Cybersecurity

Allie Sauppé | CS4HS

February 11, 2017

cybersecurity: “a computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries.” (*ACM Joint Task Force on Cybersecurity Education*)

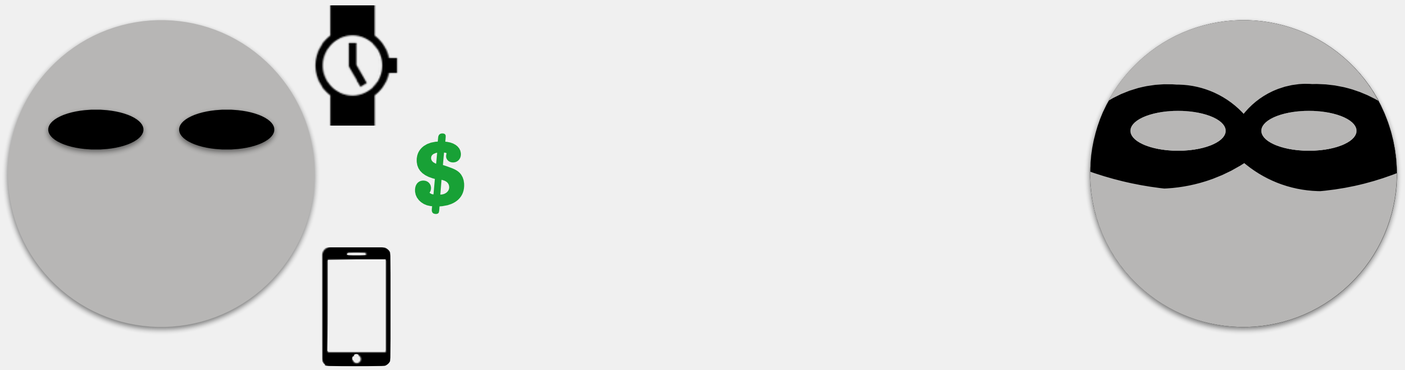
cybersecurity: "a computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves **the creation, operation, analysis, and testing of secure computer systems.** It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries." (*ACM Joint Task Force on Cybersecurity Education*)

cybersecurity: "a computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries." (*ACM Joint Task Force on Cybersecurity Education*)

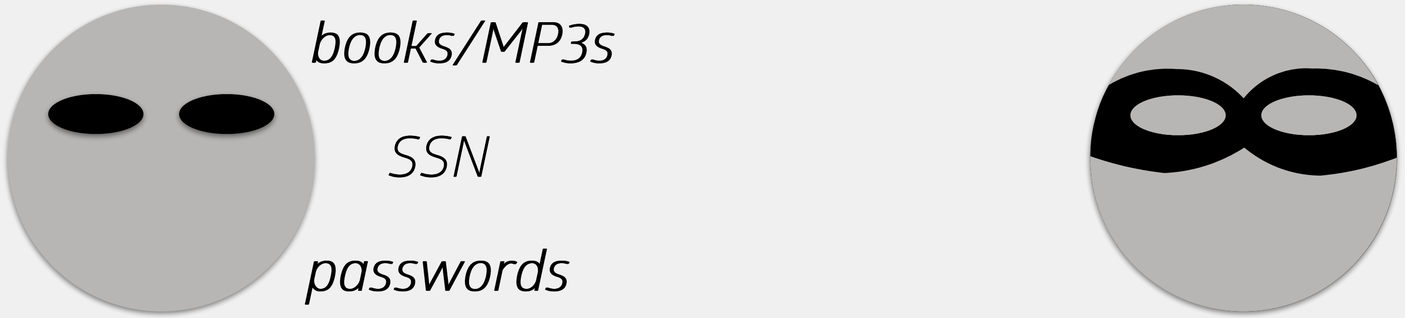
cybersecurity: "a computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of **law, policy, human factors, ethics, and risk management in the context of adversaries.**" (*ACM Joint Task Force on Cybersecurity Education*)

Ownership of Digital Information

With physical assets, stealing transfers ownership



With digital assets, stealing increases ownership



Ownership is now about **controlling**
who has access to **information**.

What Is Security?

1. Confidentiality
2. Availability
3. Integrity

What Is Security?

1. Confidentiality

    information must be properly restricted

    i.e., only available to particular people on particular devices

2. Availability

3. Integrity

What Is Security?

