COMP482
Cybersecurity
Week 1 - Wednesday

Dr. Nicholas Polanco

(he/him)

KALAMAZOO COLLEGE

Attendance

Which side would you rather be on? I will give 1 notecard to each side, please put your “team” members and 3 reasons why you chose that side. You should discuss these reasons together and come to a mutual decision.

You are required to assist your professor in making sure that an in-class exam (that allows students the use of laptops) has as little students cheating as possible.

OR

You can take the same in-class exam and need to cheat on the exam **without** getting caught.

Overview of Pretest Results

How confident are you in your ability to describe how **software/architecture** works? How confident are you in your understanding of **software/architecture** concepts?

- Very confident or confident
  - 30% & 42%
- Neutral
  - 59% & 47%
- Not confident
  - 12% & 6%

Overview of Pretest Results (continued)

How confident are you in your ability to describe how a **network** works? How confident are you in your understanding of **network** concepts?

- Confident
  - 29% & 29%
- Neutral
  - 59% & 65%
- Not confident
  - 12% & 6%

Overview of Pretest Results (continued)

How confident are you in your ability to describe how a **database** works? How confident are you in your understanding of **database** concepts?

- Very confident or confident
  - 64% & 65%
- Neutral
  - 29% & 24%
- Not confident
  - 6% & 12%

Overview of Pretest Results (continued)

How confident are you in your ability to describe how **cryptography/encryption/decryption** works? How confident are you in your understanding of **cryptography/encryption/decryption** concepts?

- Very confident or confident
  - 36% & 47%
- Neutral
  - 47% & 35%
- Not confident
  - 18% & 18%

Overview of Pretest Results (continued)

How confident are you in your ability to describe **"safe software"**?
How confident are you in your knowledge of **"safe software"** concepts and principles?

- Confident
  - 24% & 18%
- Neutral
  - 35% & 41%
- Not confident
  - 41% & 41%

Overview of Pretest Results (continued)

What are you most interested in learning about in this course?

*I had almost all the topics you all requested already in my course plan, so that was good!

What are you least interested in learning about?

I had some notes in here about social engineering and class discussions. I will adjust if these do not go well. For example, if discussions are not productive I will lecture for longer or add activities.

Overview of Pretest Results (continued)

What topic would you like to see included in additional lectures (that is not listed)?

These are a few of the topics shared (we had more): Artificial Intelligence and Cybersecurity, Autonomous Vehicles, Surveillance, Quantum Computing and Cryptography, Financial Institutions

***We can vote on additional lectures a bit later on, but I will keep these close!**

What other information would you like to share?

The class wanted resources for labs, additional work, and someone shared the lyrics to Rick Ashley's Never Gonna Give You Up.

Important Notes

1. I have added a lot of additional resources based on the classes requests, I have some marked as “upon request”.
    a. These are eBooks I have purchased, so I can give you a PDF or epub copy of these but you will need to contact me directly.
2. Please make sure to join the Teams channel, I’m not sure why I have to approve them but I will do that as more people join.
    a. This may be a resource we end up not using, but for now I would like us to have it.
3. SIP Fest is next week, you should go to that

Important Dates (Week 1)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
		Before Class: Chapter 1-1.6 In Class: Think Like a Hacker Activity		After Class: Reflection: Week 1		

What is Cybersecurity?

What is Cybersecurity?

The NIST (National Institute of Standards and Technology) Computer Security Handbook [NIST95] defines the term computer security as follows:

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

CIA Triad

This definition of computer security enables us to pull out three key objectives at the heart of computer security:

