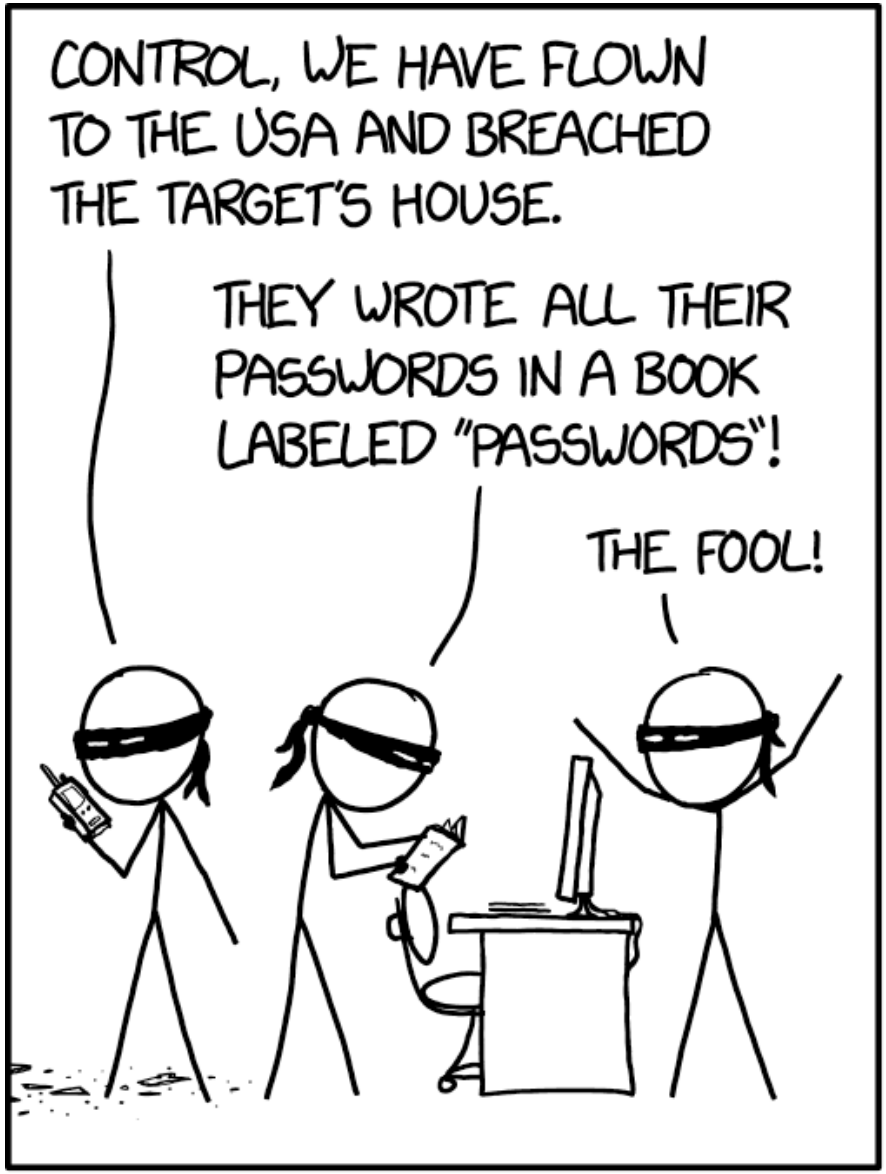
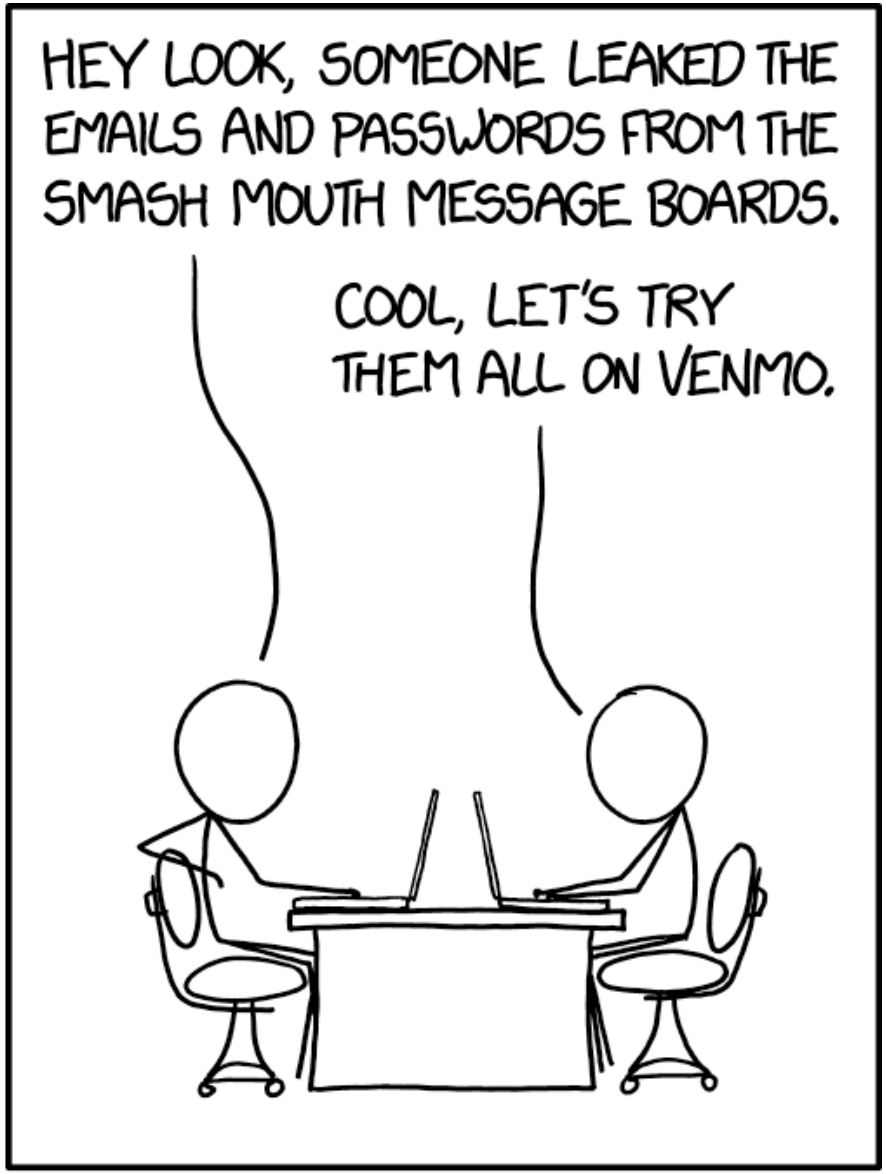
CS 55:
Security and Privacy

Who is the adversary?