1. Confidentiality
2. Availability

    information must be available to be secure

    typically equates to knowledge of location and authentication

    e.g., know where your have placed an encrypted drive, and how to decrypt it

3. Integrity

What Is Security?

1. Confidentiality
2. Availability
3. Integrity

   ensures information is reliable and trustworthy

   data integrity: information has not been altered from its original value

   owner integrity: ownership is correctly identified (i.e., authentication)

Ownership

Does ownership still have meaning when...

- data can easily be replicated?
- data can exist anonymously?

What is ownership in the age of information?

Data cannot have integrity without ownership

Therefore, security depends on identifying one or more owners

- user IDs
- email addresses
- phone numbers

Cybersecurity in High School Curricula

“Ethical and social issues in computing, and careers in computing, are woven throughout the six units. ... Students study the responsibilities of software users and software developers with respect to intellectual property rights, software failures, and the piracy of software and other digital media.” - ECS[1]

“How is cybersecurity impacting the ever-increasing number of internet users?” - AP CSP[2]

1: http://www.exploringcs.org/curriculum

2: https://secure-media.collegeboard.org/digitalServices/pdf/ap/ap-computer-science-principles-course-and-exam-description.pdf

Outline

Trust and the internet

Cyberattacks

Multiple factors (e.g., hardware, software, human behavior)

Encryption

Outline

Trust and the internet

Cyberattacks

Multiple factors (e.g., hardware, software, human behavior)

Encryption

What Is Trust?

The internet is built on trust

- users and service providers
- users and online applications
- users and other users

User’s perspective: trusting others with your data, making decisions with your data

Illusion of Security

Guaranteed security cannot be achieved

Often talk about minimizing risk in proportion to the information

- cost of attacking the system is greater than the resources contained therein
  - e.g., attacking $100 worth of information using $200 worth of hacking resources
- time to attack the system is longer than the length of time resource has value
  - do not need to protect some types of information after an event has taken place/the information has expired
  - e.g., if a resource is only valuable for 24 hours, ensure it will likely take longer than 24 hours to breach the system

Outline

Trust and the internet

Cyberattacks

Multiple factors (e.g., hardware, software, human behavior)

Encryption

Cybercrime

cybercrime: internet security attacks

- *black hats*: individuals who act as attackers against assets
- *white hats*: individuals who work to protect assets
- Cybercrime is perpetuated by black hats, prevented by white hats

Black hats have several advantages

- they can ignore the rules/laws; white hats must obey laws
- they can choose which vulnerabilities to exploit; white hats must protect them all
- they can conduct attacks on their own time; white hats don’t know when attacks will occur
- they can invent new attacks; white hats protect against previously used methods

Cybercrime Exploits

Many different types of exploits

Often rely on malicious software

- commonly known as *malware*

https://www.youtube.com/watch?v=sxLtKyJM2vM

Computer Virus

Infects a computer with undesirable software

Can have a number of side effects

- display ads that, when clicked, send sensitive information
- prevent access to the internet
- sends keystrokes (e.g., passwords, usernames, credit card info)
- erases the entire hard drive

Spoofing

Falsifies identity of email sender, network packet owner

Violates owner integrity

Unwitting users might accidentally reveal sensitive information to third-party sources

Network Sniffing

network sniffer: program that captures network information, sends to attacker

Attacker will know a user's internet habits, potentially some information

- not all information is encrypted when sent over a network
- can often be easily decoded by attackers

Denial-of-Service (DoS) Attacks

Denies one or more users access to an online service

- e.g., send many emails with large attachments such that a user can no longer receive email

Larger attacks aim to bring down popular websites

- distributed denial-of-service (DDoS)

