SECURITY IN COMPUTING, FIFTH EDITION

Review – Introduction to Information Security

CISC 3325 - Information Security

- Tzipora Halevi, Assistant Professor
  email: halevi@cis.brooklyn.cuny.edu
  Office Hours: Mondays, 2:30 - 4:30pm
  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

What Is Computer Security?

- The protection of the assets of a computer system
  - Hardware
  - Software
  - Data
- What is the value of the assets?
  - Is the asset easily replaced?
    - Cost of replacement.
  - Is the asset unique?

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

How can we help?

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

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

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.

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

Computer Security

- 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

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

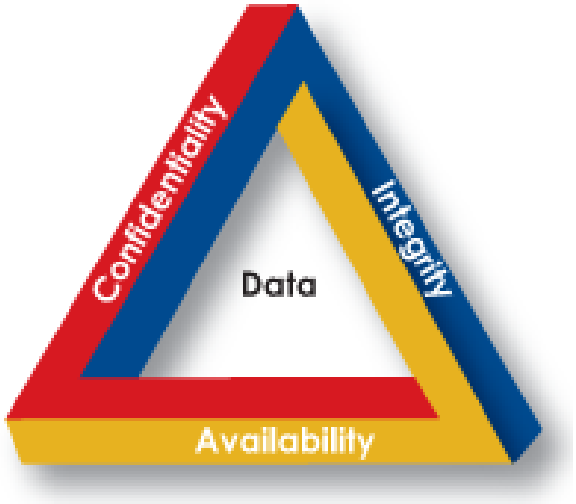
https://nizamtaher.wordpress.com/topics/topic-1-introduction-of-computer-network/

Cyber Vulnerabilities

- **Vulnerability** is a cyber-security term that refers to a flaw in a system that can leave it open to attack.
- A **vulnerability** may also 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/

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

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:
  - Process of confirming 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.

Authentication Vs. Identification

- These are two different concepts
- **Identification:**
  - **T**he act of asserting who a person is.
- **Authentication**
  - **T**he act of proving that asserted identity that the person is who she says she is

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
- 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

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
- 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
- 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

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 - Summary

- Sometimes two other desirable characteristics:
  - Authentication:
    - 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

Types of threats

- Interception
  - the asset or data is accessed by someone other than the intended receiver
- Interruption
  - the asset or data is not available
- Modification
  - an unauthorized change is made
- Fabrication
  - false information is installed

Types of Threads vs. CIA Triad

- Interception:
  - Threat to confidentiality
    - Attacker can see data
- Interruption
  - Threat to availability
- Modification and fabrication
  - Threat to data integrity

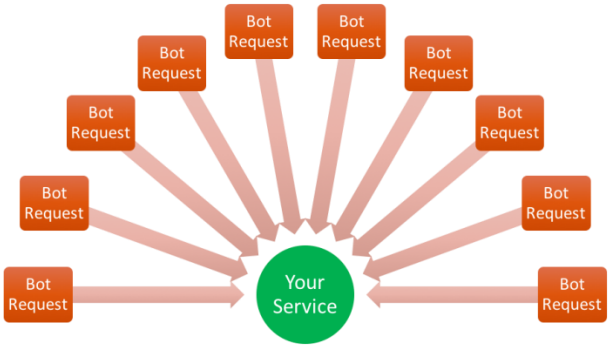
Threats and Attacks

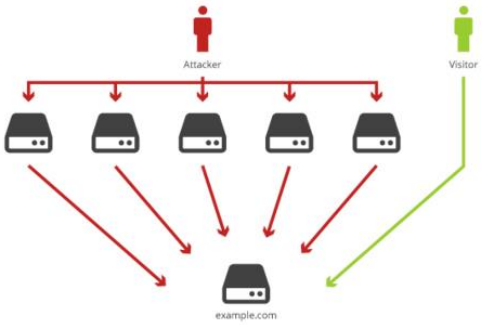
- Eavesdropping: interception of information during transmission
  - Includes side channel attacks
  - May be audio, electromagnetic, power, etc.
- Alteration: unauthorized modification of information
  - False information may be installed