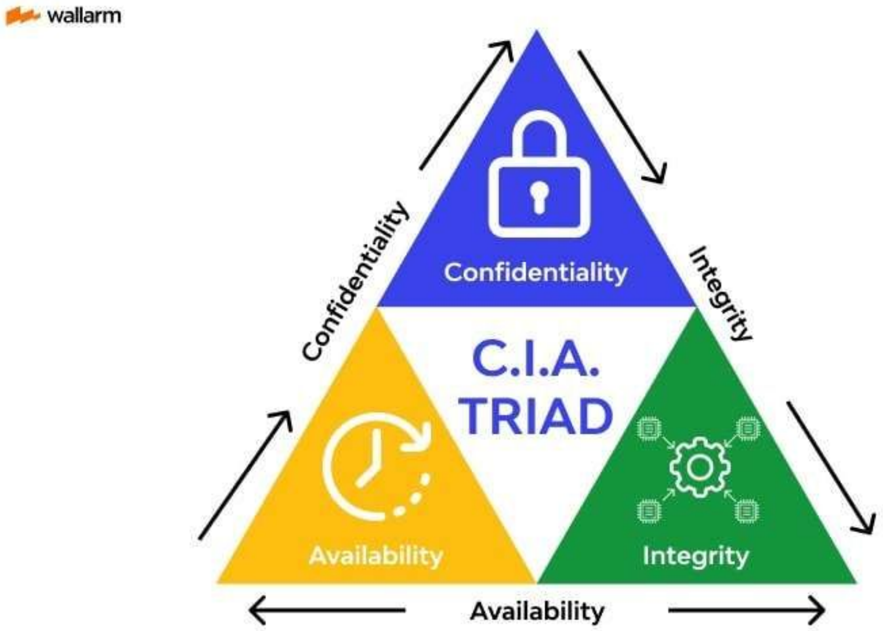

Image Credit:
https://www.wallarm.com/what/cia-triad-definition

CIA Triad (continued)

Confidentiality: This is essentially just making sure our information is kept secret. This can be broken into two related concepts:

Data confidentiality: This assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: This assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

CIA Triad (continued)

Integrity: This is an assurance that data has not been corrupted or purposefully tampered with. This also encompasses two main ideas:

Data integrity: This assures that information and programs are changed only in a specified and authorized manner.

System integrity : This assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

CIA Triad (continued)

Availability: This is saying that a system **should** remain up and running to ensure that valid users have access to the data when needed. When I need to access a resource, it **should be available.**

CIA Triad (continued)

These are some samples of what a “loss” of a given CIA principle would look like:

Confidentiality: A loss would be the unauthorized disclosure of information.

Integrity: A loss of would be the unauthorized modification or destruction of information.

Availability: A loss would be the disruption of access to or use of information or an information system.

CIA Triad (continued)

Do we feel comfortable with confidentiality, integrity, and availability being the only objectives of our computer security?

Additional Terms

Authenticity: This is the idea of something being *authentic* or *verifiable and trusted*.

- This can be confidence in the validity of a transmission, a message, or message originator.
- This can also mean verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Additional Terms (continued)

Accountability: This is the goal that actions of an entity can be traced *uniquely* to that entity.

- This supports non-repudiation (we can’t deny responsibility), deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
- We must keep records of activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

AAA (Authentication, Authorization, and Accounting)

In the security field, some feel that additional concepts are needed to present a complete picture, such as Authentication, Authorization, and Accounting (AAA).

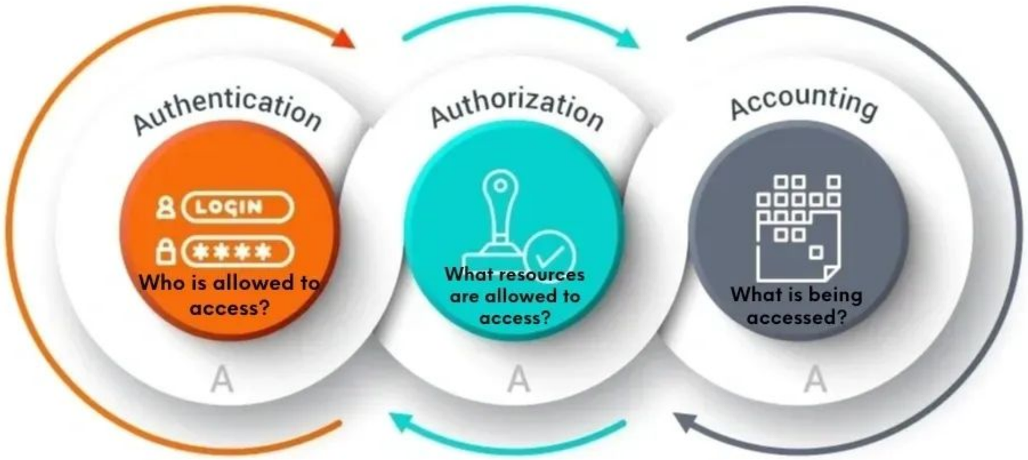

Image Credit: https://medium.com/@sabhareeshw/the-aaa-framework-the-pillars-of-secure-access-control-6c5e207f2bfa

AAA (Authentication, Authorization, and Accounting) (continued)

Authentication: This is the process of confirming someone’s identity.

- You can think of things like Multi-Factor Authentication (MFA)

Authorization: This is keeping track of which resources an entity has access to.