Controls the ability to access information

Outline

Trust and the internet

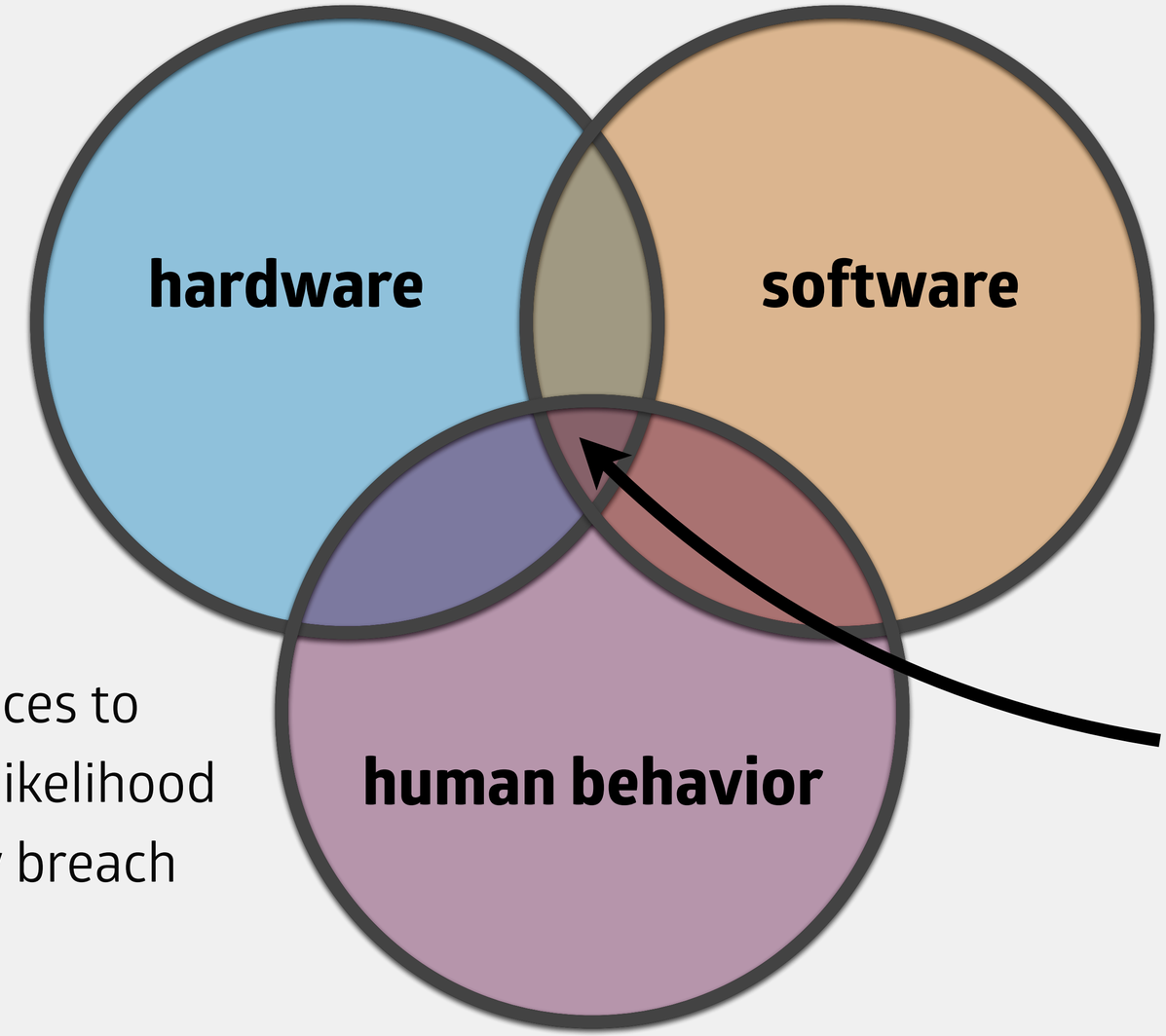
Cyberattacks

Multiple factors (e.g., hardware, software, human behavior)