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



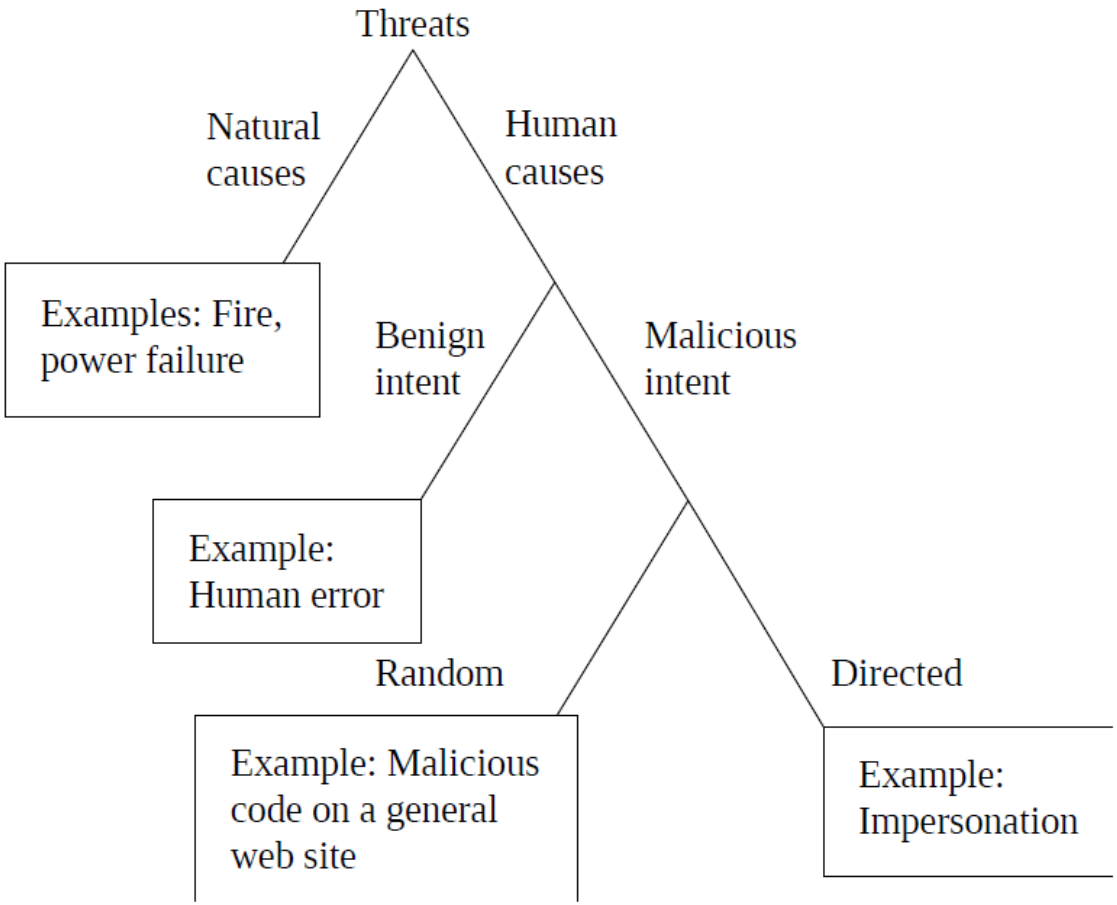


https://www.cyberdominance.com/cybersecurity/your-local-supermarket-holds-the-key-to-defending-against-distributed-denial-of-service-attacks/
https://steemit.com/ddos/@clumsysilverdad/dos-and-ddos-attacks