HOW PEOPLE THINK HACKING WORKS



HOW IT ACTUALLY WORKS

This approach is called "credential stuffing" vs credential cracking we discussed last class

Source: https://xkcd.com/2176/

Information is one of the few things that can be in multiple places at the same time

-- Pierson?

Agenda

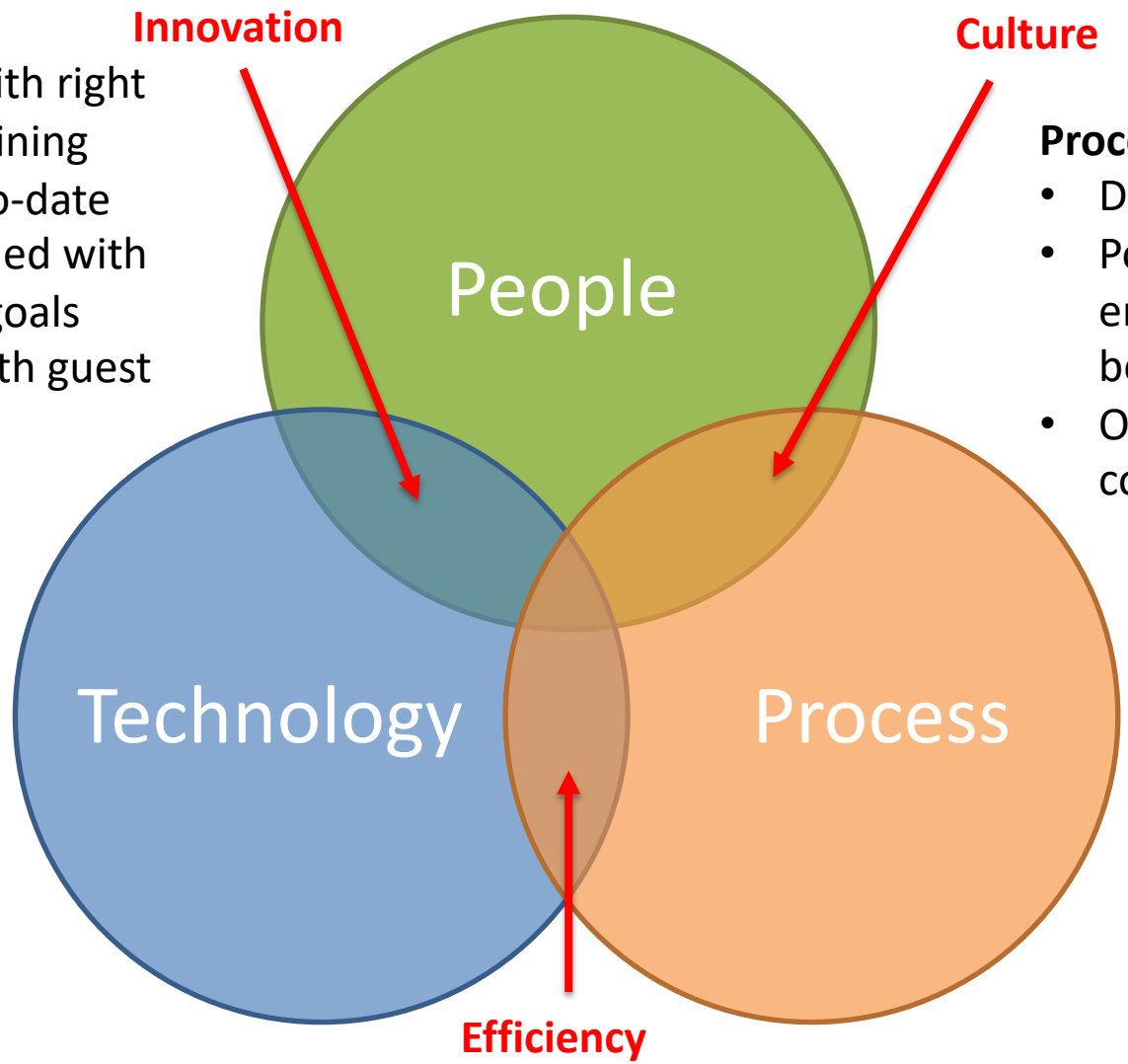
1. Security vocabulary
2. CIA/Opsec
3. Threats

We need to consider people, process, and technology when thinking about security

PPT framework: People, Process, Technology

People

- Right people with right skill set and training
- Skills kept up-to-date
- Incentives aligned with organization's goals
- Will address with guest speakers



Process

- Design workflows
- Policies that encourage desired behavior
- Often strive for consistency

Technology

- Right tools
- Configured correctly
- Updated/ patched
- Our primary focus in CS55

Our primarily focus in CS55 will be on technology, but all three can be exploited by adversaries

In technology, systems are composed of hardware, software, and data

Systems

Hardware

- Computers
- Devices (phones, tablets)
- Network equipment

Off the shelf

- **Easy to replace**
- **Replacement may be costly but calculable**
- **Temporal component may be inconvenient (breaks right before the big client presentation!)**

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

In technology, systems are composed of hardware, software, and data

Systems

Hardware

- Computers
- Devices (phones, tablets)
- Network equipment

Software

- Operating systems
- Utilities (antivirus)
- Commercial applications (word processing, spreadsheets)

Off the shelf

- **Easy to replace**
- **Replacement may be costly but calculable**
- **Temporal component may be inconvenient (breaks right before the big client presentation!)**

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

In technology, systems are composed of hardware, software, and data

Systems

Hardware

- Computers
- Devices (phones, tablets)
- Network equipment

Software

- Operating systems
- Utilities (antivirus)
- Commercial applications (word processing, spreadsheets)
- Custom applications