Encryption

Multiple Factors

protection of the physical devices housing digital data

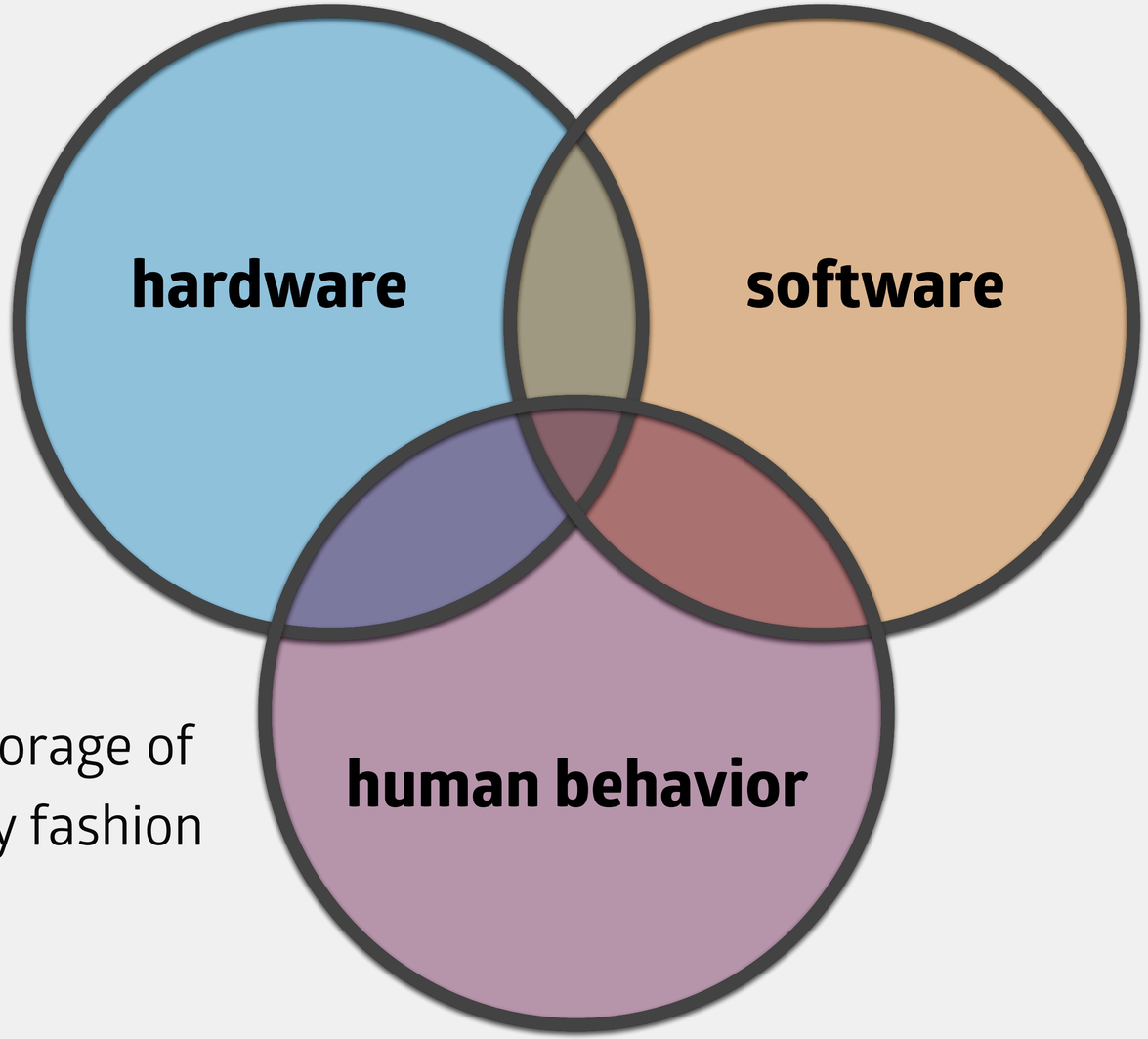


digital safeguards against malicious users or software

best practices to decrease the likelihood of a security breach

Example: Multiple Factors

hard drive is stored in a room only authorized people have keys to

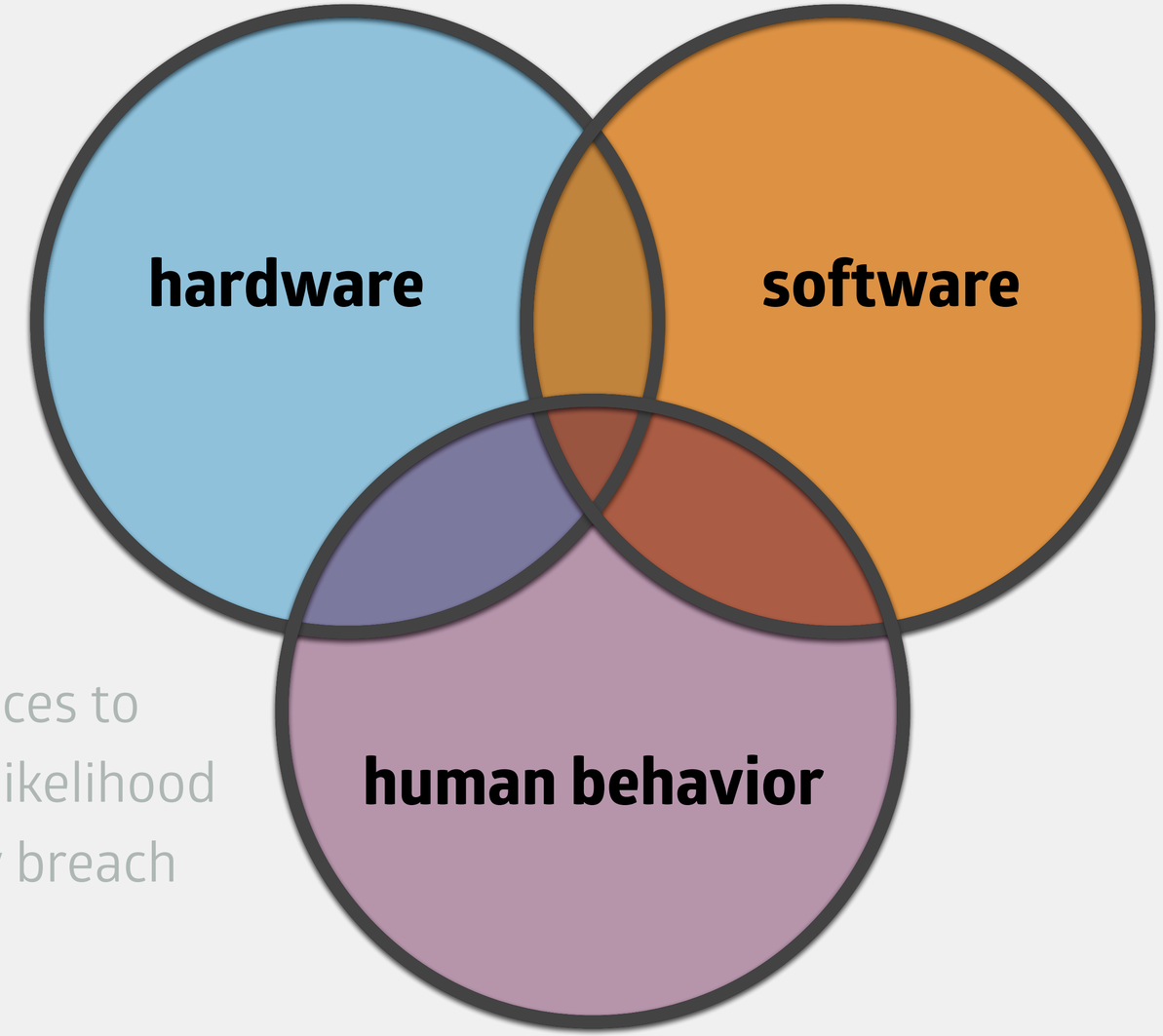


the hard drive is encrypted

protocol for storage of data in a timely fashion

Multiple Factors

protection of the physical devices housing digital data



digital safeguards against malicious users or software

best practices to decrease the likelihood of a security breach

Firewalls

Networked computers provide numerous vulnerabilities

firewall: filters network traffic content to attempt to block spam/malware

Many modern computers have this built into the operating system to scan all network traffic