- Who is a TA/Grader for a lower-level COMP course? We have different authorization levels for different users.

Accounting: This is tracking the usage of resources.

- This can be useful for *preventing* and *tracking* different problems

DRY (Don’t Repeat Yourself)

This will be covered a bit more later on when we talk about designing secure software, but for now it is useful to know.

This is just emphasizing that we should make use of scripts, tools, testing methods to ensure we **aren’t** doing the same thing over and over

- We want to work smarter, not harder.

Cybersecurity Terminology

Adversary (or threat agent): An entity that attacks, or is a threat to, a system.

Attack: An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security Policy: A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

Cybersecurity Terminology (continued)

Vulnerability: A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy.

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event, that could breach security and cause harm. A threat is a possible danger that might exploit a vulnerability.

Risk: An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Cybersecurity Terminology (continued)

Asset (or system resource): Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component— hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Countermeasure: An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

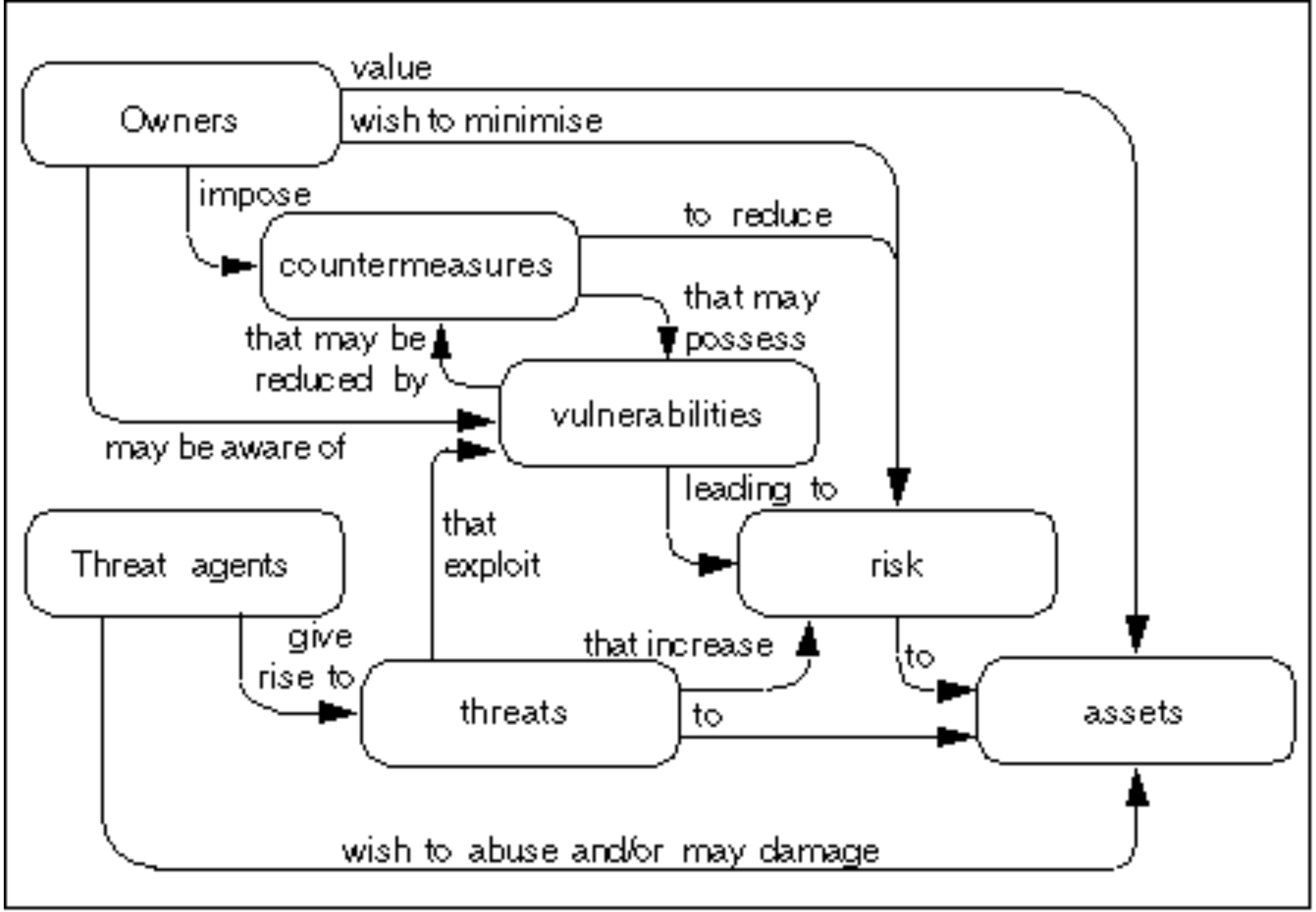

Image Credit: https://pagenotes.com/writings/ccToolbox6f/CCManual/PART1/PART14.HTM