Off the shelf

- **Easy to replace**
- **Replacement may be costly but calculable**
- **Temporal component may be inconvenient (breaks right before the big client presentation!)**

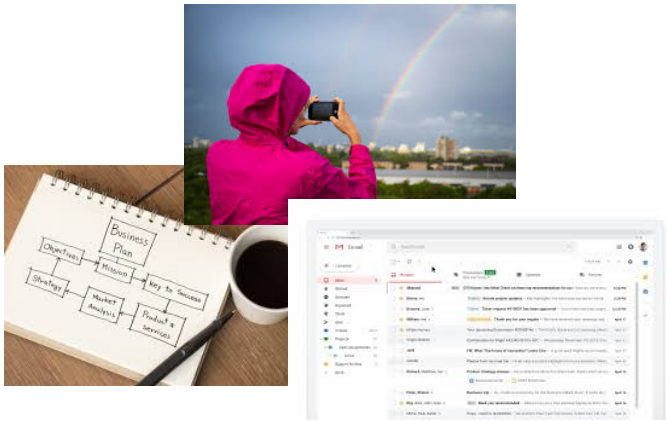
Unique

- **May be irreplaceable**
- **Value may be difficult to measure**
- **Value may depend on user**

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

The value of a system is often personal, time dependent, and difficult to measure

Value



Hardware
- Computers
- Devices (phones, tablets)
- Network equipment

Software
- Operating systems
- Utilities (antivirus)
- Commercial applications (word processing, spreadsheets)
- Custom applications

Data
- Documents
- Photos, music, videos
- Email
- Class projects
- Business plans

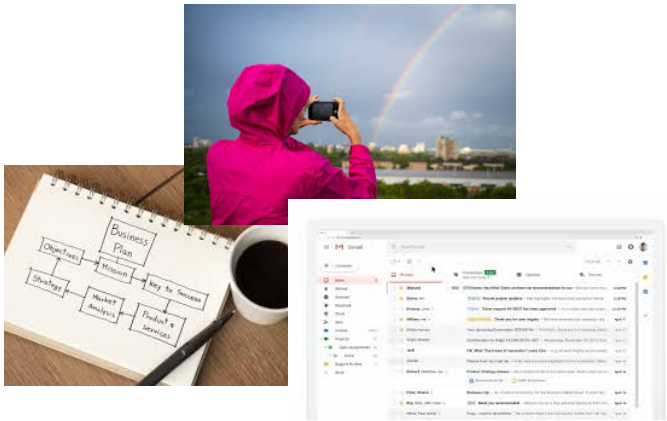
Off the shelf
- **Easy to replace**
- **Replacement may be costly but calculable**
- **Temporal component may be inconvenient (breaks right before the big client presentation!)**

Unique
- **May be irreplaceable**
- **Value may be difficult to measure**
- **Value may depend on user**

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

Vulnerabilities are weaknesses in a system

Vulnerabilities



Hardware

- Computers
- Devices (phones, tablets)
- Network equipment

Vulnerabilities

Hardware may have vulnerabilities that expose data such as Meltdown or Spectre attacks

Software

- Operating systems
- Utilities (antivirus)
- Commercial applications (word processing, spreadsheets)
- Custom applications

Software may have vulnerabilities such as buffer overflow

Data

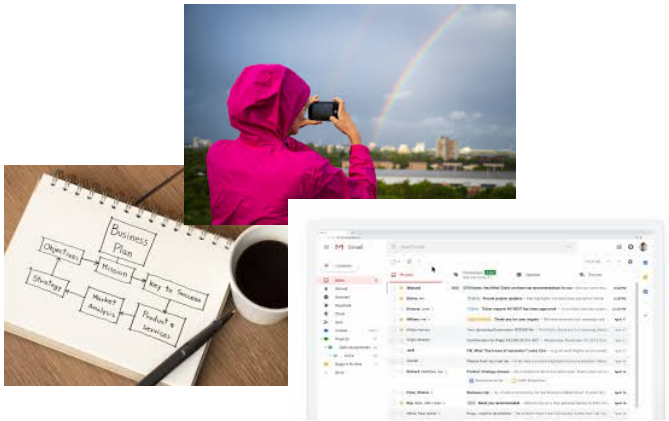
- Documents
- Photos, music, videos
- Email
- Class projects
- Business plans

Data may be "CRUD" by unauthorized people exploiting a vulnerability

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

A threat is a set of circumstances that could cause harm

Threats/Attacks



Threats

- Human
- Natural disasters
- Errors/ misconfigurations

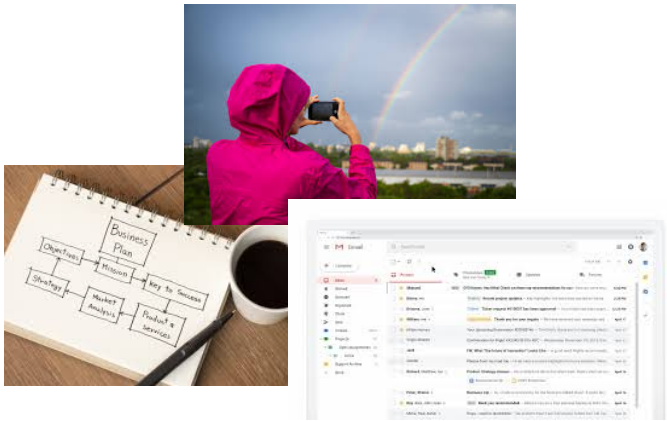
Attack

- When a human exploits a vulnerability
- Could cause one system to attack another

