Week 1 - Wednesday

COMP 4290

Last time

- What did we talk about last time?
- Course overview
- Terminology
  - Threats
  - Vulnerabilities
  - Attacks
  - Controls
- CIA

Questions?

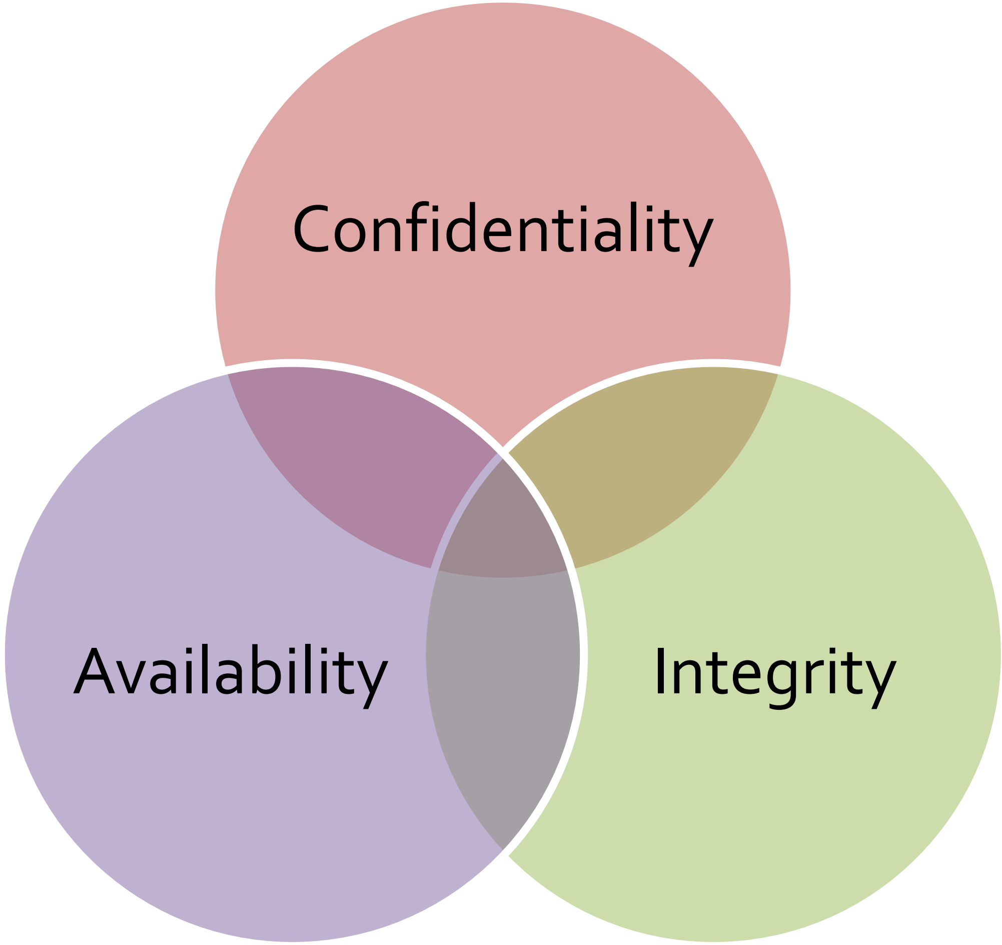
Sign up for Presentations

Form Teams for Project 1

Security tidbit: LLMs can import malicious code

- Many people are using LLMs to help them code
- But new "agentic" tools can pull information from various sources, like GitHub issue pages
- If attackers can sneak malicious code into those sources, that code can be pulled into your program
  - Techniques called "ASCII smuggling" put invisible characters into messages that LLMs can read even if humans can't see them
- Once your code runs, either for testing purposes or in a product, the malicious code can do whatever it wants on the target system
- These risks are even greater with inexperienced coders and vibe coding
- Credit to Professor Stucki for letting me know about the research
- Read more:
  - https://garymarcus.substack.com/p/llms-coding-agents-security-nightmare

CIA



Encryption

- Encryption is the scrambling of data
    - Often a key or some other secret information is used to do the scrambling
    - Without knowledge of the secret, the data becomes useless
- Modern encryption is one of the most powerful tools for preserving computer security
- Most modern attacks do not depend on breaking encryption but on circumventing it

Encryption

- The process of encryption takes **plaintext** as an input and produces **ciphertext** as an output
- Plaintext (or **cleartext**) is not necessarily human readable, but its contents are not protected in any way
- Using cryptography, we can build **protocols** to support confidentiality and integrity (and even availability indirectly)
- As useful as it is, encryption is **not** a panacea