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

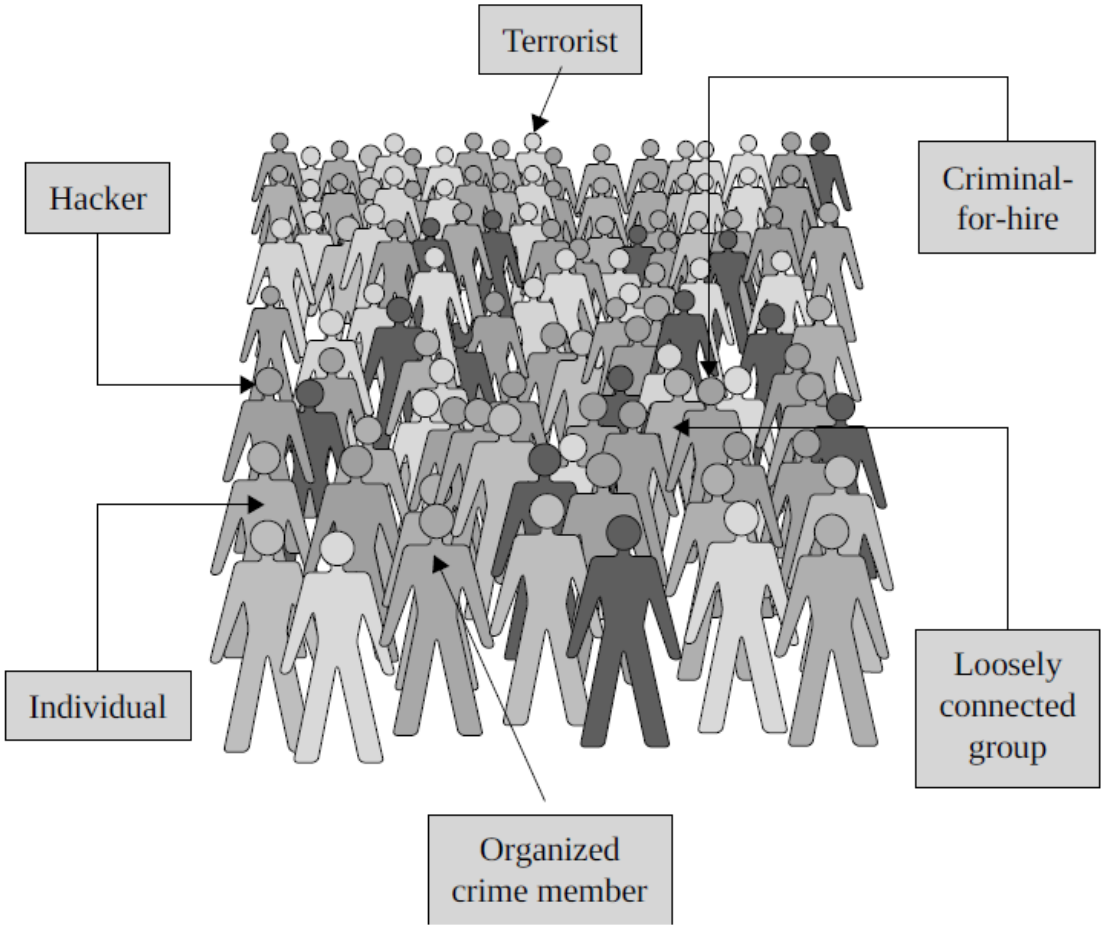
Source of the threat



Advanced Persistent Threat (APT)

- Attacks by a collection of attackers
- Organized, well financed, patient assailants
  - Often affiliated with governments or quasi-governmental groups
- Engage in long term campaigns
- Carefully select their targets, crafting attacks that appeal to specifically those targets

Who are the attackers?



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).

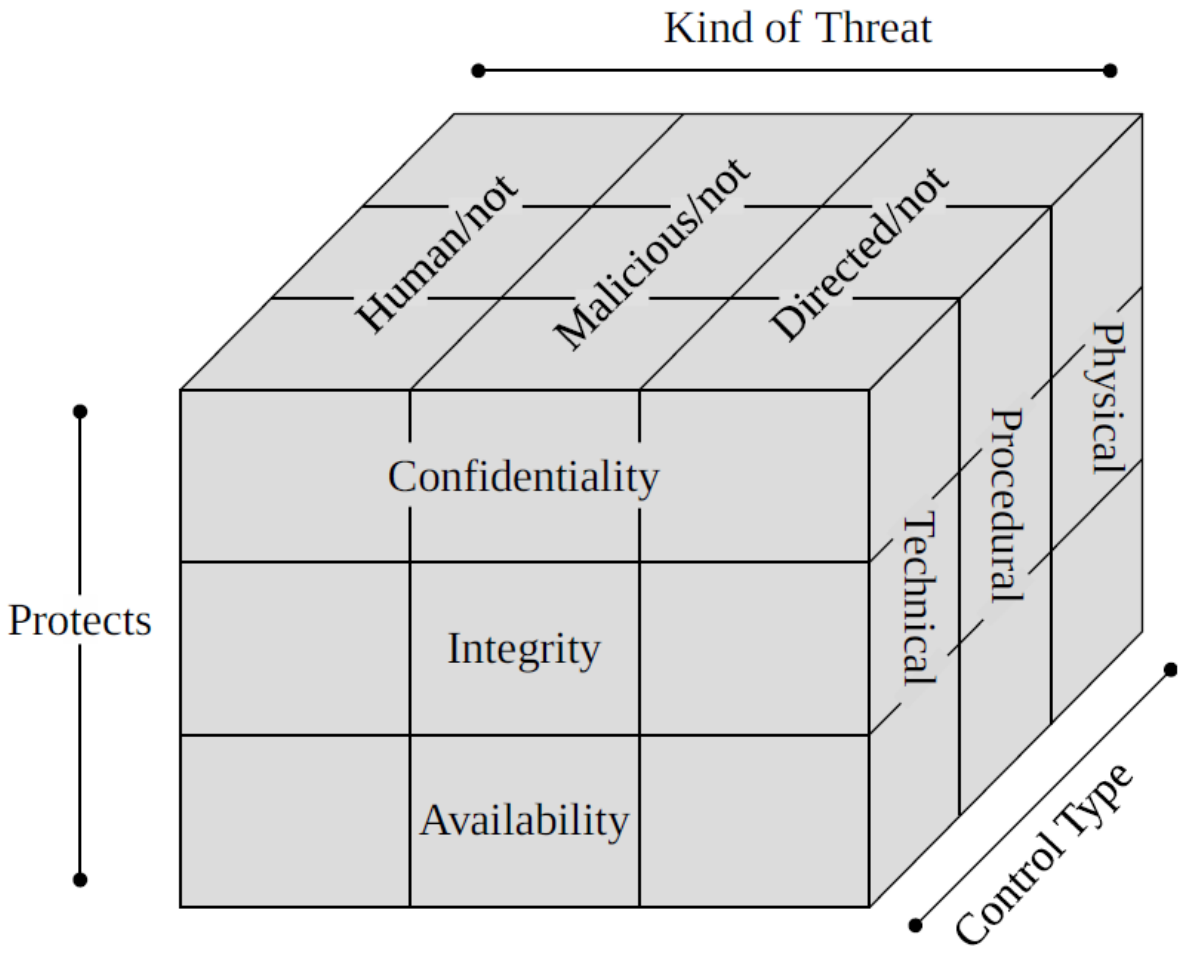
Vulnerabilities Databases

- 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/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

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

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

Questions?