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

A countermeasure prevents threats from exercising vulnerabilities

Countermeasures



Countermeasure

Threats

- Human
- Natural disasters
- Errors/ misconfigurations

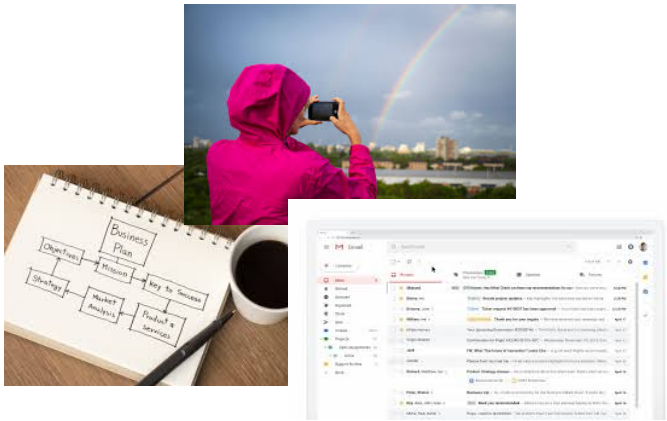
Attack

- When a human exploits a vulnerability
- Could cause one system to attack another

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

A policy specifies *who* is authorized to do *what* and *how*

Policy



Countermeasure

Policies

Subject/principal
- Person
- Process
- Program

Object/resource
- Hardware
- Software
- Data item

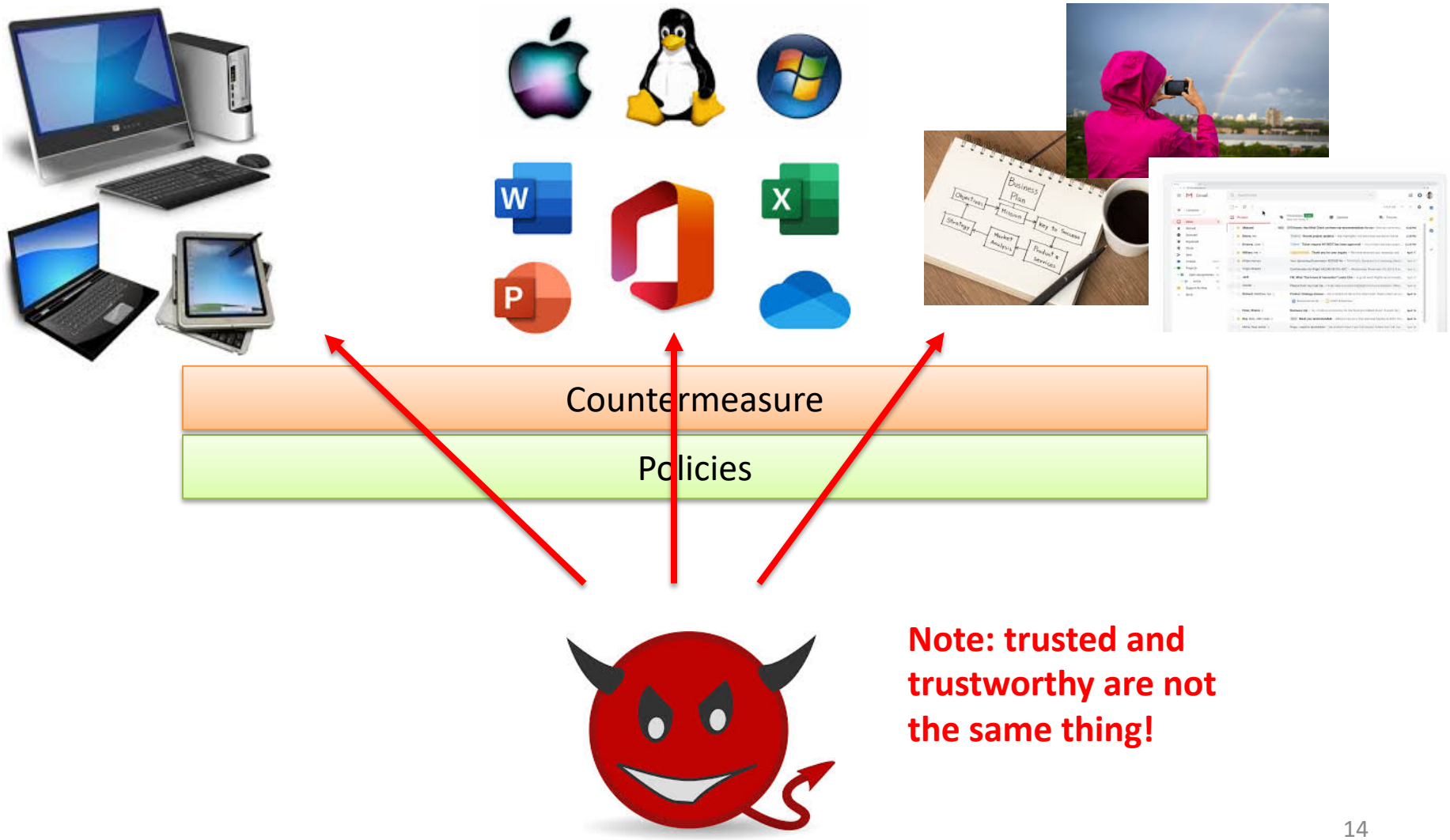
Questions
- **Who decides who is authorized**
- **Who is authorized to disclose to third parties?**

Access mode (how)
- Read
- Write
- Execute

Policy
- What subject
- Can act on what object
- With what access mode

Harm is the negative consequence of an actualized threat

Harm



Note: trusted and trustworthy are not the same thing!

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

Discussion

What types of harm can result from an actualized threat?

Book lists

- **Interception**
- **Interruption**
- **Modification**
- **Fabrication**

Researchers have identified five types of "cyber harm"

Harm

Physical/Digital	Economic	Psychological	Reputational	Societal
Equipment • Damaged/ unavailable • Destroyed • Stolen **People** • Bodily injury • Loss of life • Prosecution/ jail time	• Disrupted operations/ sales • Reduced customers/ profits • Increased clean up/PR costs • Loss of jobs	• Confusion • Anxiety • Depression • Embarrassment • Loss of confidence	• Damaged relationships • Media scrutiny • Reduced corporate good will • Inability to recruit staff	• Negative changes in public perception (of technology) • Disruptions in daily life • Negative impact on economy • Reduced state morale

Agrafiotis, Ioannis, et al. "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate." *Journal of Cybersecurity* 4.1 (2018).

Agenda

1. Security vocabulary
2. CIA/Opsec
3. Threats

Discussion

What security-related properties would you like in a technology system?

