CISC 7320X - COMPUTER SECURITY

Introduction

CISC 7320X - Computer Security

- Tzipora Halevi, Assistant Professor
  email: halevi@cis.brooklyn.cuny.edu
  Office Hours: Wednesdays, 6.30 pm – 8.00 pm
  Ingersol room 2156A
- Book:
  - Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, *Security in Computing,* 5th edition, Prentice Hall imprint, Pearson Education, Inc., 2015

Course Structure

- Assignment+ project - 33%
  - Done individually or in small groups
- Exams + quizzes + participation – 33%
  - Done individually
- Final exam - 34%

Class Policies

- Late homework/project: reduced credit
- Never share homework, solutions, code, etc.,
  - Don’t let any other student see them
  - Work on your own
    - unless assignment states otherwise
    - Don’t look at other students’ homework or past assignments you may find online
- Quote and properly cite references used in your work

INTRODUCTION

Class Objectives

- Define *information 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

What is Information?

- Meaning conveyed by a sequence of symbols
- Examples:
  - Bits
  - Alphabetic
  - Genetic sequence
- Can information be measured?
  - Yes, using information theory
    - Developed by Shannon

What is Security?

- State of being free from dangers or threats
- Protection of a person, building, organization, country against threats or crime

What is Information Security?

- The practice of protecting information by mitigating information risks
- The practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction
-
- Wikipedia

What Is Computer Security?

- The protection of the assets of a computer system
  - Hardware
  - Software
  - Data

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

FIGURE 1-2 Computer Objects of Value

What Is Computer Security?

- What is the value of the assets?
  - Is the asset easily replaced?
    - Cost of replacement.
  - Is the asset unique?

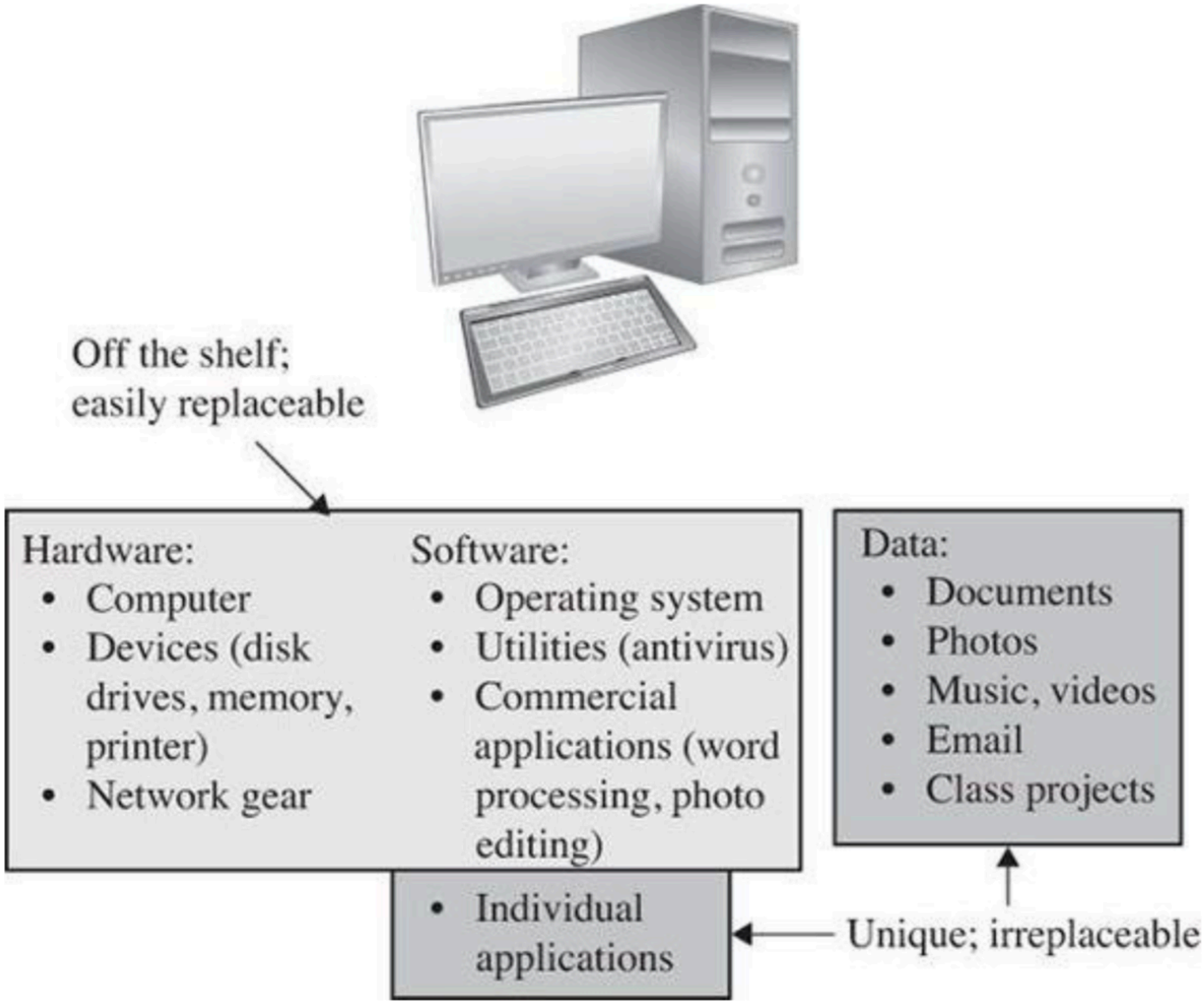


FIGURE 1-3 Values of Assets

What is Computer Security?