Anti-Virus Software

anti-virus software: protects against computer viruses and other malware

Used to detect and attempt to remove malware

- not always successful

Needs to be kept up to date for new threats

Software Updates

All reasonably large software contains vulnerabilities

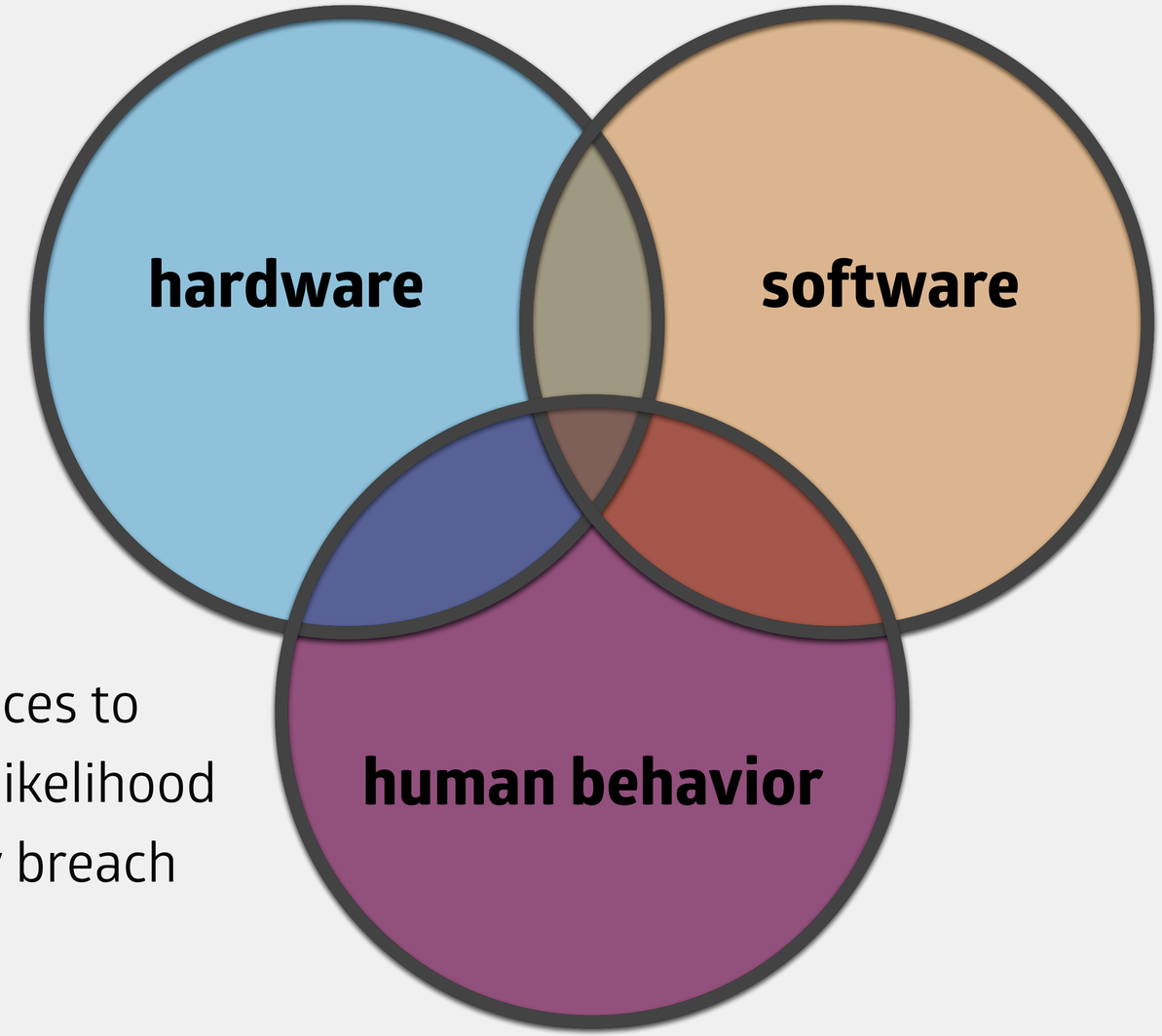
- many of these vulnerabilities pose security risks
- the larger the software, the more vulnerabilities

Operating systems are a prime source of vulnerabilities

- require frequent *software updates* to protect/patch against these vulnerabilities

Multiple Factors

protection of the physical devices housing digital data



digital safeguards against malicious users or software

best practices to decrease the likelihood of a security breach

Empowering Users

Security requires balancing ease of use and difficulty to access

- users tend to prefer ease of use

Need to be educated on best practices

- never write down passwords
- connect only to trusted networks
- provide protocols for handling information
- enforce a need-to-know policy

How to Secure

Two steps to (greater) security

1. authenticate
2. authorization

Remember, we can’t guarantee security!

Step 1: Authentication

authenticate: to verify identity the identity of the *subject* (person, process, device)

Four ways to authenticate

1. something the subject knows

    e.g., a password, secret handshake

2. something the subject possesses

    e.g., a physical key, credit card

3. something the subject is

    e.g., their identity (biometrics), a classification associated with their identity

4. somewhere the subject is located

    e.g., computers located on UWL's network

Two-Factor Authentication

One type of authentication is fairly strong (particularly the first three types)

two-factor authentication: using two forms of authentication together

Examples

- credit card + pin number
- account password + pin sent via text message
- login password + thumbprint scanner

Step 2: Authorization

Requires identity authentication first

authorization: verifies the privileges granted to this identity

Four main classes of authorization with digital data

1. **read**: can view a document
2. **write**: can make changes to the document
3. **own**: can rename, delete, changes other users' access to document (limited to one user)
4. **execute**: can run a program

