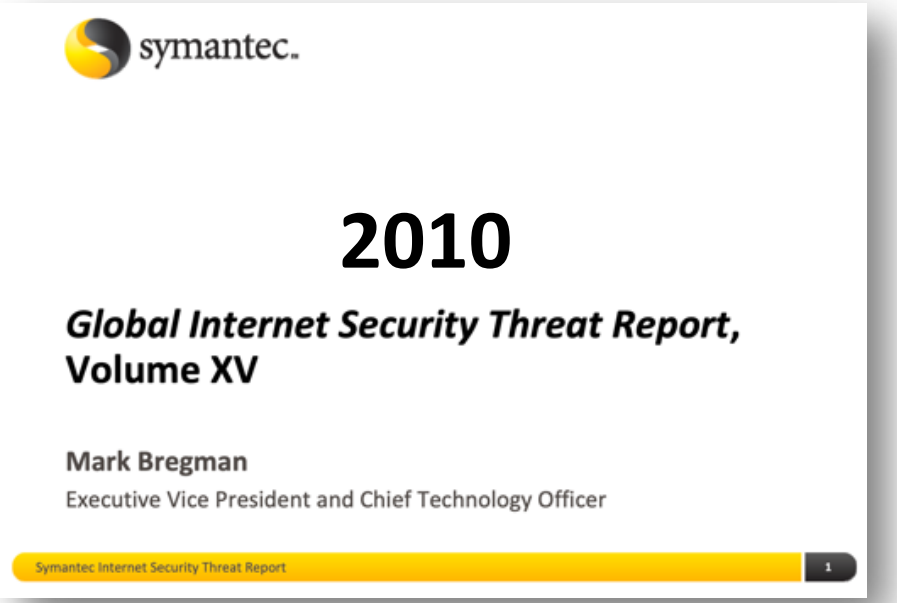
- *Computer as enabler of attack*:
  - Websites, web logs, and email lists are effective, fast, and inexpensive ways to allow many people to coordinate.
- *Computer as enhancer of attack*:
  - The Internet has proved to be an invaluable means for terrorists to spread propaganda and recruit agents.

Harm

- The negative consequence of an actualized threat is **harm**; we protect ourselves against threats in order to reduce or eliminate harm.
- We have already described many examples of computer harm: a stolen computer, modified or lost file, revealed private letter, or denied access to data.
  - These events cause harm that we want to avoid.



- In their 2010 global Internet threat report, security firm Symantec surveyed the kinds of goods and services offered for sale on underground web pages.
- These black-market websites demonstrate that the market price of computer assets can be dramatically different from their value to rightful owners.


symantec.

2010

Global Internet Security Threat Report, Volume XV

Mark Bregman

Executive Vice President and Chief Technology Officer

Symantec Internet Security Threat Report 1

https://www.fdic.gov/news/events/2010_fraud/Bregman.pdf

Overall Rank 2009	2008	Item	Percentage 2009	2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Harm

- The value of many assets can change over time, so the degree of harm (and therefore the severity of a threat) can change, too.
- With unlimited time, money, and capability, we might try to protect against all kinds of harm.
  - But because our resources are limited, we must **prioritize** our protection, safeguarding only against **serious threats** and the ones we can control.
- Choosing the threats we try to mitigate involve a process called **risk management**, and it includes weighing the seriousness of a threat against our ability to protect.
- **Risk management involves choosing which threats to control and what resources to devote to protection.**

