PRIVACY, SECURITY AND USABILITY

Security

Topics for today

- What is computer security? Why should we care about security?
- Threat models
- Performing security analysis
- Encryption basics

What is cyber-security?

- Also referred to as computer-security or IT security
- Allow intended use of computer systems
  - hardware, software or information stored
- Prevent unwanted use that may cause harm
  - Protect from theft, damage, disruption, etc.

What is Computer Security?

- Traditionally, computers are protected against:
  - Prevent theft/damage to hardware
  - Prevent theft/damage to information
  - Prevent disruption of service

Growing Importance of Computer Security

- Increasing reliance on computer systems and the Internet
- 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

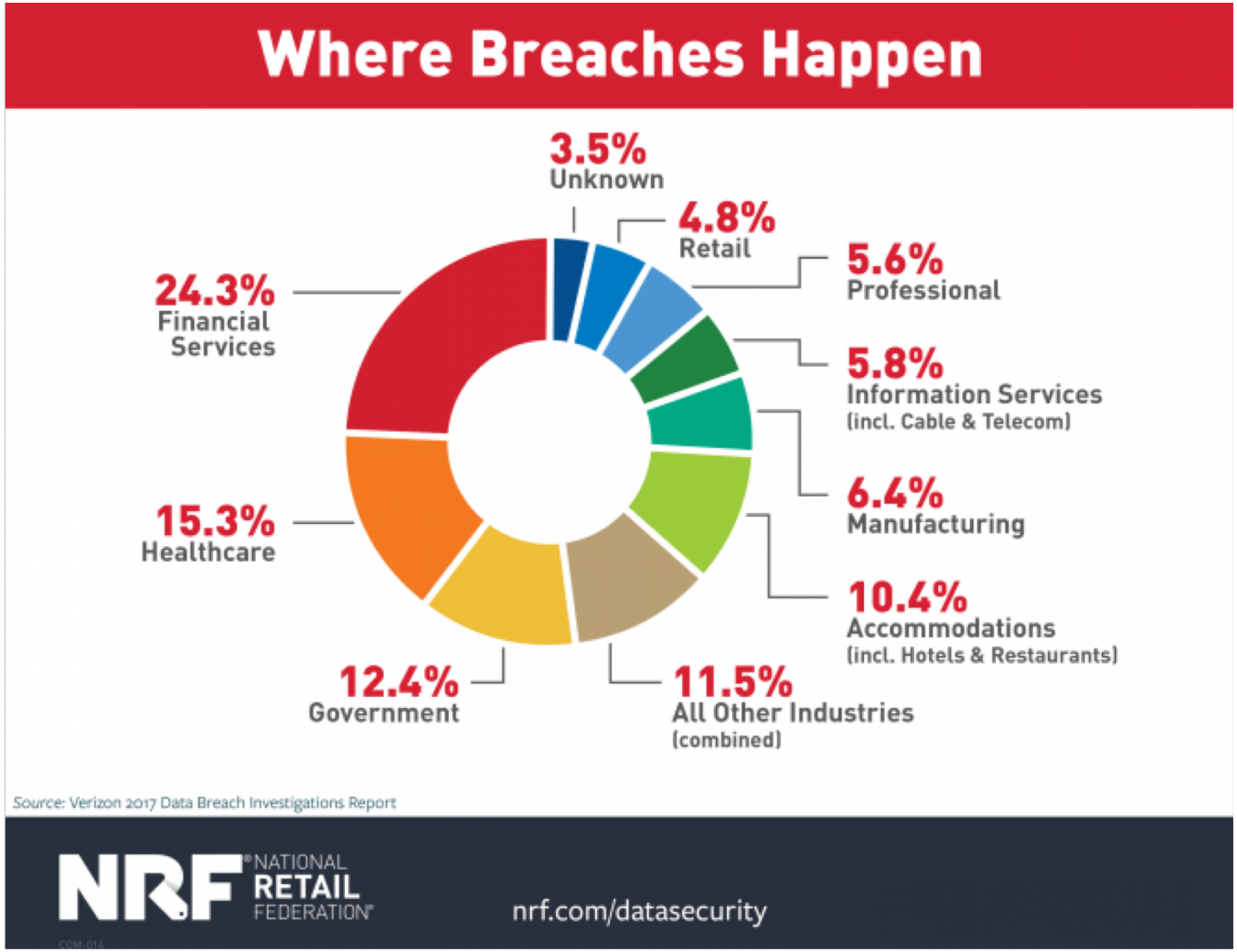
MORE LIKE THIS

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

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

- 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

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?

