COMP482
Cybersecurity
Week 2 - Monday

Dr. Nicholas Polanco
(he/him)

KALAMAZOO COLLEGE

Attendance Quiz (in groups)

Sum of Two Numbers

- Problem: Given an array of integers and a target number, write a function to determine if there are two numbers in the array that sum up to the target.
- Example:
  - Input: [2, 7, 11, 15], Target: 9
  - Output: True (because 2 + 7 = 9)

https://forms.office.com/r/BtVc9FH95i

Important Notes

1. You should go to SIP Fest this week!
2. I have updated Kit, the assignments should be visible now.
    a. I am going to go ahead and grade assignments that have been submitted
3. I have reworked the schedule based on topics we are interested in, we have **a lot of things to cover**. I am also taking removing some of the reading elements, I will instead try and suggest TryHackMe modules and write more “hands-on” learning opportunities.
    a. Reminder: TryHackMe grade at the end of the course is meant to see how you engaged with the class

Important Dates (Week 2)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
		Due: Think Like a Hacker Activity		Due: Recent Attacks Reflection 1 Project “Idea” Meeting		

Physical Security in Cybersecurity

Physical Security in Cybersecurity

This is the implementation of measures designed to prevent unauthorized physical access to facilities, equipment, and resources, and to protect personnel and property from damage or harm that could impact digital assets or operations.

Does this always need to focus on “attackers”? What other issues could we run into?

Why Does Physical Cybersecurity Matter?

Physical cybersecurity plays a crucial role in the broader field of cybersecurity because it focuses on the protection of physical assets, infrastructure, and personnel that support digital systems and networks.

While traditional cybersecurity is primarily concerned with protecting digital data, networks, and systems from cyberattacks, physical cybersecurity addresses the physical threats that can compromise those systems.

Image Credit

Types of Physical Security Threats

1. Unauthorized Access
   - Threat: Intruders gain physical access to servers, data centers, or devices.
   - Risks: Data theft, hardware tampering, or installing rogue devices.
   - Examples: Tailgating, stolen keycards, fake credentials.

2. Theft of Equipment
   - Threat: Laptops, hard drives, or servers are stolen.
   - Risks: Loss of sensitive data or intellectual property.
   - Examples: Stealing a backup drive, swiping a laptop from a car or office.

Image Credit

Types of Physical Security Threats (continued)

3. Environmental Threats
   - Threat: Natural disasters or environmental hazards.
   - Risks: Downtime, data loss, hardware damage.
   - Examples: fire, flood, earthquake, extreme temperatures, power outages or surges

4. Vandalism & Sabotage
   - Threat: Deliberate destruction or tampering with hardware.
   - Risks: Service disruption, corrupted data, financial loss.
   - Examples: Cutting cables, damaging servers, smashing cameras.

Types of Physical Security Threats (continued)

5. Interference or Interception (Side-Channel Attacks)
   - Threat: Gaining data through electromagnetic radiation, vibrations, or power fluctuations.
   - Risks: Stealing encryption keys or passwords.
   - Examples: TEMPEST attacks, power analysis, listening to keyboard sounds.

6. Social Engineering (Physical)
   - Threat: Tricking someone into granting access.
   - Risks: Bypasses security without needing technical skills.
   - Examples: Pretending to be a delivery driver or tech support, piggybacking into secure areas, leaving USB drives in parking lots (baiting)

Types of Physical Security Threats (continued)

7. Dumpster Diving
   - Threat: Searching trash for sensitive information.
   - Risks: Recovery of documents, passwords, or credentials.
   - Examples: Unshredded printouts, sticky notes with login info, old hard drives.

8. Insider Threats
   - Threat: Employees or contractors with malicious intent.
   - Risks: Espionage, theft, or sabotage from within.
   - Examples: Copying data to USB, unlocking doors, disabling alarms.

Physical Security Attack Devices

Keylogger

A type of hardware (can also be software) that records every keystroke made on a device. The purpose of a keylogger is to capture user input, which may include passwords, messages, or any other typed data.

Image Credit

Keylogger (continued)

You can find links for these online **to purchase** for ~$50, with online instructions of how to use them.

<u>Why is this is massive problem?</u>

Applications

- Observe WWW, E-mail & chat usage by children and employees
- Monitor employee productivity
- Protect your child from on-line hazards and predators
- Save a copy of typed text
- ...and several more, see keystroke recorder benefits

Image Credit
https://www.wku.edu/news/articles/index.php?view=article&articleid=8295
https://www.keelog.com/usb-keylogger/

KALAMAZOO COLLEGE

Keylogger (continued)

These devices typically have internal memory where the recorded keystrokes are stored. They can store hundreds of thousands of keystrokes.

- After some time, the data can be retrieved manually by disconnecting the keylogger and plugging it into another computer, or, in some models, it may transmit the data over a network.

How many of you check the USB cable on your keyboards when you use a public computer? Have any of you used the computers in this lab? Did you check?