Attackers

Individuals

- Most computer criminals are amateurs
  - They commit crimes of opportunity
  - Time-stealing is common
- Disgruntled or recently fired employees can use their knowledge of a system to attack it
- Many hackers attempt to gain access to other people's computer systems for the fun or challenge of it
  - They often brag about their exploits

Organized crime

- Most professional hackers are trained computer scientists who have turned to crime
- In the early days of hacking and viruses, destroying hardware, software, or data was the goal
- Professional hackers now look to make money by stealing valuable data
- There are connections to organized crime
- Many attacks come from Russia, Asia, and Brazil
- Professionals want to remain undetected so that they can keep stealing data
- Ransomware is big business:
  - Purplesec reports an average cost of over $5 million per attack
  - The FBI reported losses of over $16 billion in 2023 for Internet crime

Terrorists

- Modern terrorists are often computer savvy
- Four common forms of terrorist computer usage are:
  - **Targets of attacks**

    Denial-of-service and defacement of websites
  - **Methods of attack**

    Using computers to launch an attack
  - **Enablers of attacks**

    Coordinating or initiating other forms of terrorism through websites, e-mail, etc.
  - **Enhancers of attacks**

    Using the Internet to spread propaganda and recruit agents

Harm and risk

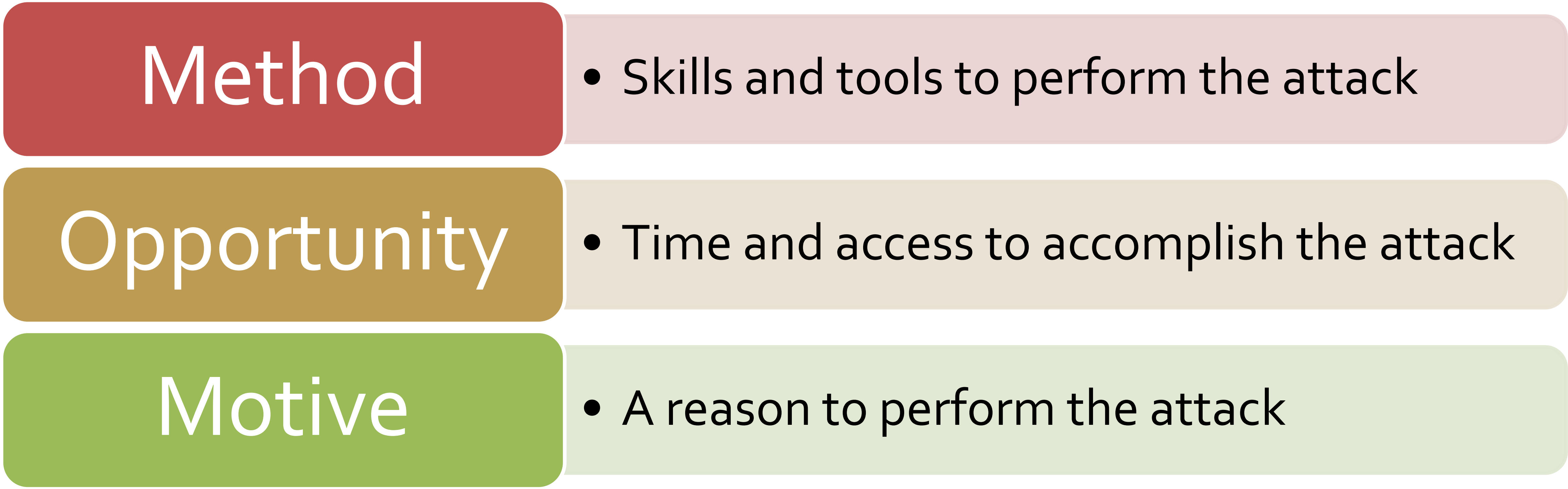
- **Harm** is the bad thing that happens when the threat occurs
- **Risk management** is about choosing which threats to control and which not to
    - Remember that this is usually a financial decision
- **Residual risk** is the risk that is still not controlled after risk management

Risk perception

- What's the chance that a huge meteor will hit during our lifetimes?
  - Small!
  - **Likelihood** is the chance that a threat will happen
- What will happen if a huge meteor hits?
  - Terrible things!
  - **Impact** is the damage of a threat
- Humans overestimate the likelihood of rare, dreaded events

Method, opportunity, motive

- As with traditional crime, a computer attacker must have three things:



Method
- Skills and tools to perform the attack

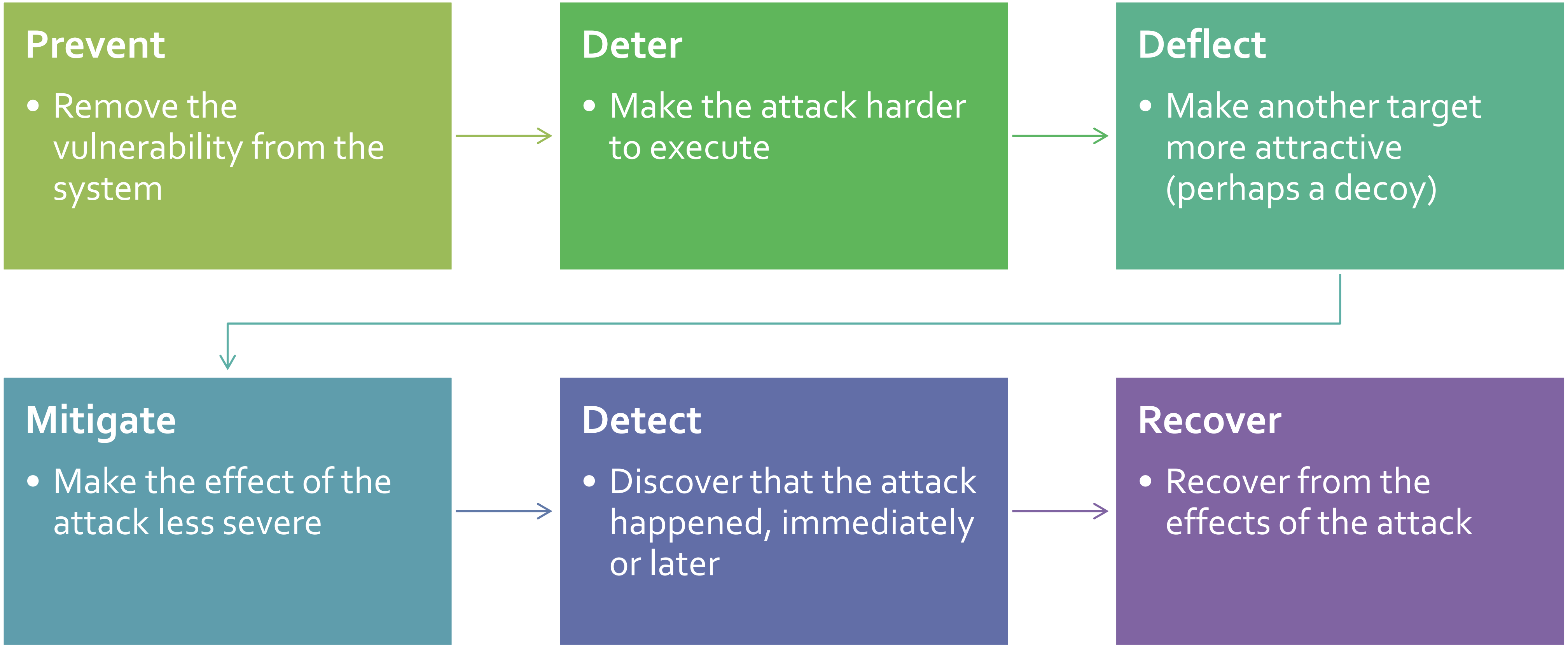
Opportunity
- Time and access to accomplish the attack

Motive
- A reason to perform the attack

Controls

Controls

- There are six common ways of controlling attacks, many of which can be used together



Prevent

- Remove the vulnerability from the system

Deter

- Make the attack harder to execute

Deflect

- Make another target more attractive (perhaps a decoy)