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

Privacy, Confidentiality and Anonymity

- What is the difference between them?
  - **Privacy** refers to the right of an individual to keep his or her information private
  - **Confidentiality** refers to the duty of anyone entrusted with health information to keep that information private
  - **Anonymity** refers to security of identity: the quality or state of being anonymous (unknown)

Secrecy vs. Confidentiality

- Secrecy:
  - User keeps its data secret
    - i.e., keeps past mistakes a secret
- Confidentiality
  - Keep access to another's user's data hidden from unauthorized users
    - E.g., credit entities should keep user's credit score secret

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

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/

Threats, Attacks and Controls

- A ***threat*** to a computing system is a set of circumstances that has the potential to cause loss or harm
- 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***

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

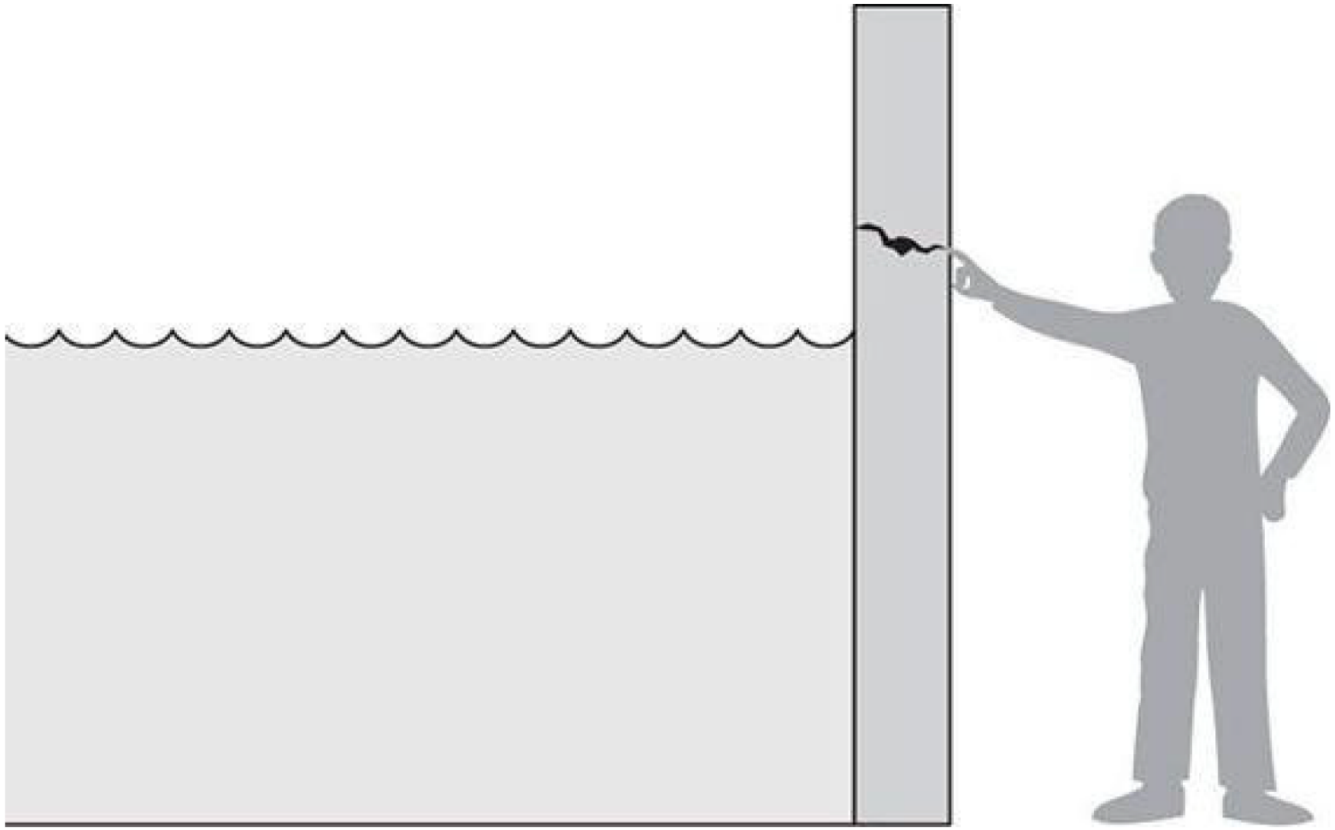


FIGURE 1-4 Threat and Vulnerability

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

Threat Model

- What are we protecting?
  - What is the assets value?
  - where are valuable assets stored, where is the system most vulnerable to attacks, etc.
  - What is the operating value? What would losing the resources cost (per day/total)?
    - Business cost may be large
    - Some attacks meant to disrupt business, done for fun/fame

Threat Model

- What are the security requirements?
  - Confidentiality
  - Integrity
  - Availability
  - Access control
  - Privacy
  - Authenticity
  - Anonymity
  - Auditability
  - Other?