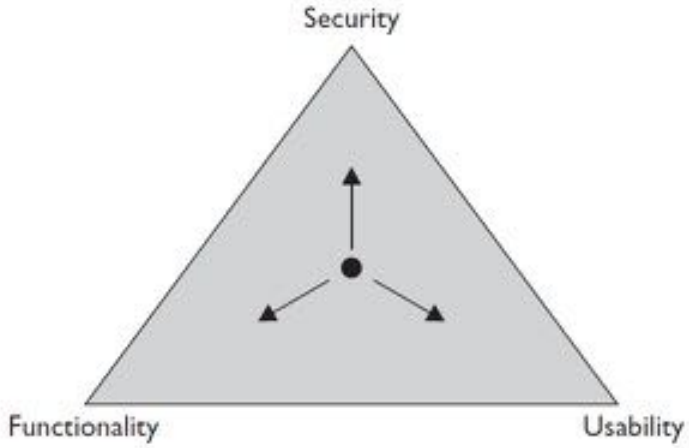

bmc
Threat
A new incident that has potential to harm a system
Vulnerability
A known weakness of an asset that hackers could exploit
Risk
The potential for loss or damage when a threat exploits a vulnerability

Risk and Common Sense

- The number and kinds of threats are practically unlimited because devising an attack requires an active *imagination*, *determination*, *persistence*, and *time* (as well as access and resources).
- The nature and number of threats in the computer world reflect life in general:
  - The causes of harm are limitless and largely unpredictable.
  - Natural disasters like volcanoes and earthquakes happen with little or no warning, as do auto accidents, heart attacks, influenza, and random acts of violence.

Risk and Common Sense

- To protect against accidents or the flu, you might decide to stay indoors, never venturing outside – too restrictive
  - But by doing so, you trade one set of risks for another; while you are inside, you are vulnerable to building collapse.
- There are too many possible causes of harm for us to protect ourselves—or our computers—completely against all of them.



Risk and Common Sense

- In real life we make decisions every day about the best way to provide our security.
  - For example, although we may choose to live in an area that is not prone to earthquakes, we cannot eliminate earthquake risk.
  - Some choices are conscious, such as deciding not to walk down a dark alley in an unsafe neighborhood; other times our sub- conscious guides us, from experience or expertise, to take some precaution.
- We evaluate the likelihood and severity of harm, and then consider ways (called countermeasures or controls) to address threats and determine the controls' effectiveness.

Risk and Common Sense

- Computer security is similar. Because we cannot protect against everything, we **prioritize**: Only so much time, energy, or money is available for protection, so we address some risks and let others slide.
- Or we consider alternative courses of action, such as transferring risk by purchasing insurance or even doing nothing if the side effects of the countermeasure could be worse than the possible harm. *The risk that remains uncovered by controls* is called **residual risk**.

Risk and Common Sense

- A basic model of risk management involves:
  - a user's **calculating** the value of all assets;
  - **determining** the amount of harm from all possible threats;
  - **computing** the costs of protection; and
  - **selecting** safeguards (that is, controls or countermeasures) based on the degree of risk and on limited resources and applying the safeguards to optimize harm averted.
- This approach to risk management is a logical and sensible approach to protection, but it has **significant drawbacks**.

Risk and Common Sense

- In reality, it is **difficult** to assess the value of each asset;
  - as we have seen, value can change depending on context, timing, and a host of other characteristics.
- Even harder is **determining the impact** of all possible threats.
  - The range of possible threats is effectively limitless, and it is difficult (if not impossible in some situations) to know the short- and long-term impacts of an action.
- Although we should not apply protection haphazardly, we will necessarily protect against threats we consider **most likely or most damaging**.
  - For this reason, it is essential to understand how we perceive threats and evaluate their likely occurrence and impact.

Risk and Common Sense

- Let us look more carefully at the nature of a security threat. We have seen that one aspect—its potential harm—is the amount of damage it can cause; this aspect is the **impact** component of the risk.
- We also consider the magnitude of the threat's **likelihood**.
  - A likely threat is not just one that someone might want to pull off but rather one that could occur.
    - 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.
- So a good place to start in assessing risk is to look at whether the proposed action is feasible. Three factors determine feasibility, as we describe next.

Method—Opportunity—Motive (MOM)

- A malicious attacker must have three things to ensure success: **method**, **opportunity**, and **motive**.
  - Roughly speaking, method is the how; opportunity, the when; and motive, the why of an attack.
  - Deny the attacker any of those three and the attack will not succeed.
- Understanding method, motive, and opportunity can be a good way to think about potential threats.
- Reducing any of those dimensions can lower the risk to the system.