- Traditionally, computers are protected against:
  - Theft/damage to hardware
  - Theft/damage to information
  - Disruption of service

Growing Importance of Computer Security

- Increasing reliance on computer systems and the Internet
- Use of wireless networks such as Bluetooth and Wi-Fi
- Expanding array of smart devices
  - and ‘Internet of Things’ (IoT) devices

Why is computer security important?

- Attacks Impact everyone's day-to-day life
  - Millions of compromised computers
  - Millions of stolen passwords
    - Risk of identity theft
- Serious financial damage caused by security breaches

CYBERCRIME REPORT

FROM THE EDITORS AT CYBERSECURITY VENTURES

2017 Edition

The Official 2017 Annual Cybercrime Report is sponsored by **Herjavec Group**, a leading global information security advisory firm and Managed Security Services Provider (MSSP) with offices across the United States, Canada, and the United Kingdom. Read the Official Press Release or Download a PDF Version of the Report.

DAMAGE COSTS

Cybersecurity Ventures predicts cybercrime damages will cost the world $6 trillion annually by 2021

Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades.

– *Steve Morgan, Editor-In-Chief*

Menlo Park, Calif. — Oct. 16, 2017

Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. The impact on society is reflected in the numbers.

https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

NEWS

Cyber attacks cost U.S. enterprises $1.3 million on average in 2017

IT security budgets, as well the costs of data breaches, are up for North American enterprises and SMBs.

U.S. Army illustration

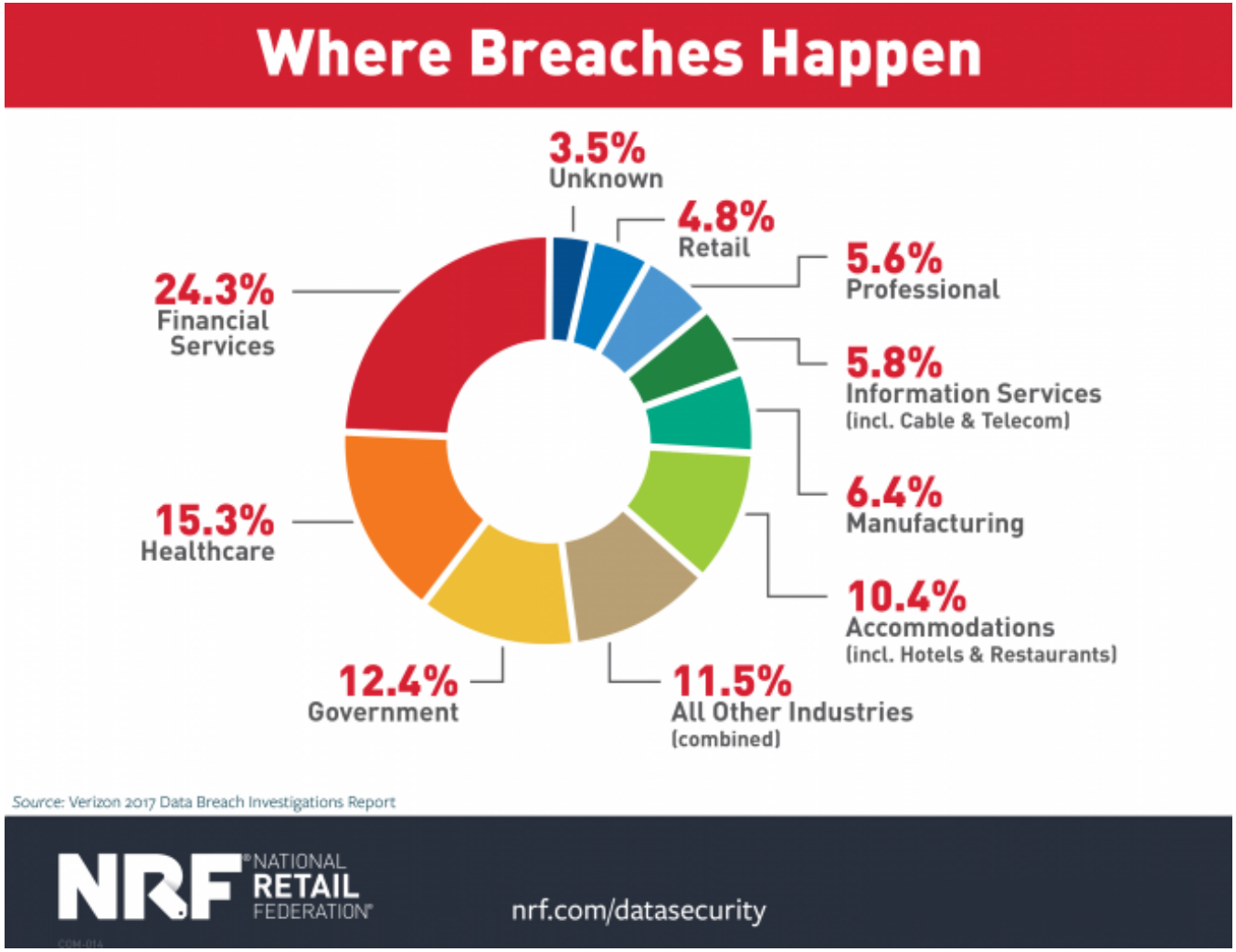
MORE LIKE THIS

Show the
it out with
Kaspersk
rumors

The curre
cybercrin

Who is a
ransomw

VIDEO
Office 36
examples
Hash En 1



https://nrf.com/advocacy/policy-agenda/data-security

How can we help?