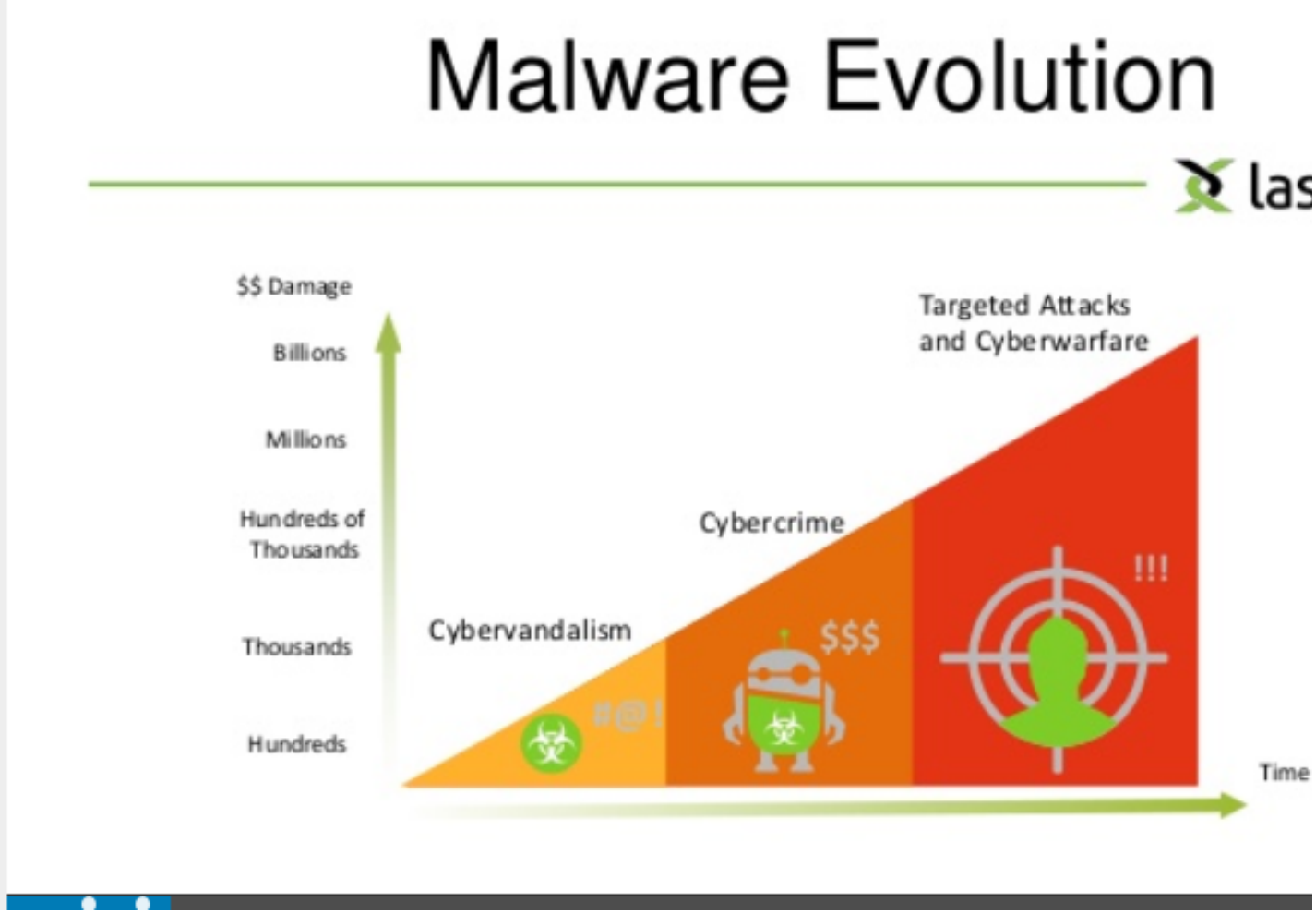
SECURITY THREATS

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

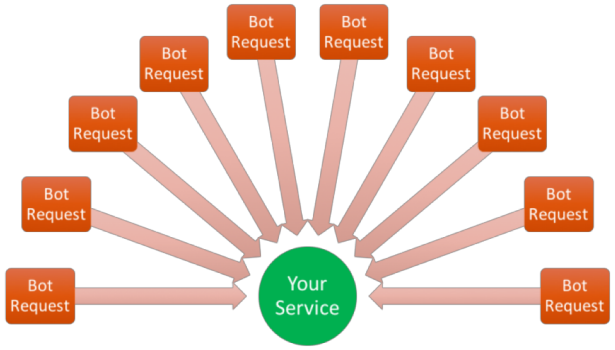
Threats and Attacks

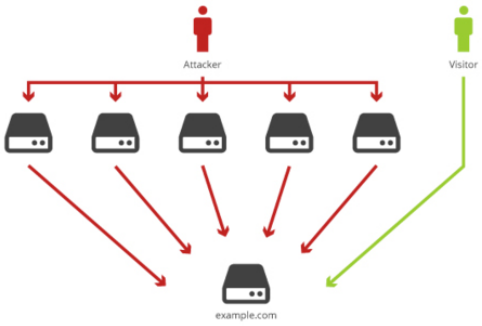
- Eavesdropping: interception of information during transmission
  - Includes side channel attacks
  - May be audio, electromagnetic, power, etc.
- Alteration: unauthorized modification of information