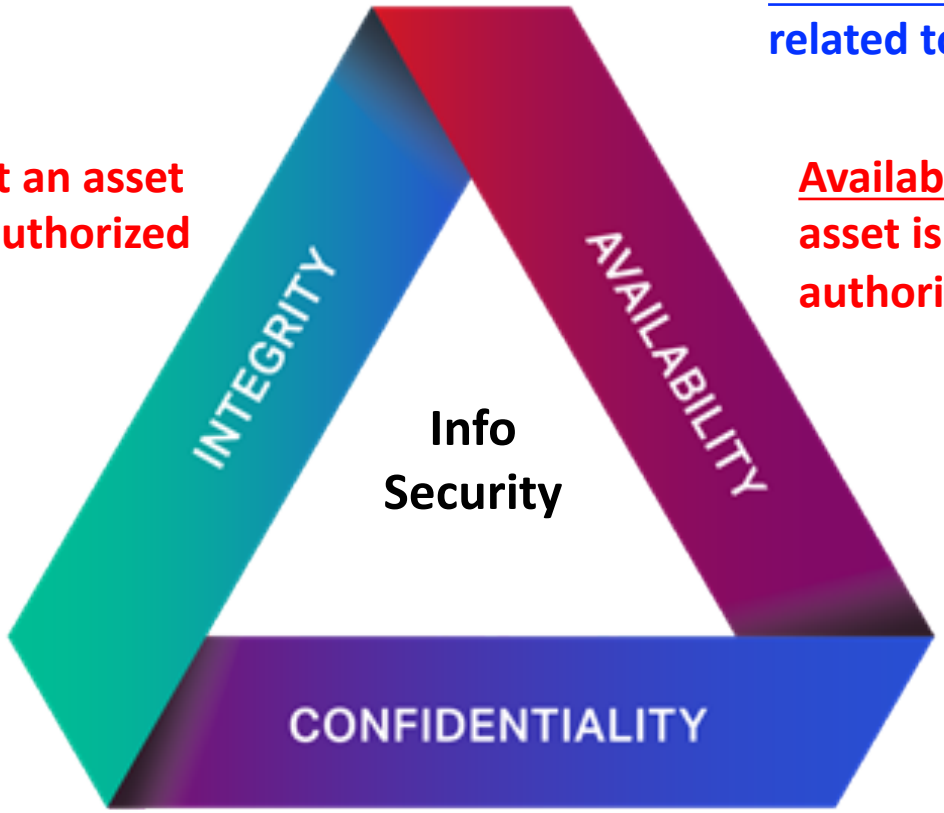
The CIA model is commonly used to describe desired security properties

Security triad

Auditability: trace all actions related to an asset

Integrity: ensure that an asset is modified only by authorized parties

Availability: ensure that an asset is viewed only by authorized parties



Authentication: confirm the identity of a sender

Nonrepudiation: a sender cannot convincingly deny having sent something

Confidentiality: ensure that as asset cannot be accessed by unauthorized parties

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

Example: a thief steals your computer

What could be compromised?

- Confidentiality
- Integrity
- Availability

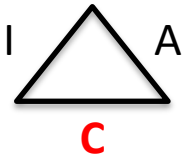
Harms

- Interception
- Interruption
- Modification
- Fabrication

Image: https://www.computerhope.com/issues/ch001011.htm

Sometimes confidentiality is compromised by seemingly unimportant data

Essential Elements of Friendly Information (EEFI)

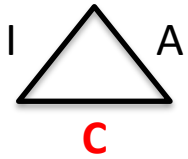


Pizza orders skyrocket right before military base goes to war
Planners are up all night working, they get hungry!

https://www.wired.com/2007/05/army-bloggers/

Military base locations inferred from data collected by fitness trackers

Essential Elements of Friendly Information (EEFI)



What is probably here?

US soldier wore fitness trackers and uploaded data to jogging tracking site

Military base locations and details inferred

Russian soldiers post photos tagged in Ukraine

https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases
https://www.csoonline.com/article/3391566/what-is-opsec-a-process-for-protecting-critical-information.html

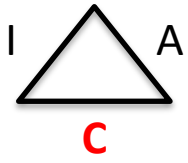
There are several ways an adversary can compromise confidentiality

Human intelligence (**HUMINT**)
Use humans (spies, diplomats, informers) to gather intel

Signals intelligence (**SIGINT**)
Capture information broadcast over the air (or tap landlines)

Imagery intelligence (**IMINT**)
Use satellite (or other) imagery

Open-source intelligence (**OSINT**)
Use published (web) information



https://fas.org/irp/nsa/ioss/threat96/part02.htm

IMINT example: Google Street View

What mistake is this security guard making?

IMINT example: duplicating keys from a photo (using Microsoft Word)

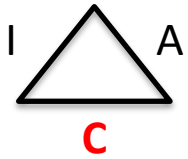
https://www.youtube.com/watch?v=vxJ3Kovz-bo&start=197

IMINT example: duplicating keys from a photo (using Microsoft Word)

What is the "key" takeaway?
Keep your keys in your pocket!

https://www.youtube.com/watch?v=vxJ3Kovz-bo&start=197

Operational Security (OPSEC) is a method of protecting Confidentiality



Operational Security: protecting *critical information* that if revealed to an adversary could be useful to them

EEFI – Essential Elements of Friendly Information

- Could be analyzed and grouped with other data by a clever adversary
- Could reveal a bigger picture that should stay hidden

Critical information

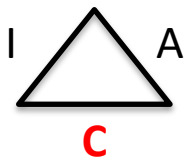
- Specific facts about friendly intentions, capabilities, and activities
- Needed by adversaries for them to plan and act effectively