- Security education can help us
  - Avoid attacks
  - Create safer systems
- We start by defining risk management

What describes best ”Information”?

- A discipline developed by Claude Shannon in the 1940’s
- Data, such as census, medical or readings from sensors etc.
- A sequence of symbols that convey some meaning in a given context
- Documents such as books, the content on the World Wide Web (WWW) etc

What describes best ”Information”?

- A discipline developed by Claude Shannon in the 1940’s
- Data, such as census, medical or readings from sensors etc.
- A sequence of symbols that convey some meaning in a given context
- Documents such as books, the content on the World Wide Web (WWW) etc

FUNDAMENTAL CONCEPTS

Computer Network

- A digital telecommunications network which allows nodes to share resources
- Networked computing devices exchange data with each other using a data link
- The connections between nodes are established using either cable media or wireless media

https://nizamtaher.wordpress.com/topics/topic-1-introduction-of-computer-network/

Cyber Vulnerabilities

- **Vulnerability** is a **cyber**-security term that refers to a flaw in a system
  - can leave it open to attack.
- May refer to any type of weakness in a computer system itself
  - Either in a set of procedures, or in anything that leaves information security exposed to a threat
- Cutting down vulnerabilities provides fewer options for malicious users to gain access to secure information.

https://www.techopedia.com/definition/13484/vulnerability
http://blog.escanav.com/2014/06/vulnerabilities-recorded-by-us-cert-cyber-security-bulletin/

Threats, Attacks and Controls

- A ***threat*** to a computing system is a set of circumstances with potential to cause loss or harm
  - Vulnerabilities make threat outcome possible
- A human who exploits a vulnerability perpetrates an ***attack*** on the system
- A ***control*** is an action, device, procedure, or technique that removes or reduces a vulnerability

Threats, Attacks and Controls

- ***Controls*** prevent ***threats*** from exercising vulnerabilities.
- A ***threat*** is blocked by control of a ***vulnerability***