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

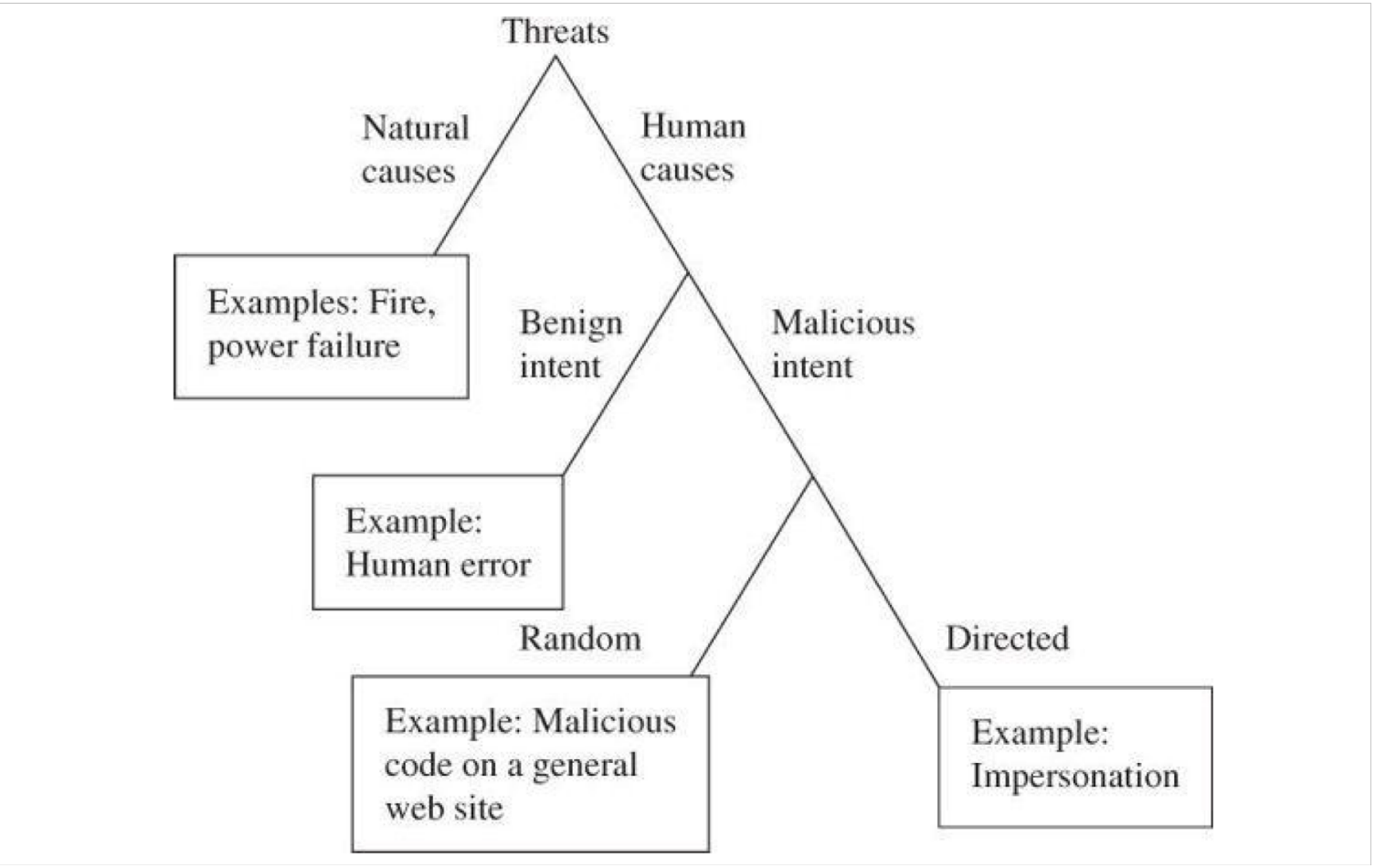
Threats and Attacks (cont.)