MOM: Method

- By **method** we mean the skills, knowledge, tools, and other things with which to perpetrate the attack.
- Think of comic figures that want to do something, for example, to steal valuable jewelry, but the characters are so inept that their every move is doomed to fail.
- These people lack the capability or method to succeed, in part because there are no classes in jewel theft or books on burglary for dummies.

MOM: Method

- Anyone can find plenty of courses and books about computing, however, knowledge of specific models of computer systems is widely available in bookstores and on the Internet.
- Mass-market systems (such as the Microsoft or Apple or Unix operating systems) are readily available for purchase, as are common software products, such as word processors or database management systems, so potential attackers can even get hardware and software on which to experiment and perfect an attack.
- Various attack tools—scripts, model programs, and tools to test for weaknesses—are available from hackers' sites on the Internet, to the degree that many attacks require only the attacker's ability to download and run a program.

MOM: Method

- The term **script kiddie** describes someone who downloads a complete attack code package and needs only to enter a few details to identify the target and let the script perform the attack.
  - Often, only time and inclination limit an attacker.

MOM: Opportunity

- **Opportunity** is *the time and access to execute an attack*.
  - You hear that a fabulous apartment has just become available, so you rush to the rental agent, only to find someone else rented it five minutes earlier. You missed your opportunity.
- Many computer systems present ample opportunity for attack. Systems available to the public are, by definition, accessible; often their owners take special care to make them fully available so that if one hardware component fails, the owner has spares instantly ready to be pressed into service.
- Other people are oblivious to the need to protect their computers, so unattended laptops and unsecured network connections give ample opportunity for attack.
- Some systems have private or undocumented entry points for administration or maintenance, but attackers can also find and use those entry points to attack the systems.

MOM: Motive

- Finally, an attacker must have a **motive** or reason to want to attack.
  - You probably have ample opportunity and ability to throw a rock through your neighbor's window, but you do not. Why not? Because you have no reason to want to harm your neighbor: You lack motive.
- We have already described some of the motives for computer crime: money, fame, self-esteem, politics, terror. It is often difficult to determine motive for an attack.

Method—Opportunity—Motive (MOM)

- By demonstrating **feasibility**, the factors of **method**, **opportunity**, and **motive** determine whether an attack can succeed.
- These factors give the advantage to the attacker because they are **qualities** or **strengths** the attacker must possess.
- Another factor, this **time** giving an advantage to the defender, determines whether an attack will succeed:
  - The attacker needs a vulnerability, an undefended place to attack. If the defender removes vulnerabilities, the attacker cannot attack.

Vulnerabilities

- A **vulnerability** *is a weakness in the security of the computer system.*
- In this course, we consider many, such as weak authentication, lack of access control, errors in programs, finite or insufficient resources, and inadequate physical protection.
- Paired with a credible attack, each of these vulnerabilities can allow har to confidentiality, integrity, or availability.
  - Each attack vector seeks to exploit a particular vulnerability.
- Security analysts speak of a system's **attack surface**, which is the system's full set of vulnerabilities—actual and potential.
  - The attack surface includes physical hazards, malicious attacks by outsiders, stealth data theft by insiders, mistakes, and impersonations.

Controls

- A **control** or **countermeasure** is a means to counter threats.
- Harm occurs when a threat is realized against a vulnerability. To protect against harm, then, we can neutralize the threat, close the vulnerability, or both.
- The possibility for harm to occur is called **risk**.