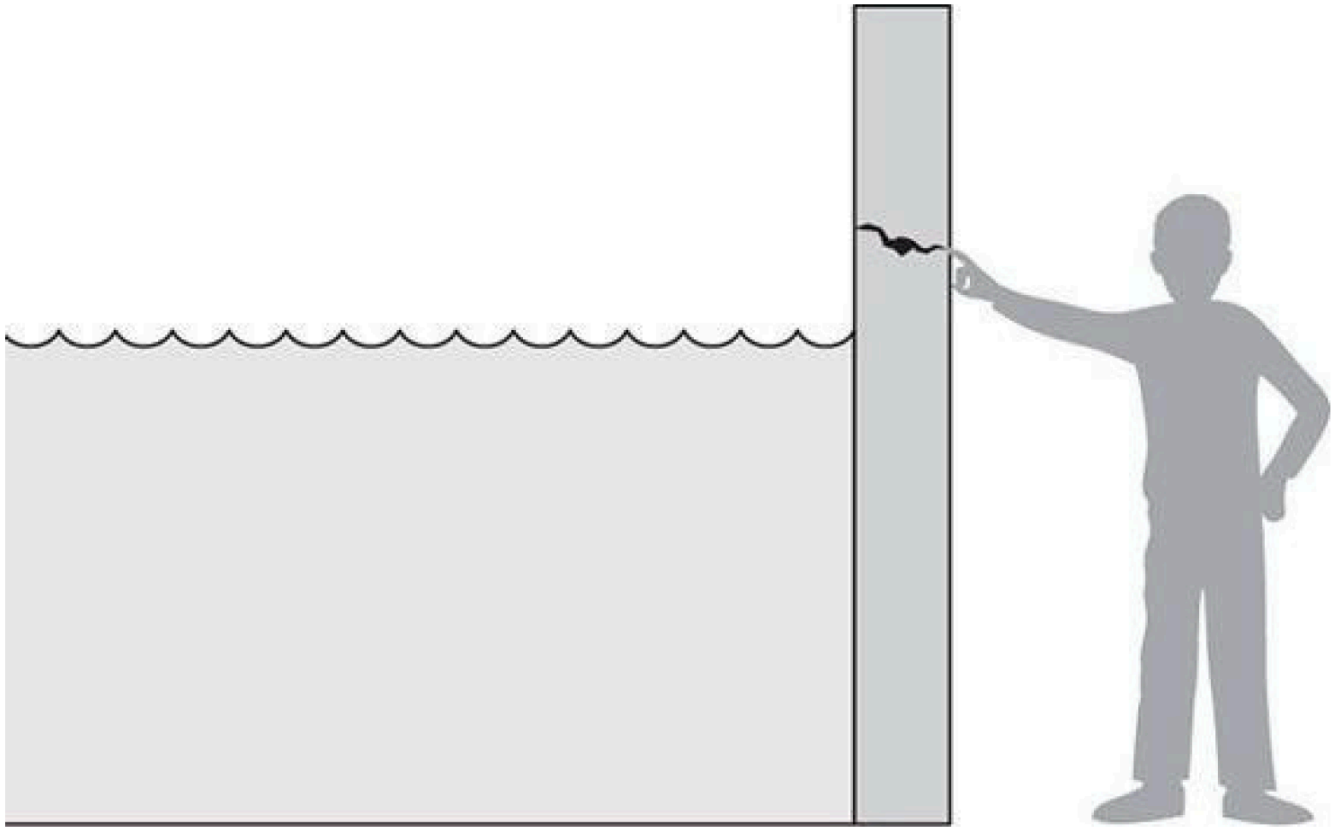


FIGURE 1-4 Threat and Vulnerability

Threats and Vulnerabilities

- Example: A crack in the wall, man standing next to wall
- ***Vulnerability*** is the crack
- ***Threat*** is that the man will drown if the water level rises

Zero-Day Vulnerability

- A vulnerability that is not known to the software developer or vendor
- However, it is known to the attacker
- Name refers to the number of days the developer had to fix the problem
  - Zero days

Exploit

- Software that is used to take advantage of a security bug or a vulnerability

Threat Model

- Key notion of threat model:
  - what/who are you defending against?
    - Determines which defenses to consider
      - E.g., where are valuable assets stored, where is the system most vulnerable to attacks, etc.

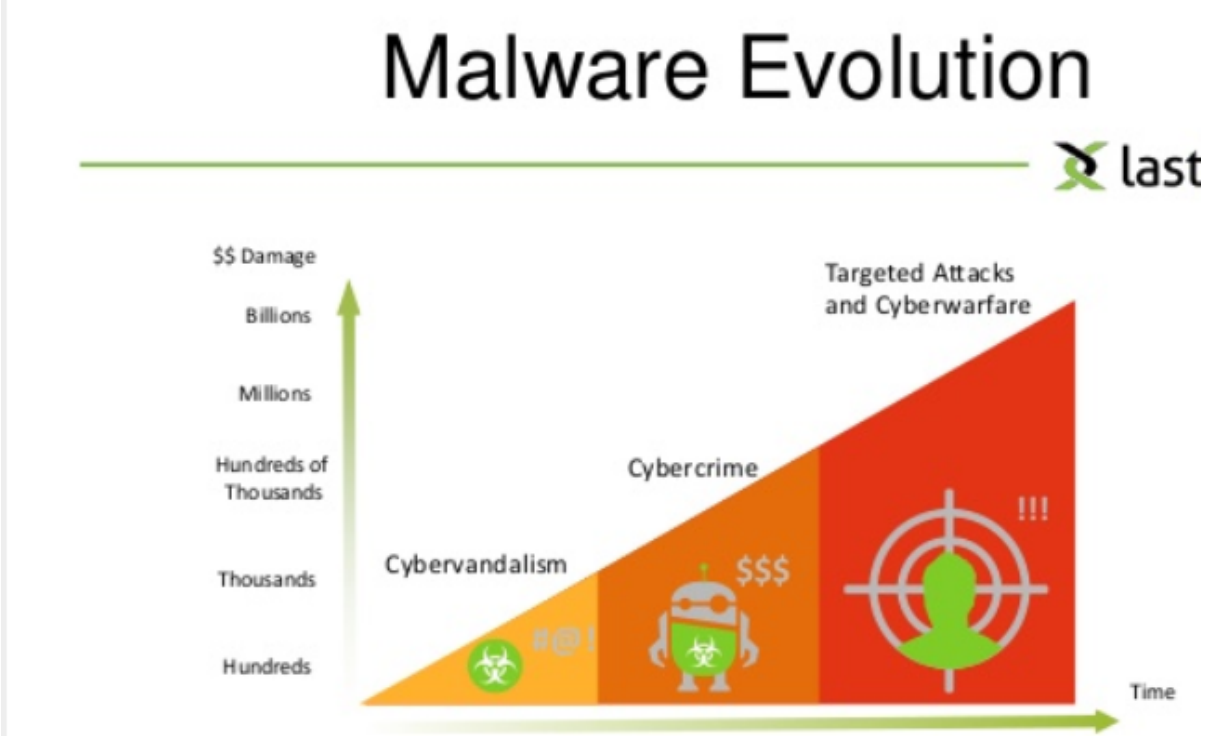
SECURITY THREATS

Security Threats History

- 1990's: fewer attacks, attackers gained fame,
  - Some attacks accidental,
- late 2000's: financially motivated
  - pharmaceuticals, credit card theft, identity theft
  - Phishing evolved into spear-phishing
    - More targeted form of attack
    - Uses target personal information to impersonate a trusted source
- 2010's: politically motivated
  - Government actors: Stuxnet, Flame, Aurora
  - Private activism: Anonymous, Wikileaks

Security Threats History

- Threats Have Evolved
  - Attackers have become more sophisticated;
- Arms race between attackers and defenders fuels rapid innovation in malware
- Many attacks aim for profit
  - are facilitated by a well-developed “underground economy” or cyber-crime organizations



https://www.slideshare.net/lastlinesecurity/ip-expo-oct-2014

How to protect from loss, destruction and illegal access

- Identify vulnerabilities – weaknesses that can be exploited to cause harm
- Monitor for threats – methods or situations that can cause harm
- Recognize an attack that exploits the vulnerabilities
- Take countermeasures or use methods to control an attack

Conclusions

- To protect computer systems, you must know your enemy
- Security is not about perfection: it's about defenses that are good enough to stop the threats you're likely to encounter

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY (C.I.A.)