- 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

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

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

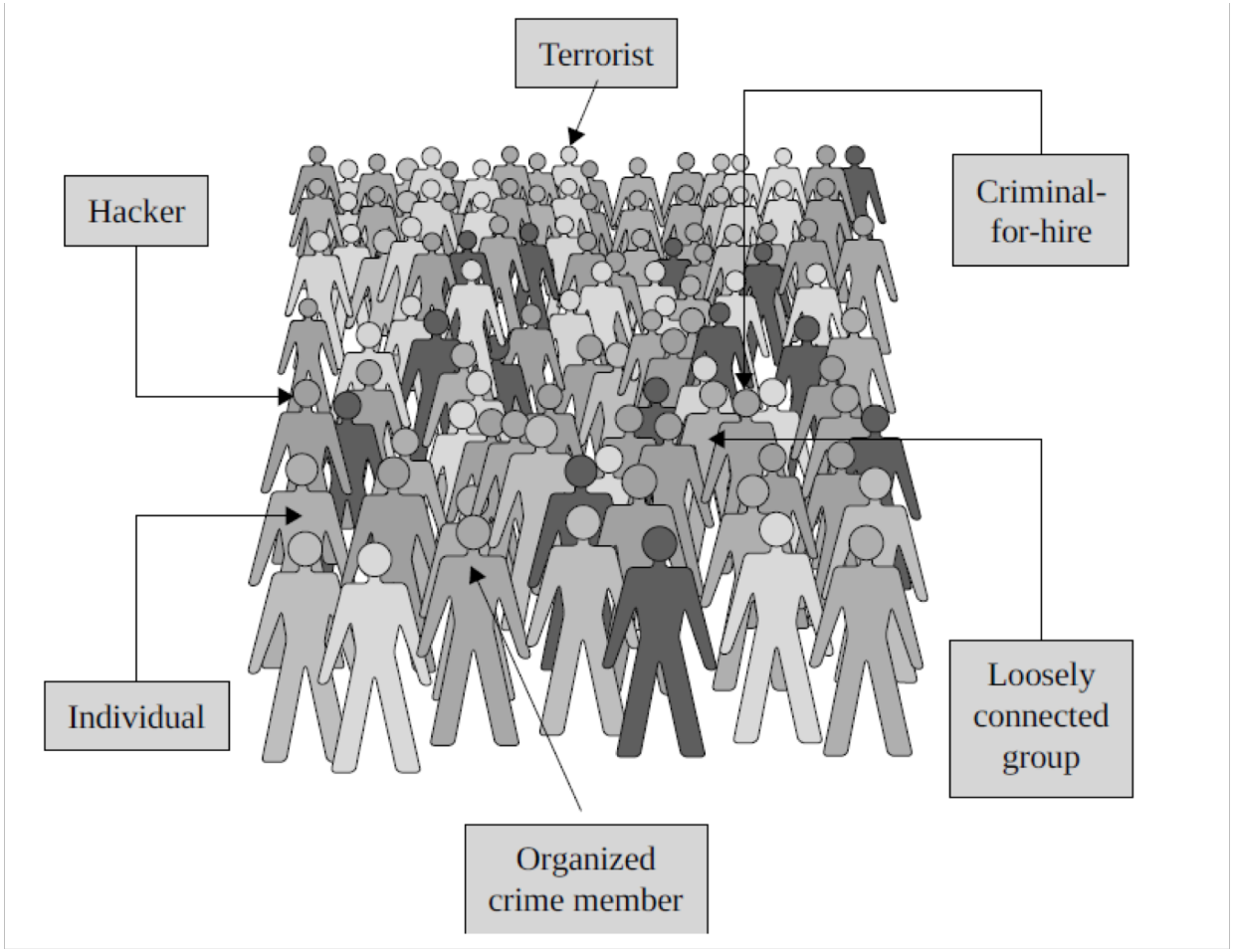
Types of Attackers

- 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?



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

Attacker Capabilities

- Passive vs. Active Attackers
  - Eavesdropping vs. tempering with transmitted data
- Attacker resources
  - Individual/organized/government sponsored
- Access
  - External attacker has no access to resources
    - Cryptographic keys
    - Needs to penetrate network without detection
  - Internal attacker
    - Has access to cryptographic, internal network