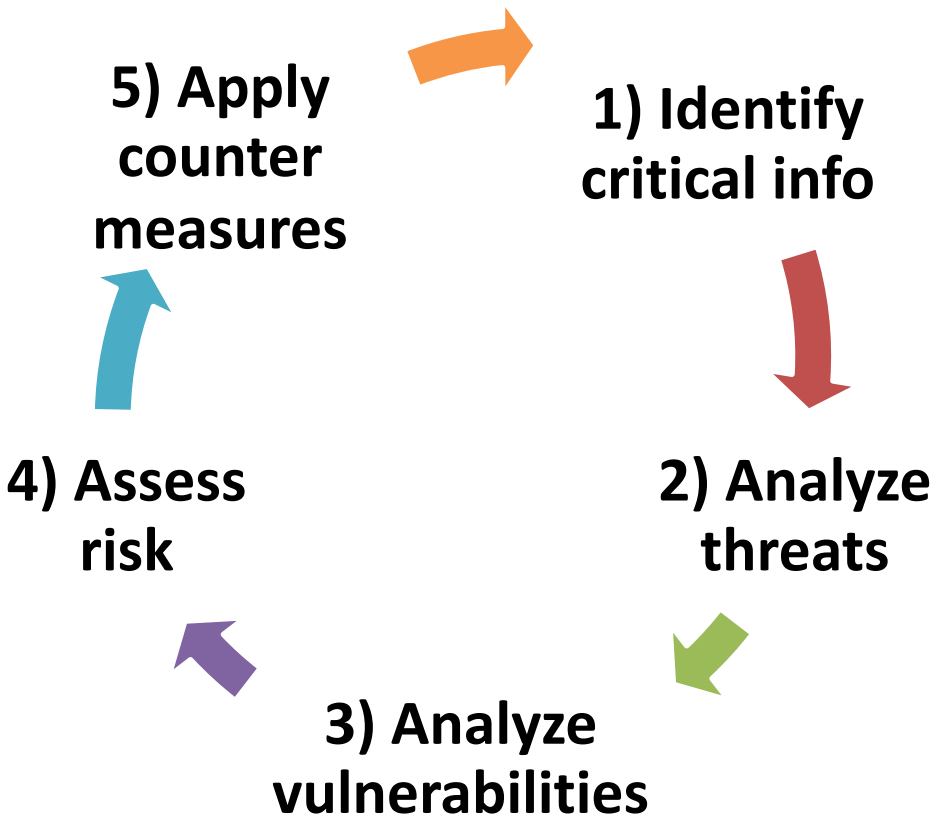
Adversary's goal: guarantee failure or unacceptable consequences for friendly mission accomplishment

https://www.csoonline.com/article/3391566/what-is-opsec-a-process-for-protecting-critical-information.html
Joint Pub 1-02

OPSEC involves a five-step process

OPSEC process

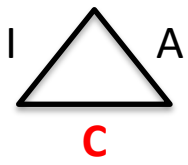




https://fas.org/irp/doddir/army/ar530-1.pdf

OPSEC involves a five-step process

OPSEC process



1) Identify friendly critical info with CALI

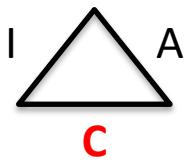
- Capabilities
- Activities
- Limitations
- Intentions

Focus on vital information, not everything

https://fas.org/irp/doddir/army/ar530-1.pdf

OPSEC involves a five-step process

OPSEC process



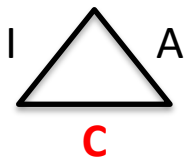
2) Identify adversaries

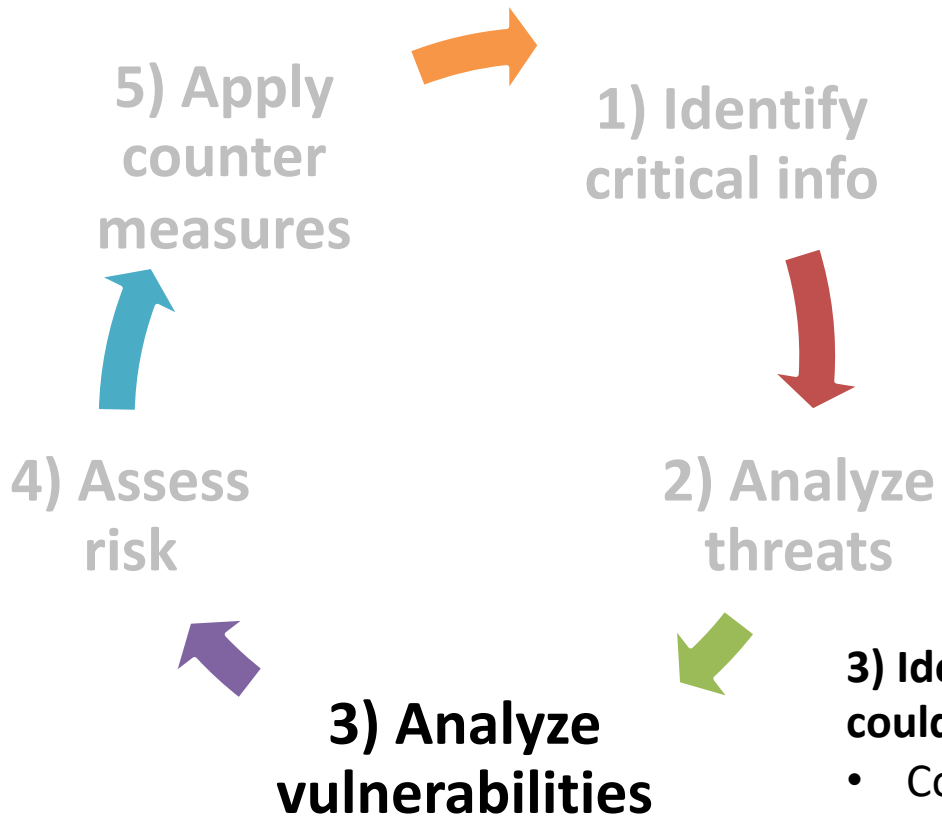
- Who is trying to compromise confidentiality
- What are their capabilities and intentions

https://fas.org/irp/doddir/army/ar530-1.pdf

OPSEC involves a five-step process

OPSEC process





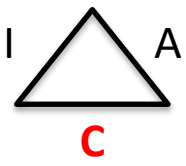
3) Identify OPSEC indicators that could reveal critical information