Controls

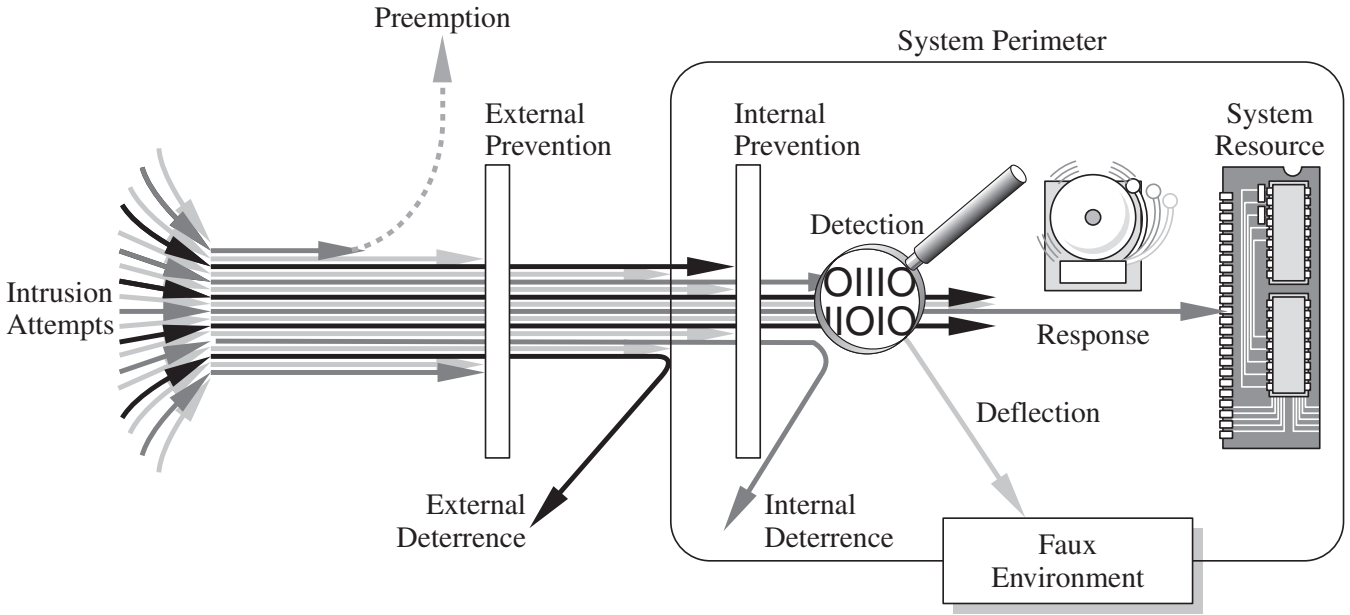
- We can deal with harm in several ways:
  - **prevent** it, by blocking the attack or closing the vulnerability
  - **deter** it, by making the attack harder but not impossible
  - **deflect** it, by making another target more attractive (or this one less so)
  - **mitigate** it, by making its impact less severe
  - **detect** it, either as it happens or some time after the fact
  - **recover** from its effects
- Of course, more than one of these controls can be used simultaneously.
  - we might try to prevent intrusions—but if we suspect we cannot prevent all of them, we might also install a detection device to warn of an imminent attack.
  - we could have in place incident-response procedures to help in the recovery in case an intrusion does succeed.

Controls

- **Security professionals balance the cost and effectiveness of controls with the likelihood and severity of harm.**
- To consider the controls or countermeasures that attempt to prevent exploiting a computing system’s vulnerabilities.
- Computer security has the same characteristics. We have many controls at our disposal. Some are easier than others to use or implement. Some are cheaper than others to use or implement. And some are more difficult than others for intruders to override.

Different Types of Controls

- In this simple representation of a networked system, it is easy to see all the touch points where controls can be placed, as well as some different types of controls, including deterrence, deflection, response, prevention, and preemption. (*Threat Modeling*)



Controls

- We present an overview of the controls available to us:
  - **Physical controls:** stop or block an attack by using something tangible too.
    - locks, (human) guards, sprinklers and other fire extinguishers.
  - **Procedural** or **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, program or operating system access controls, network protocols, firewalls, intrusion detection systems, encryption, network traffic flow regulators

Controls Available

- Encryption
  - We take data in their normal, unscrambled state, called:
    - cleartext or plaintext and transform them so that they are unintelligible to the outside observer; the transformed data are called enciphered text or ciphertext.
- Encryption clearly addresses the need for confidentiality of data.
- Additionally, it can be used to ensure **integrity**;
  - data that cannot be read generally cannot easily be changed in a meaningful manner.
- Encryption **does** not solve all computer security problems, and other tools must complement its use.
  - if encryption is not used properly, it may have no effect on security or could even degrade the performance of the entire system.