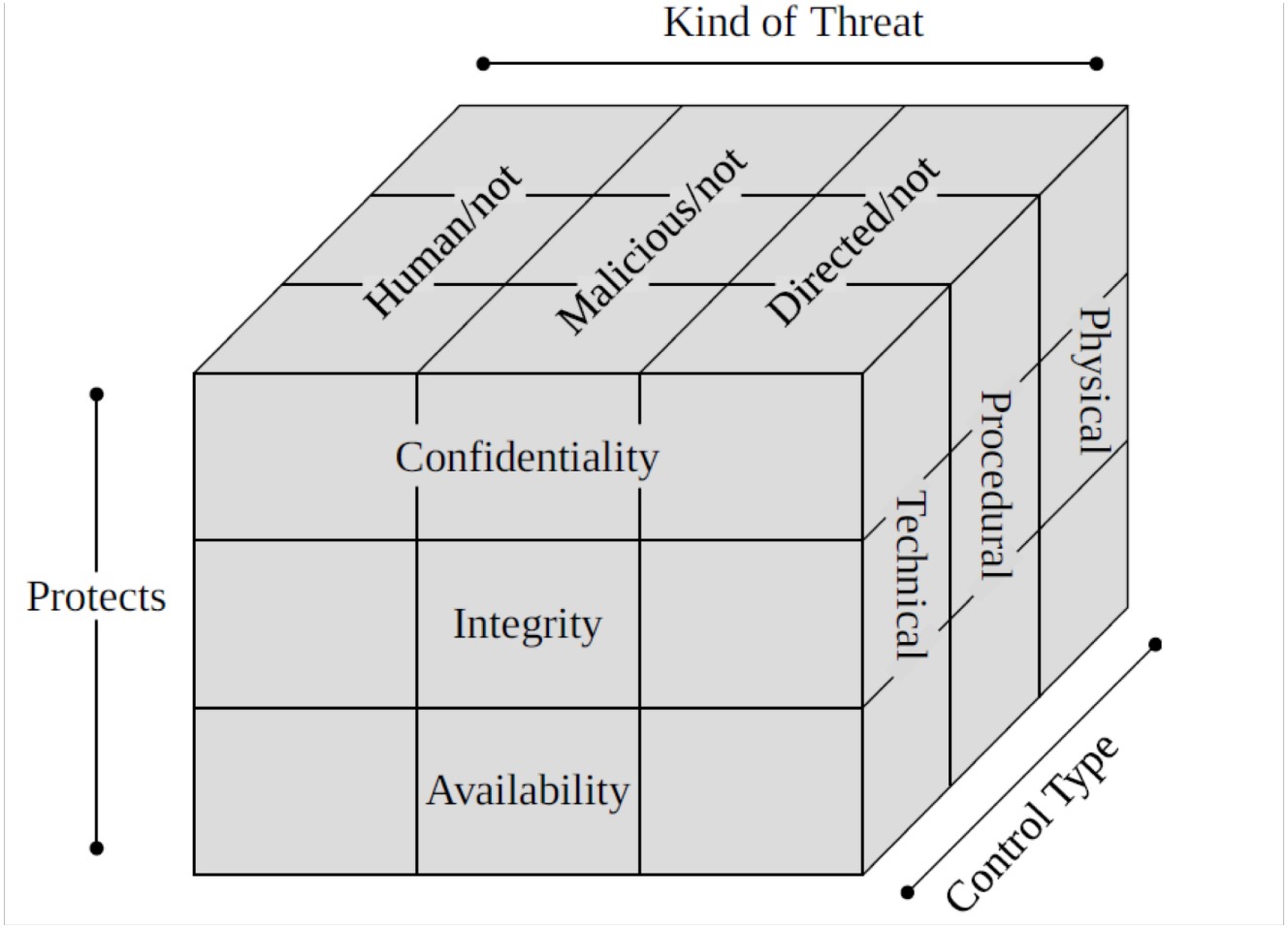
Controls

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

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



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

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

Real-World Security Approaches

- Legal protections
  - Deter the attacker
    - May replace some security measurements
- Implement security measures
  - Use Cryptography, VPN, firewalls
- Protect availability through redundancy
  - Multiple servers, duplicate data storage centers