Mitigate

- Make the effect of the attack less severe

Detect

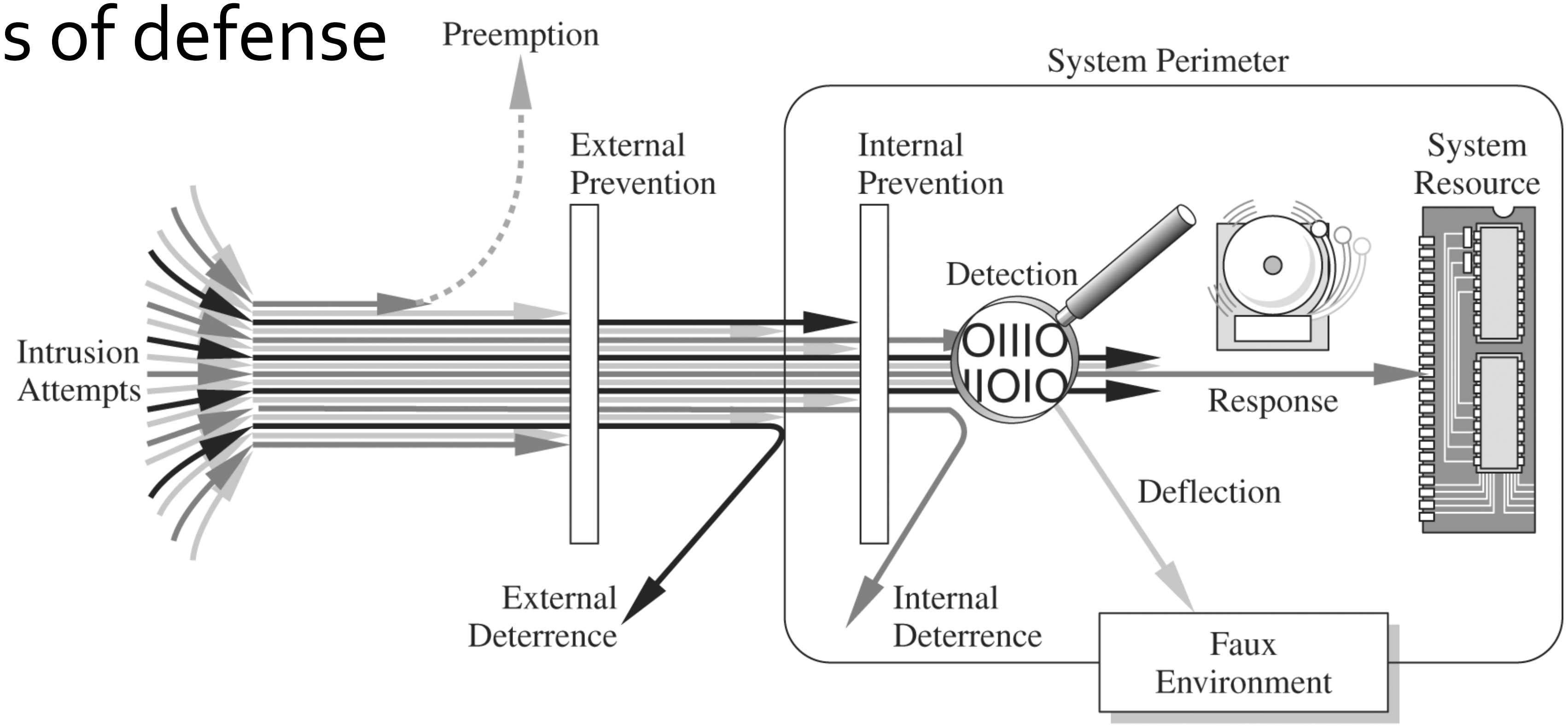
- Discover that the attack happened, immediately or later

Recover

- Recover from the effects of the attack

Effects of controls

- Many different controls can be used to achieve the six methods of defense



Pfleeger/Pfleeger Fig. 01-06

Physical controls

- Physical controls can be inexpensive and effective
  - Locks on doors
  - Security guards
  - Backup copies of data
  - Planning for natural disasters and fires
- Simple controls are often the best
- Attackers will always look for a weak point in your defenses

Procedural controls

- Human beings ultimately get involved
- It's important to have policies and procedures to guide their actions, such as:
  - Change passwords regularly
  - Don't give people your password
  - Don't allow coworkers access to data they should not have
- Laws are important policies with consequences, but they react slowly to the rapid changes in technology

Technical controls

- Software controls:
  - Passwords
  - OS and network controls
    - Tools to protect users from each other
  - Independent control programs
    - Application programs that protect against specific vulnerabilities
  - Development controls
    - Quality control for creating software so that vulnerabilities are not introduced
- Hardware controls
  - Smart cards on satellite or cable television set-top boxes
  - Fingerprint or other biometric readers
  - Firewalls

Effectiveness of controls

- Many issues impact the effectiveness of controls
  - **Awareness of problem**

    Users must be convinced that it is worth using the controls
  - **Likelihood of use**

    The controls must be easy enough to use that the task performed is not seriously affected
  - **Overlapping controls**

    Overlapping controls or **defense in depth** can help, but sometimes the controls negatively impact each other
  - **Periodic review**

    Conditions change, and controls must be reviewed periodically and updated when needed

Counting

Counting

- A lot of computer security depends on how many items are in a set
  - Number of possible passwords
  - Possible encryption keys
- To understand the security, we need to count the number of items
- Consider a string where each character in the string has a set number of possibilities, independent from the others:

Place	___	___	___	___	___	___	___	___	___	___
Possibilities	a	b	c	d	e	f	g	h	i	j

- The total number of possible strings is the product of the possibilities in each place: $a \cdot b \cdot c \cdot d \cdot e \cdot f \cdot g \cdot j \cdot i \cdot j$

Counting practice

- How many passwords are there of exactly length 8, containing only letters and digits?
- How many passwords are there with lengths between 4 and 8, containing only letters and digits?
- How many 128-bit AES keys exist?
- How many 10-byte sequences are possible?

Upcoming

Next time…

- Authentication
- Passwords
- Biometrics

Reminders

- Read Section 2.1
- Start Assignment 1
- Start Project 1