Different users have different authentications

Outline

Trust and the internet

Cyberattacks

Multiple factors (e.g., hardware, software, human behavior)

Encryption

Encryption

Textual data uses a universal encoding

- makes it easy for others to intercept, read your data
- true for other types of data as well

encryption: conversion of data into a form that cannot be easily read

- essentially, scrambling data
- should allow access to those who are authorized to read the data

Encryption Terms

ciphertext: the encrypted form of the data

one-way encryption: a form of encryption where data can be encrypted, but not decrypted

two-way encryption: a form of encryption where data can be both encrypted and decrypted

key: a password for accessing encrypted data

One-way Encryption

What use is encrypting data if we can't decrypt it?

Used for storing passwords on computers

nearly impossible for anyone to decrypt what the password is

`someRandomPwd!` → `#Jenh4$hSjP2ns` →

user chooses password

encryption algorithm

User	Password
Allie	`#Jenh4$hSjP2ns`

One-way Encryption

What use is encrypting data if we can't decrypt it?

Used for storing passwords on computers

nearly impossible for anyone to decrypt what the password is

One-way Encryption

What use is encrypting data if we can't decrypt it?

Used for storing passwords on computers

nearly impossible for anyone to decrypt what the password is

Two-way Encryption

Used for storing/sending data in a secure fashion

- enables both encryption and decryption

public key encryption: involves two keys for encrypting and decrypting data

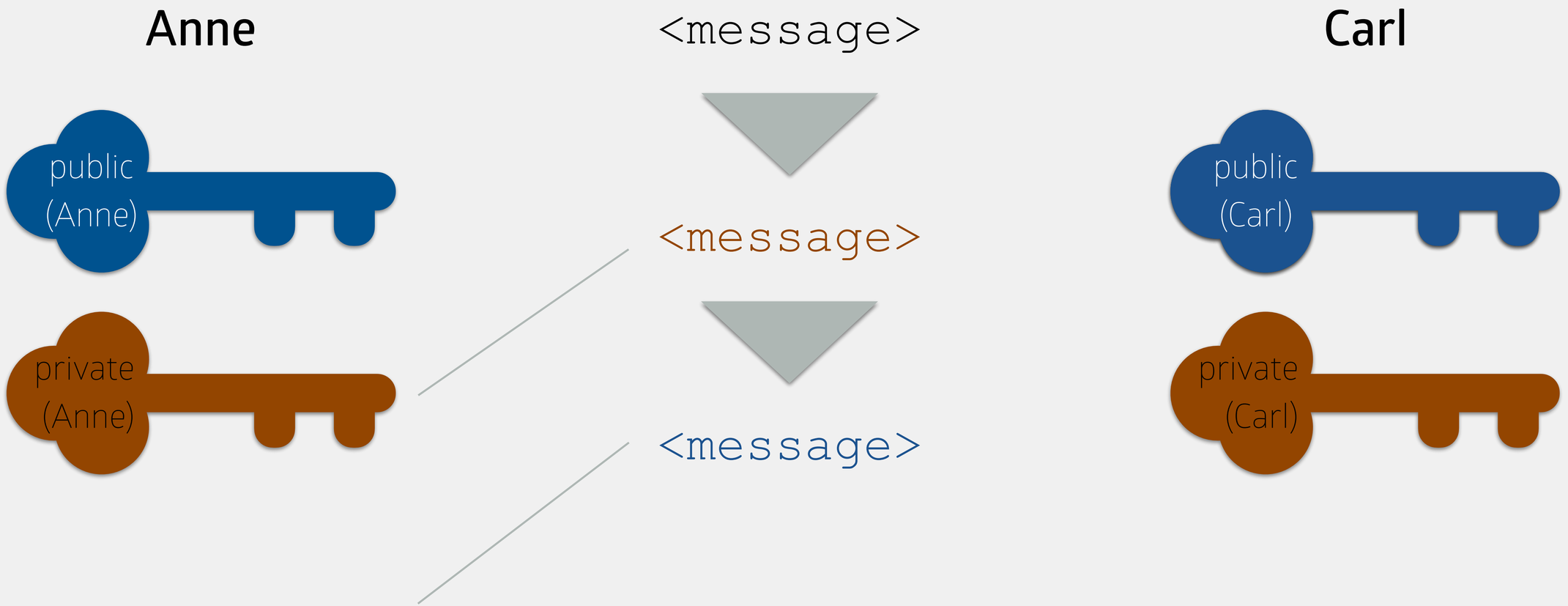
- need a *public* and *private* key
- every person has both
- give out public keys to anyone, keep private keys private