- Detection and recovery
  - Trained security experts, intrusion detection system

Implementing Security

- Think like an attacker
  - Adversary is targeting assets, data
    - Not defenses
  - Will try to attack weakest part of the system
    - Use social engineering techniques, etc.

What was the asset protected?

https://ggwash.org/view/69989/heres-what-happens-when-your-bicycle-is-stolen-dc

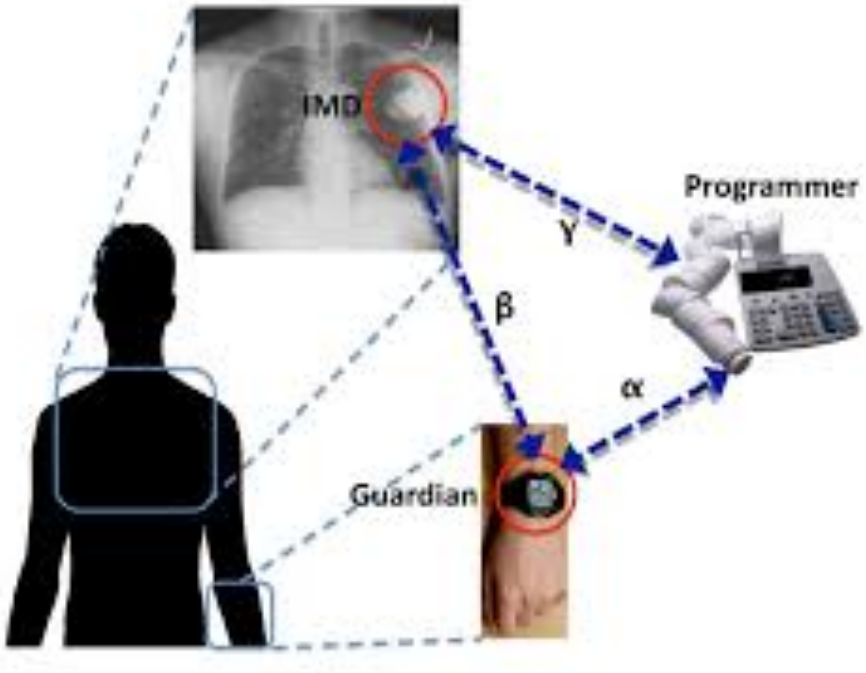
https://oaksandspokes.com/how-to-lock/

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

Questions?