Confidentiality

- Avoidance of the unauthorized disclosure of information
  - Protect data, keep information secret
  - Provide access only to authorized users

Confidentiality

- How secure is the information?
  - How secure does it need to be?
- Example:
  - Information on our course website
    - Public for everyone to see
  - Personal information
    - Some method of protection should be used

Confidentiality

- Examples of 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
    - specialized version of “an unauthorized person accesses a data item

Confidentiality

- Examples of failure of data confidentiality (cont.):
  - An unauthorized person accesses an approximate data value
    - E.g., knowing that someone's salary falls in a particular range
      - But not knowing someone's exact salary
  - An unauthorized person learns the existence of a piece of data
    - E.g., knowing that a company is developing a certain new product

Tools to ensure confidentiality

- Encryption:
  - Information encrypted using a secret key
  - Transformed info can be read using decryption key
    - Info essentially can not be read without this key
- Access Control:
  - Policies that limit access to confidential info
    - To people/systems with a “need to know”
    - May be based on person’s id, name or his role

Tools to ensure confidentiality (cont.)

- Authentication:
  - Determination of someone's ID or role
  - Maybe based on:
    - Something that the person has
      - Smart card, radio key, etc.
    - Something the person knows:
      - Password, etc
    - A physical trait of a person:
      - Fingerprints, etc.

Tools to ensure confidentiality (cont.)

- Authorization:
  - Is the person allowed access to the info?
    - Based on access control policy
  - Mechanism should be secure, prevent an attacker from tricking the system and gaining unauthorized access

Tools to ensure confidentiality (cont.)

- Physical Security:
  - Physical barriers that limit access to protected info
    - Such as locks, cabinets, doors.
    - Placing a computer in a windowless room.
    - Building a Faraday cage to prevent electromagnetic signals
      - To prevent side-channel attacks

Integrity

- Ensure information has not been altered in an unauthorized way
- Information may be compromised maliciously or by accident
  - Through hard drive crashes
  - Through a computer virus

Integrity

- How correct is the information?
- Has the data been modified during retrieval, in transit, or in storage?

- Failure of integrity occurs if:
  - Someone modifies the data stored or in transit
    - Unauthorized to do so

Tools to protect integrity

- ***Regular backups***
- ***Checksums***: map the content to a numerical value and save that value.
  - Read it back upon reading the information
- ***Data correcting codes***: store data in such a way that small changes can be easily detected
  - And corrected

Tools to protect integrity

- ***Regular backups***
- ***Checksums***: map the content to a numerical value and save that value.
  - Read it back upon reading the information
- ***Data correcting codes***: store data in such a way that small changes can be easily detected
  - And corrected
- What do all the above tools use?
  - The above tools all use redundancy
    - Replication of some of the information content or content

Availability

- Information is available when it is needed
  - Accessible and modifiable
    - to those authorized to do so
- How much uptime is the system providing?
- Is the data accessible by users all the time?

Availability

- Tools for ensuring availability:
  - Physical protections: housing that can withstand unexpected situations
    - Such as earthquakes, storms, etc.
    - Powered with generators
  - Computational redundancies:
    - Extra disks or web servers, such that failure of a single device will not degrade availability of data

Availability

- We are looking to build systems that are reliable
  - provide service across a wide range of operating states
- A system should remain accessible to authorized users for a range of operating conditions
  - such as if under attack, or being heavily used

C-I-A Triad

- A person or system can do three basic things with a data item: view it, modify it, or use it
  - Viewing relates to confidentiality
    - Only authorized users can view data
  - Modifying relates to integrity
    - Is the data correct
  - Using relates to availability
    - Can I access the data

C-I-A Triad - Summary

- Confidentiality – only those individuals or accounts who have permission can access a system.
- Integrity – a system or account can be altered only by authorized users
- Availability – a system/account is available when expected

C-I-A Triad

- C-I-A

Approaches to CIA

- We may have different priorities
  - We may have high Integrity and Confidentiality
    - But low availability
      - I.e., data kept secret and integrity secure, but not easily available
    - High Integrity, Availability and low Confidentiality
      - Example?
        - An ad on a website
- So not all aspects may be equally important in any scenario

SOME QUESTIONS

A message has integrity if:

- Is is authenticated
- It is verifiably unaltered
- It contains the sender's handwritten signature
- It contains the truth

A message has integrity if:

- Is is authenticated
- It is verifiably unaltered
- It contains the sender's handwritten signature
- It contains the truth

A third party (e.g. a spy) is not able to read a message when:

- The message is sent with integrity
- The message is sent using a nonrepudiation technique
- The message has high availability
- The message is using a cryptographic protocol to implement confidentiality

A third party (e.g. a spy) is not able to read a message when:

- The message is sent with integrity
- The message is sent using a nonrepudiation technique
- The message has high availability
- The message is using a cryptographic protocol to implement confidentiality