A Simple Model for Computer Security

We should first model our assets, the aspects that users and owners wish to protect. These can be categorized as follows:

- **Hardware**: This includes computer systems and other data processing, data storage, and data communications devices
- **Software**: This includes the operating system, system utilities, and applications
- **Data**: This includes files and databases, as well as security-related data, such as password files.
- **Communications facilities and networks**: These can be local and wide area network communication links, bridges, routers, and so on.

What are the Challenges?

1. The idea of "computer security" is really not as simple as it appears to the novice. The mechanisms used to meet requirements (like confidentiality, authentication, nonrepudiation, integrity) can be quite complex!
2. Once you start *actually* developing a particular security mechanism or algorithm, you need to consider <u>potential attacks on those security features</u>.
   a. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

What are the Challenges? (continued)

3. Since we need to watch the solution we are implementing to protect the system, the procedures used to provide services are often **really** counterintuitive.
   a. A security mechanism is often complex, and it is only when the various aspects of the threat are considered that these elaborate security mechanisms make sense.
4. We have to now decide where to put these complex mechanisms.
   a. This can be physical or logical locations.

What are the Challenges? (continued)

5. These mechanisms typically involve more than a particular algorithm or protocol. They can require that participants be in possession of some secret information (e.g., an encryption key)\
   a. Therefore, we now need to manage the creation, distribution, and protection of that secret information.
6. We are in a **constant** battle between a perpetrator who tries to find holes, and the designer or administrator who tries to close them.
   a. The advantage that the attacker has is that they only need to find a single weakness!
   b. The designer must find and eliminate all weaknesses to achieve perfect security.

What are the Challenges? (continued)

7. We typically don’t perceive benefit from security investment until a security failure occurs.
8. The idea of a secure system requires regular monitoring, and this is difficult in today’s short-term, overloaded environment.
9. The concept of security is often **an afterthought** incorporated into the system after the design is complete rather than being an integral part of the design process.
10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

The Security Mindset

How do we even get started defending our systems?

Thinking Like an Attacker!

- Understand techniques for circumventing security
- Look **for ways security can break**, not why it won't

Thinking Like a Defender!

- Know what you're defending, and against whom.
- Weigh benefits vs. costs
  - Remember, no system is ever completely secure.
- Rational paranoia or justified suspicion

Thinking like an Attacker

1. We are going to look for weakest links

2. Identify assumptions that security depends on
   a. Are they false?

3. Think outside the box
   a. Not constrained by system designer’s worldview!

4. We are going to start practicing!
   a. When you interact with a system, think about what it means to be secure, and how it might be exploited.

Thinking like an Defender

1. We need a security policy
    a. What are we trying to protect?
    b. What properties are we trying to enforce?
2. We can use a threat model
    a. Who are the attackers? What are the capabilities? What are motivations?
    b. What kind of attack are we trying to prevent?

Thinking like an Defender (continued)

3. We need a risk assessment
   a. What are the weaknesses of the system?
   b. What will successful attacks cost us?
   c. How likely?
4. We use countermeasures
   a. Costs vs. benefits?
   b. Technical vs. nontechnical?

Discussion

How would you break into the COMP lab?

- What is the weakest link?
- What assumptions are made about the security of the lab?
- What ideas do we have that are "outside the box"?

Should you lock your door?

- What are the assets?
- What are the adversaries?
- What does our risk assessment tell us?
- Do we have countermeasures? Should we add any?
- What is the costs/benefit?

Activity: Think Like a Hacker

The activity is on the course website, you can work in groups for this. We will also have some time tomorrow to continue working on this activity.

Questions?

References

William Stallings and Lawrie Brown. 2007. Computer Security: Principles and Practice (2st. ed.). Prentice Hall Press, USA.

What jobs are offered in Cybersecurity?

I have provided a list of some sample jobs you can find in the field of Cybersecurity:

- Security Analyst
- Security Engineer
- Incident Reporter
- Digital Forensic Examiner
- Malware Analyst
- Penetration Tester
- Red Teamer