Case Study: Implantable Medical Devices



http://www.cs.wm.edu/~liqun/paper/infocom11_1.pdf

Case Study: Implantable Medical Devices

- Pacemakers and cardiac defibrillators
- Functionality:
  - Collect patient diagnostic and medical information
    - Stores patient data
    - May be transmitted to doctor through phone or computer
    - Access needed to info in emergency situation
  - Perform medical functions
    - Regulates heart function
    - May send strong electrical signals when needed
      - To revive patient

Case Study: Implantable Medical Devices

- Security concerns?
  - What if valid user can not access device
    - Attack on Availability
  - What if an attacker gains access
    - Can kill patient
      - Attack on Integrity
  - What if device battery runs out of power?
    - Attack on availability
    - Security solutions need to be efficient

IMPLEMENTATION AND USABILITY ISSUES

https://ebiinterfaces.wordpress.com/2012/08/03/lightbulb-tactics-dealing-with-usability-issues-that-dont-get-fixed/
http://www.usefulusability.com/usability-is-in-the-details/

Efficiency and Usability

- Computer security solutions should be efficient
  - Users don’t like and won’t use slow systems
- Usability issues may cause user errors
  - Increased cognitive load, time-on task
  - Will not cause task to fail
    - Therefore, usability needs to be analyzed separately
  - Human factor should be considered when designing security solutions!

Passwords

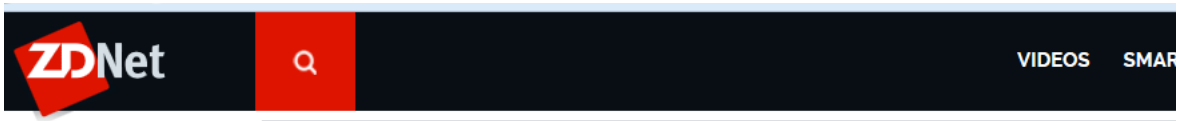
- Passwords are a common means of authentication
  - Even systems with biometrics and physical tokens often combine them with passwords
- Vulnerable to dictionary attacks, peeking, guessing
  - Passwords that use random numbers and letters are typically stronger

Secure Passwords

- Case study: Ashley Madison hack
- 36 million hashed passwords leaked
  - Researchers cracked passwords
    - Using automated guessing, other attacks
    - Easier passwords easier to crack

Secure Passwords

- Ashley Madison Attack - most common passwords guessed:



Password	Times used
123456	120,511
12345	48,452
password	39,448
default	34,275
123456789	26,620
qwerty	20,778
12345678	14,172
abc123	10,869

http://www.zdnet.com/article/these-are-the-top-100-passwords-from-the-ashley-madison-hack/

Secure Passwords

- Conclusions:
  - Weak passwords easier to guess
    - Vulnerable even when hashed
  - Many passwords can be guessed
    - by exploiting the predictability in the way most end users choose passwords
  - Password cracking tools significantly improved

http://www.enterprisefeatures.com/secure-passwords-a-cautionary-tale/

Secure Passwords

- Passwords are still most common login authentication mechanism
- Should be strong and hard to guess
- User needs a way to remember them
  - Writing them on a sticky note on a computer is not secure!
- Should not be reused
- Should be changed every so often

http://www.enterprisefeatures.com/secure-passwords-a-cautionary-tale/

Social Engineering

- Using trickery to extract information from users
- Phishing and spear-phishing are such attacks

https://thedcoder.info/introduction-to-social-engineering/

Summary

- Security is important
  - May be difficult to achieve
- Tradeoffs need to be considered
  - Security, privacy and usability
- Security is about managing risk
  - Not achieving perfection
  - Optimize cost and resources
    - Based on threat analysis

Questions?