THREATS AND ATTACKS

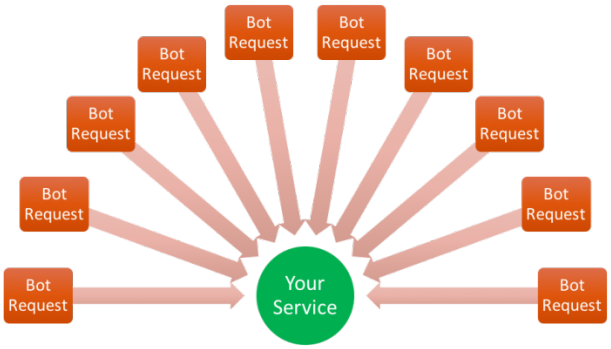
Threats and Attacks

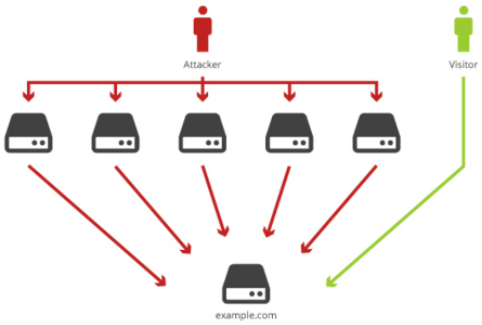
- Eavesdropping: interception of information during transmission
  - Includes side channel attacks
  - May be audio, electromagnetic, power, etc.
- Alteration: unauthorized modification of information
  - False information may be installed

http://blog.jammer-store.com/2011/09/cell-phone-spying-with-eavesdropping-trojan-danger/

Threats and Attacks (cont.)

- Denial-of-service: interruption or degradation of data or information
  - This is an attack on availability
  - For example, email spam, which fills the mailbox





https://www.cyberdominance.com/cybersecurity/your-local-supermarket-holds-the-key-to-defending-against-distributed-denial-of-service-attacks/
https://steemit.com/ddos/@clumsysilverdad/dos-and-ddos-attacks

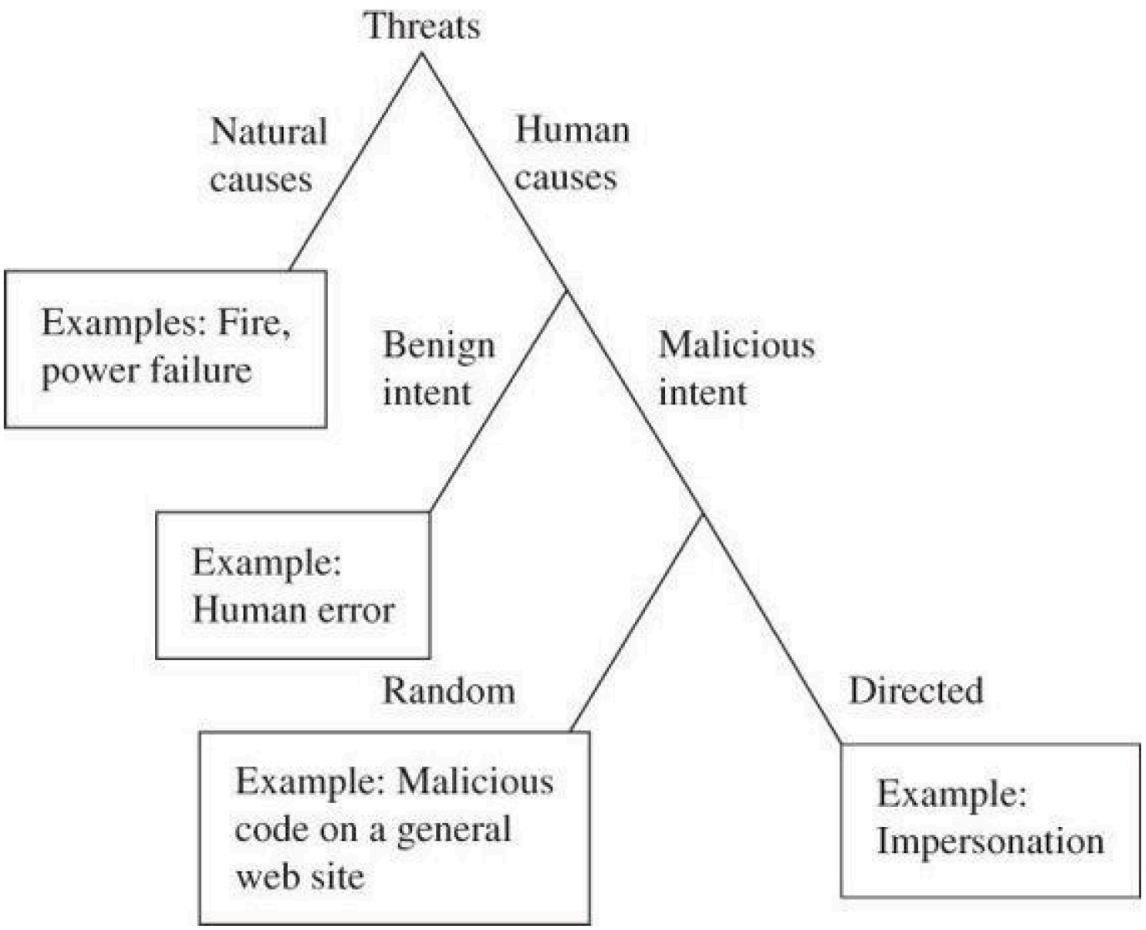
Threats and Attacks (cont.)