Controls Available

- Weak encryption can be worse than no encryption at all, because it gives users an unwarranted sense of protection.
- Therefore, we must understand those situations in which encryption is most useful as well as ways to use it effectively.

Controls Available

- **Software/Program Controls**
  - Programs must be secure enough to prevent outside attack
  - They must also be developed and maintained so that we can be confident of the programs' dependability.
- Program controls include the following:
  - Internal program controls: parts of the program that enforce security restrictions,
    - i.e. access limitations in a database management program
  - Operating system and network system controls: limitations enforced by the operating system or network to protect each user from all other users
    - i.e. chmod on UNIX: (Read, Write, Execute) vs. (Owner, Group, Other)
  - Independent control programs: application programs,
    - i.e. password checkers, intrusion detection utilities, or virus scanners, that protect against certain types of vulnerabilities

Controls Available

- **Development controls:**
  - quality standards under which a program is designed, coded (implementation), tested, and maintained to prevent software faults from becoming exploitable vulnerabilities
    - i.e. Penetration testing (pen testing or ethical hacking), is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.
- Software controls frequently affect users directly?
  - For example, when the user is interrupted and asked for a password before being given access to a program or data.
  - Because they influence the usability of the system, software controls must be carefully designed.
    - Ease of use and capabilities are often competing goals in the design of a collection of software controls.

Controls Available

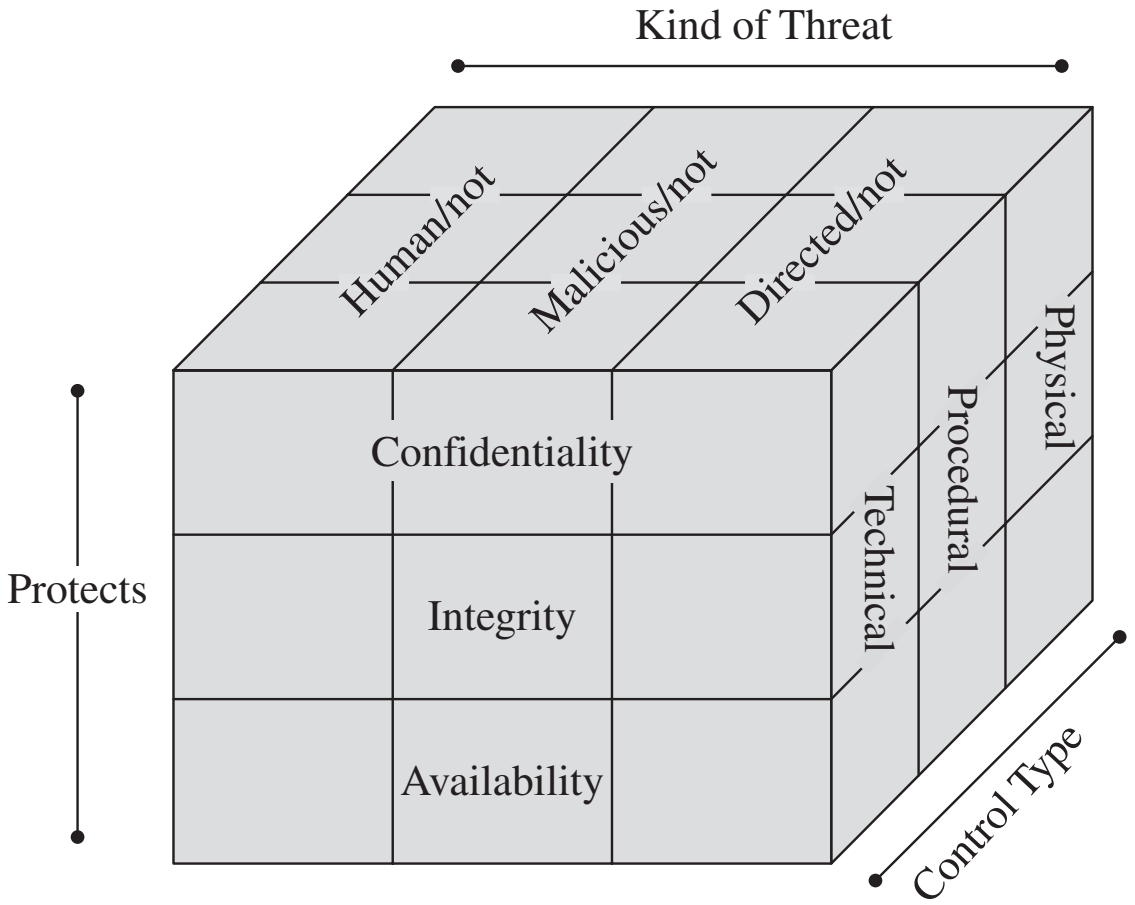
- Hardware Controls
  - Numerous hardware devices have been created to assist in providing computer security. These devices include a variety of means, such as
    - hardware or smart card implementations of encryption
    - locks or cables limiting access or deterring theft
    - devices to verify users' identities
    - firewalls
    - intrusion detection systems
    - circuit boards that control access to storage media