- Compare vs. adversary's capabilities
- Vulnerabilities are weaknesses in friendly organization

https://fas.org/irp/doddir/army/ar530-1.pdf

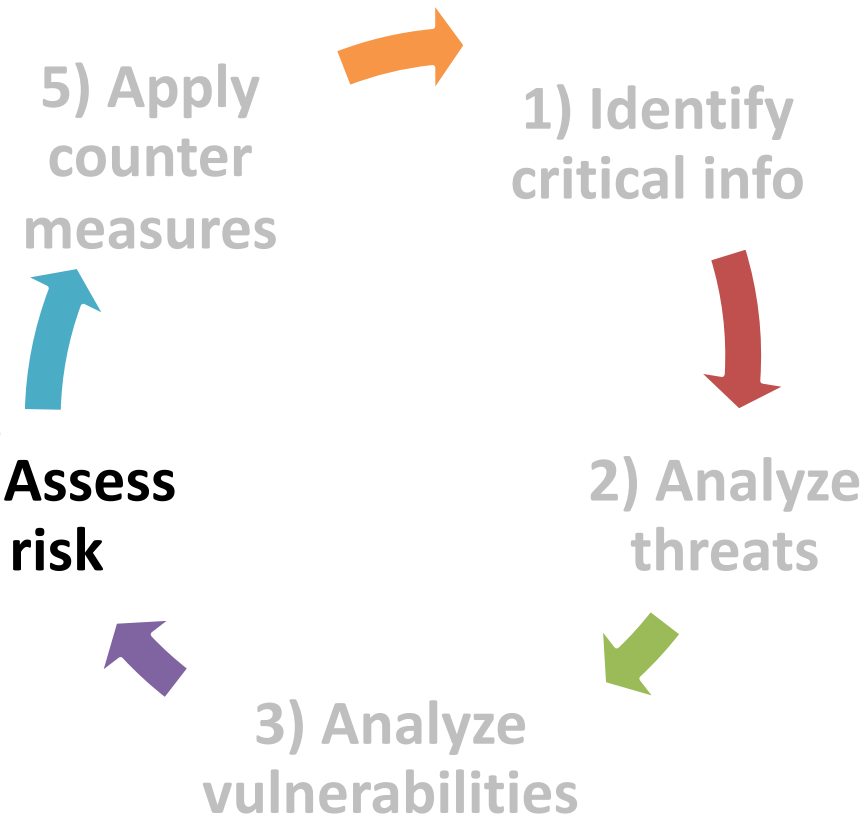
OPSEC involves a five-step process

OPSEC process



4) Assess adversary capabilities and friendly vulnerabilities

- Identify possible countermeasures
- Risk = probability of compromise times damage if compromised



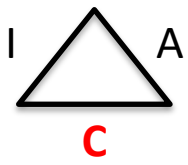
https://fas.org/irp/doddir/army/ar530-1.pdf

OPSEC involves a five-step process

OPSEC process

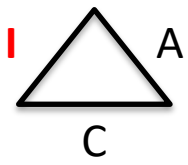
5) Apply counter measures

- Continuously monitor for efficacy
- Repeat cycle



https://fas.org/irp/doddir/army/ar530-1.pdf

Integrity is harder to define than confidentiality



People use Integrity differently in different contexts, it can mean:

- Precise
- Accurate
- Unmodified
- Modified only in acceptable ways
- Modified only by authorized people
- Modified only authorized processes
- Consistent
- Meaningful and usable

Welke and Mayfield identify three aspects of Integrity:

1. Only authorized actions
2. Separation and protection of resources
3. Error detection and correction

Preventing integrity compromise is often same as confidentiality

One countermeasure to detect if a document has been modified is to provide a hash

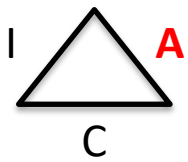
- **Must ensure adversary can't provide a hash of the modified document**
- **PKI can help**

Met card catalog example

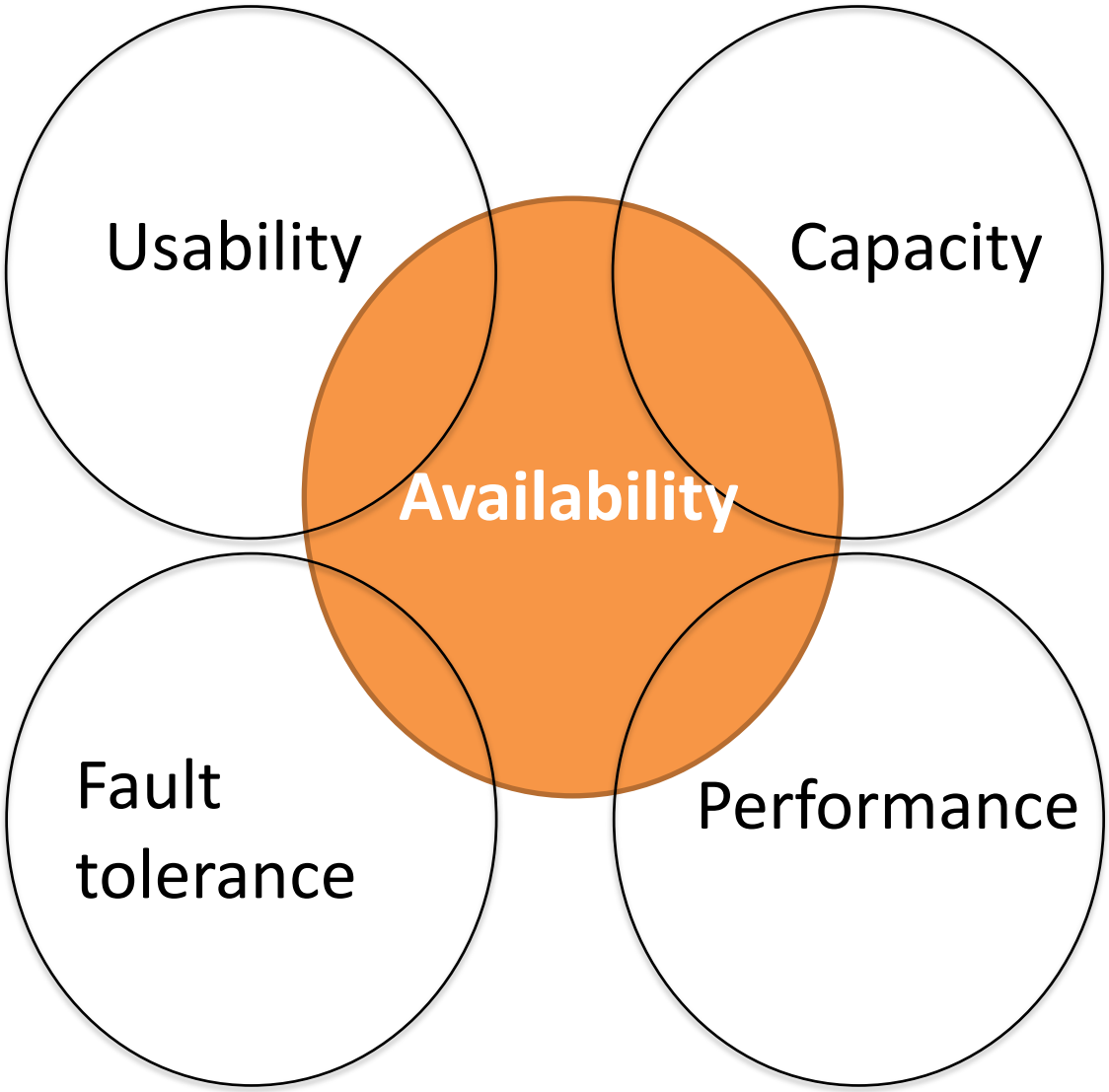
https://apps.dtic.mil/sti/citations/ADA253990