- Masquerading: fabrication of information, purported to be from some who is not the actual author
  - For example, phishing and spear-phishing attacks
- Repudiation: denial of commitment or data receipt
  - Attempt to back out of a contract
  - Non-repudiation = assurance that someone can not deny something

Attacks

- Attacks may be random or directed
- In a random attack, the attacker wants to harm any computer or user
- In a directed attack, the attacker intends harm to specific computers

Source of the threat



Advanced Persistent Threat (APT)

- An attack that lasts for a long period of time
  - Organized
  - Directed
  - Well financed
  - Patient
  - Silent

APT

- APT

Types of Attackers

- Individuals
  - Perpetrators of original computer attacks
  - May act with motives of fun, challenge, or revenge
- Organized, Worldwide Groups
  - More recent attacks have involved groups of people
  - heavily influenced by financial gain

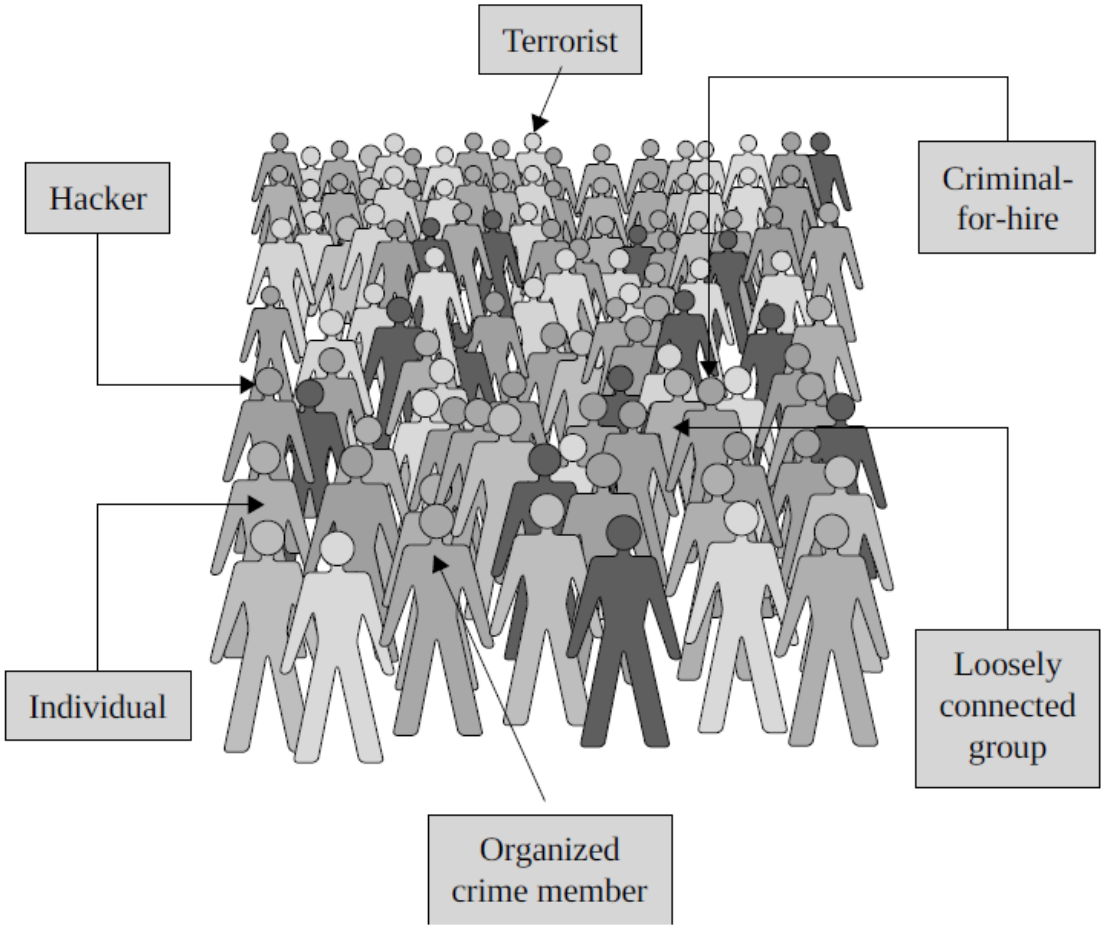
Types of Attackers

- Organized Crime
  - Organized crime groups are discovering that computer crime can be lucrative
    - goals may include fraud, extortion, money laundering, and drug trafficking
  - May use computer crime to finance other crime aspects
    - such as stealing credit card numbers or bank account details

Types of Attackers

- Terrorists may use:
  - Computer as target of attack
    - E.g. Denial of service attacks
  - Computer as method of attack
    - E.g. Stuxnet
  - Computer as enabler of attack
    - Allow people to coordinate through websites
  - Computer as enhancer of attack
    - E.g., recruit terrorists

Who are the attackers?



Vulnerabilities Databases

- http://cve.mitre.org - a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cybersecurity issues.
- https://nvd.nist.gov - the U.S. government repository of standards-based vulnerability management data

How are attacks accomplished?