Controls Available

- **Policies and Procedures**
  - Sometimes, we can rely on agreed-on procedures or policies among users rather than enforcing security through hardware or software means
    - i.e. frequent changes of passwords
  - We must not forget the value of community standards and expectations when we consider how to enforce security.
- **Physical Controls**
  - i.e. locks on doors,
  - guards at entry points,
  - backup copies of important software and data, and
  - physical site planning that reduces the risk of natural disasters.

Controls/Countermeasures

- You can think in terms of the property to be protected and the kind of threat when you are choosing appropriate types of countermeasures.
- Thinking about controls in this way enables you to easily map the controls against the threats they help address.
- It can be effective to use **overlapping controls** or **defense in depth**: more than one control or more than one class of control to achieve protection.



Effectiveness of Controls

- **Awareness of Problem**
  - People using controls must be convinced of the need for security. That is, people will willingly cooperate with security requirements only if they understand
    - why security is appropriate in a given situation.
- **Likelihood of Use**
  - Of course, no control is effective unless it is used
- **Overlapping Controls**
  - Several different controls may apply to address a single vulnerability.

Effectiveness of Controls

- **Principle of Effectiveness**:
  - Controls must be used properly to be effective.
    - They must be efficient, easy to use, and appropriate.
  - This principle implies that computer security controls
    - must be efficient enough, in terms of time, memory space, human activity, or other resources used,
    - using the control does not seriously affect the task being protected.
    - Controls should be selective so that they do not exclude legitimate accesses.
- **Periodic Review**
  - Just when the security specialist finds a way to secure assets against certain kinds of attacks, the opposition doubles its efforts in an attempt to defeat the security mechanisms. Thus, judging the effectiveness of a control is an ongoing task.

Principle of Weakest Link

- Security can be no stronger than its weakest link !!!
  - Whether it is the power supply that powers the firewall or the operating system under the security application or the human who plans, implements, and administers controls, a failure of any control can lead to a security failure.

Summary

- Vulnerabilities are weaknesses in a system;
  - threats exploit those weaknesses;
  - controls protect those weaknesses from exploitation
- Confidentiality, integrity, and availability are the three basic security primitives
- Different attackers pose different kinds of threats based on their capabilities and motivations
- Different controls address different threats; controls come in many flavors and can exist at various points in the system