Availability applies to hardware, software, and data

Availability



Present in usable, reachable form



Has enough capacity to meet user's needs

Handles faults gracefully

Making clear progress (bounded wait time) / completes

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

Agenda

1. Security vocabulary
2. CIA/Opsec
3. Threats

Threats can be natural or human, benign or malicious, random or directed

Threat taxonomy

Threats

Natural

Just you
- Component failure
- Fire/water pipe break

Localized
- Block-wide power outage

Regional
- Hurricane/flood

Human

Benign
- Spill coffee
- Type 12 instead of 21

Malicious

Random
- Malicious code on a general web site
- Scam phone calls to all numbers
- Phishing

Directed
- Social engineering
- Spear fishing
- APTs

Not always clear when attack is underway (e.g., system failure could be natural or directed attack)

Disaster Recovery (DR)
- **Organization's plan to recovery different types of threats**
- **My view: large tomes are not useful!**

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

Discussion

How do you know if something is an attack or an ordinary human or technological breakdown?

Have you ever experienced harm as a result of a failure of computer security? Was it malicious or not? Did the attack target you specifically or were you unlucky?

There are many different types of threat actors

Script kiddie

- Runs pre-made scripts
- May not know what's really happening
- Not necessarily young
- No funding
- Often motivated by the hunt

Hacktivist

- Hacker and activist
- Have an agenda
- Can be sophisticated
- Normally funding is limited, but that is changing

Adapted from https://www.professormesser.com/security-plus/sy0-501/threat-actors/

There are many different types of threat actors

Organized crime

- Motivated by money
- Sophisticated
- Well funded
- May sell data hacked

Government

- Experts working for government agency
- Extremely sophisticated
- Advanced Persistent Threat (APT)

Insiders

- Understand organization
- Have a grudge

Adapted from https://www.professormesser.com/security-plus/sy0-501/threat-actors/

Threats: who is missing?

The book mentions:

- Spies
- Crooks
- Geeks
- Terrorists

Who is missing?
Corporations!

Target determined a young woman was pregnant before her father knew

- Each time you shop online, you share information with retailers
- Retailers study patterns closely to determine what you like
- Purchases tied to your credit card/browsing habits
- Also buy information from other sources (demographic, other retailers)
- How Target knew:
  - Women on Target's baby registry buy lots of lotion around second trimester
  - In first 20 weeks also buy lots of vitamins, unscented soap, and cotton balls (could also have skin infection!)
  - Used 25 products to predict pregnancy, then sent coupons to likely women
  - Buy cocoa-butter lotion, large purse (could double as diaper bag), zinc and magnesium supplements => 87% chance due within four months
- Dad confronted Target suggesting they are encouraging her to get pregnant – found out truth later
- Target now spreads out pregnancy coupons with other ones to not appear creepy
- Did it work? Sales went from $44B to $67B after profiling
- Did Target break any laws?
- What about other companies like Facebook, Twitter, Instagram?

https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did

Adversaries need method, opportunity and motive for a successful attack

Adversary
Defender

Method
How will the attack succeed?

Skills are needed to overcome counter measures

Opportunity
Time and access are needed to execute an attack

Attack at night when no one is around

Motive
Reason to attack

- Money
- Fame
- Self-esteem
- Politics
- Terror

Vulnerability
A weakness an adversary can exploit
Attack surface: all vulnerabilities

Counter measures (or controls)
Means to counter threats

- Physical
- Procedural
- Technical

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

Counter measures can deal with threats in several ways

Prevent: block the attack or close vulnerability

Deter: make the attack harder, but not impossible

Deflect: make another target more attractive

Mitigate: make the impact less severe

Detect and respond: notice attack and act to stop it

Recover: return to normal operation

Adapted from *Security in Computing* by Pfleeger, Pfleeger, and Margulies

The fortress mentality doesn't work anymore; need P > D + R

Protection > Detection + Reaction

>

+

Protection

- Secure systems development
- Cryptography
- Secure comms
- Firewalls/VPNs
- Physical security

Detection

- IDS/IPS
- Pen testing/ forensics

Reaction

- Automatic
- Manual
- Incident management
- Team leadership
- Disaster recovery

Lots of focus on protection, don't forget detection and reaction!

Note: this framework is not particularly popular, but I like it!

Schwartau, Winn. "Time-based security explained: Provable security models and formulas for the practitioner and vendor." *Computers & Security* 17.8 (1998): 693-714.

We'd like to protect systems

Discussion: what constitutes a system?

- A product or component such a a cryptographic protocol, a smart card, or the hardware of a phone, a laptop or server
- One or more of the above plus an operating system, communications and other infrastructure
- The above plus one or more applications, including both client and server/cloud components
- Any or all of the above plus IT staff
- Any or all of the above plus internal users and management
- Any or all of the above plus customer s and other external users

My definition: combination of people, process, and technology