- Method of attack:
  - a group or individual uses their knowledge of the hardware or software to access the system
  - a group or individual downloads the information needed to access the system
- Opportunity for an attack – unsecured access or data
- Motive – why is the attack occurring

Controls

- A control or countermeasure is a means to counter threats
- What can we do to prevent potential harm?

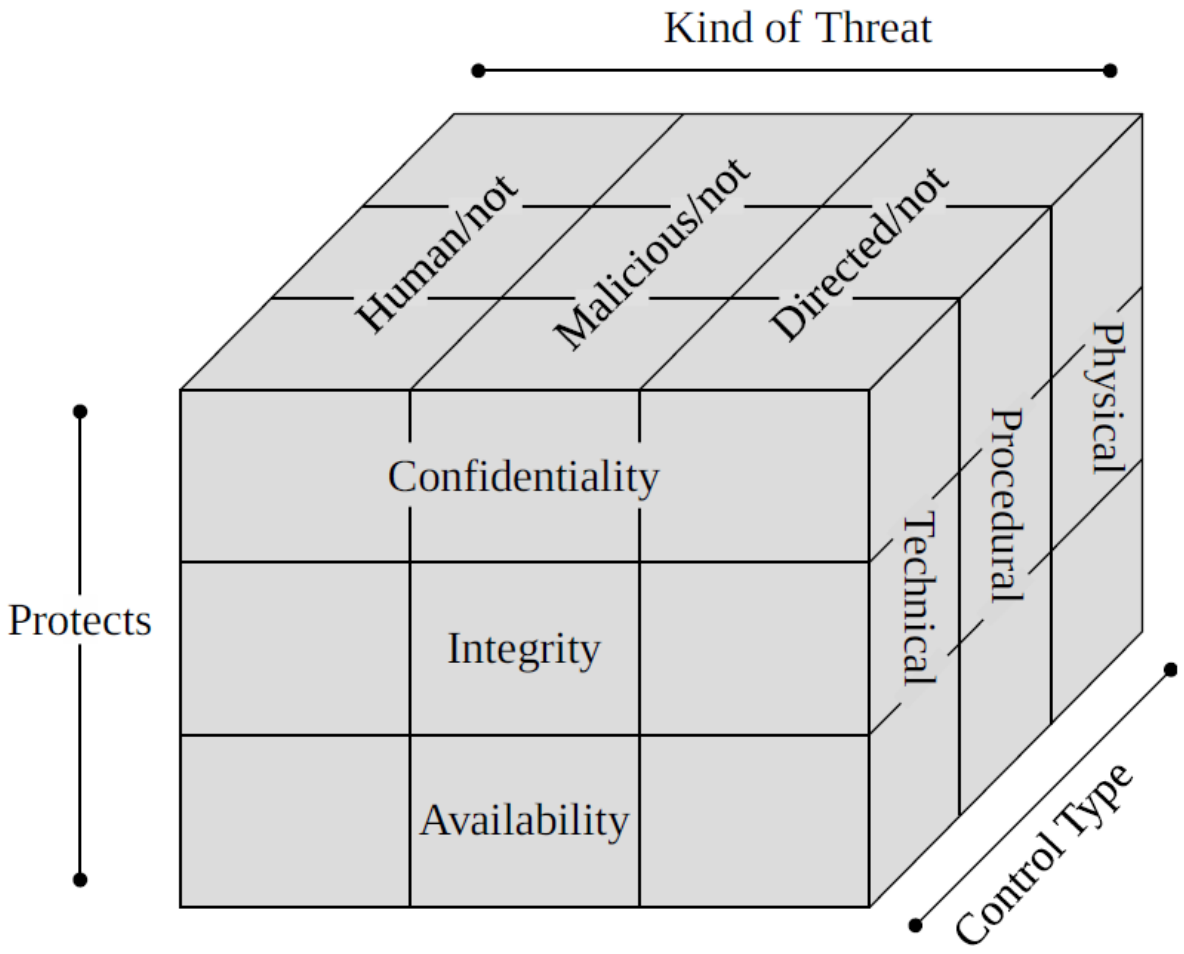
How to prevent or respond to an attack

- Block the attack or remove the vulnerability
- Make the attack harder to accomplish
- Decrease the attractiveness of the target
- Have counter measures that make the attack less severe
- Detect that an attack is in progress and take counter measures
- Have a plan to recover from an attack

Controls

- Physical controls:
  - stop or block an attack by using something tangible
    - such as walls and fences, locks, etc.
- Procedural or administrative controls
  - use a command or agreement that requires or advises people how to act
    - E.g. laws, regulations
- Technical controls counter threats with technology
  - hardware or software
    - E.g. passwords, firewall, encryption

Controls/Countermeasures



Risk Management

- Can not protect against every attack:
  - Decide what is most valuable and analyze how to protect it
  - Estimate how likely an attack is
  - What is the impact of the attack

Risk Management

- High-level goals of computer security:
  - identification, evaluation, prioritization of risks
    - Defined as a threat model
    - Estimate the effects of uncertainty
  - Not perfect protection
  - Efforts concentrate on making it harder to attack
    - Finding ways to spend time & money efficiently
    - minimize the probability or impact of unfortunate events

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

Summary

- 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

Questions?