Public/private keys work together

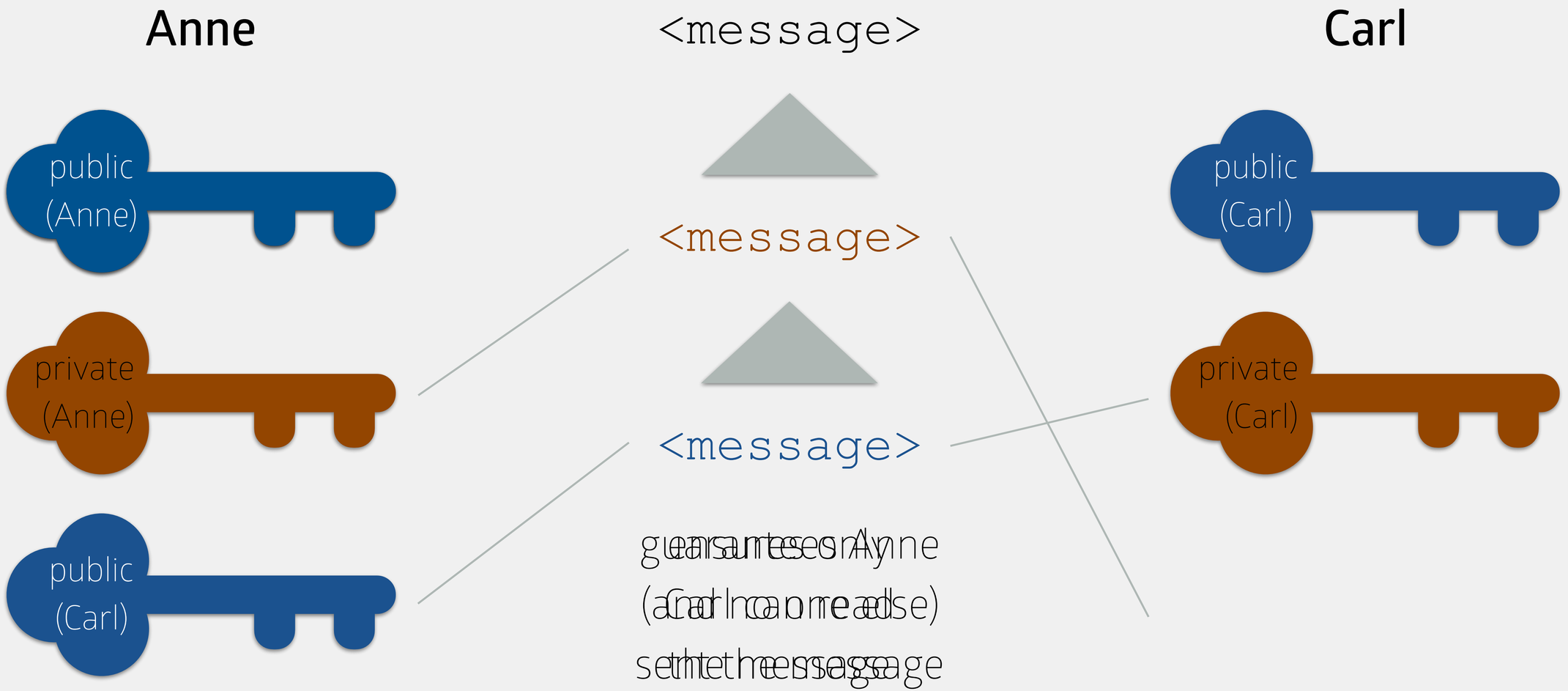
- each key can decrypt the other

Public Key Encryption

Public Key Encryption



Public Key Encryption



Two-way Encryption

Allows us to guarantee two things:

- only the person we intend to read the data can read it
- allows the person who is reading the data to know who sent it

Encounters problems when we want to share with more than one person

- would need to encrypt each file separately

Key Takeaways

Computers have changed how we view security

Trust is a key factor that should not be taken lightly

Numerous exploits deal with copying info. or removing access to info.

Effective cybersecurity requires coordination of multiple factors

Encryption is a popular software technique for improving security