RFID Scanners and Skimmers

RFID (Radio Frequency Identification) technology allows for wireless communication between an RFID scanner (reader) and an RFID tag (a small chip embedded in a card, label, or other object). The RFID scanner sends out radio waves, and the tag responds with its stored information.

Image Credit

RFID Scanners and Skimmers (continued)

Image Credit
https://www.amazon.com/Chainway-C72-Wireless-Inventory-Scanning/dp/B0CCPR58B3
https://www.nwcu.com/learn/how-spot-atm-skimmer

KALAMAZOO COLLEGE

RFID Scanners and Skimmers

Eavesdropping/Skimming:

- The RFID scanner checks nearby RFID tags (usually from your wallet or purse).
- The scanner captures the unique ID or other data stored on the RFID chip, such as your name, card number, or even personal details if it's an ID card.
    - They can then clone the information onto another RFID tag or card.

Image Credit

USB Rubber Ducky

A type of USB device that looks like an ordinary flash drive, but it functions as a powerful hacking tool. It is often used by security professionals or hackers for penetration testing and exploiting vulnerabilities.

Image Credit

USB Rubber Ducky (continued)

Who here would plug in a USB they found on the ground?

Image Credit
https://thehbpgroup.co.uk/blog/does-your-business-fear-the-rubber-ducky

KALAMAZOO COLLEGE

USB Rubber Ducky (continued)

They function as a keyboard emulator, so it automatically sends pre-programmed keystrokes to the computer, simulating the actions of a human typing on a keyboard. This allows it to execute commands or scripts on the target system.

Why is this a problem? Wouldn't you just be able to unplug something that started to type things?

Image Credit

Additional Hardware

We have a lot more devices we *could* (or can, in the future) talk about, but I hope you begin to understand the importance of physical security!

If you are interested, you can see more at a few of the websites below:

https://shop.hak5.org/

Physical Security Best Practices

Controlled Access to Physical Locations

What can we do?

Image Credit

KALAMAZOO COLLEGE

Controlled Access to Physical Locations

What can we do?

- Keycard systems or biometric scanners for building and room access.
- Security personnel to monitor entrances and exits.
- Visitor logs and screening processes to track non-employees in sensitive areas.
  - Example: Data centers with multi-layered access controls (e.g., biometrics + keycards + physical locks).

Image Credit

Device Security

What can we do?

Device Security

What can we do?

- Locking devices to furniture with cable locks (e.g., laptops, desktops).
- Screen privacy filters to avoid unauthorized viewing.
- Encrypted storage devices to protect data in case of theft.
  - Example: Employees using physical locks on laptops to prevent theft in public areas (cafes, airports).

Image Credit

Monitoring and Surveillance

What can we do?

Image Credit

KALAMAZOO COLLEGE

Monitoring and Surveillance

What can we do?

- CCTV cameras to monitor critical areas (e.g., server rooms, entrance/exits).
- Alarms and motion detectors to detect unauthorized access or movement.
- 24/7 surveillance for sensitive facilities, especially data centers or areas with high-value assets.
  - Example: A server room with CCTV and motion-triggered alarms to prevent unauthorized access after hours.

Image Credit

Secure Disposal of Physical Assets

What can we do?

Image Credit

KALAMAZOO COLLEGE

Secure Disposal of Physical Assets

What can we do?

- Data wiping and destruction before disposing of or recycling old devices (hard drives, USB drives).
- Shredding or physical destruction of hard drives to prevent data recovery.
- Proper disposal protocols for electronic waste (e-waste).
  - Example: A company ensuring all sensitive data is completely erased from devices before sending them for recycling.

Image Credit

Employee Awareness and Training

What can we do?

Image Credit

KALAMAZOO COLLEGE

Employee Awareness and Training

What can we do?

- Regular security training on physical asset protection for all employees.
- Awareness programs to ensure staff understand the importance of securing devices and facilities.
- Reporting mechanisms for suspicious activities or lost/stolen devices.
  - Example: Employees trained to secure devices when they leave their desks, including locking their computers and ensuring sensitive papers are properly stored.

Image Credit

Key Components of Physical Security in Cybersecurity

1. Access Control Systems
   a. This can include locks, key cards, biometric scanners, PIN pads
   b. Ensures that only authorized personnel can access sensitive areas like server rooms or data centers.

2. Surveillance and Monitoring
   a. CCTV, motion detectors, security guards
   b. Provides real-time monitoring to deter and detect unauthorized access or suspicious activities.

3. Environmental Controls
   a. Fire suppression systems, HVAC, flood protection
   b. Protects systems from environmental threats that could cause downtime or data loss.

Image Credit

Image Credit

https://www.data-path.co.uk/the-main-6-benefits-of-access-control-systems/
https://www.bayalarm.com/blog/how-do-motion-sensors-work-a-guide/
https://canovate.com/en/what-is-a-fire-suppression-system/

KALAMAZOO COLLEGE

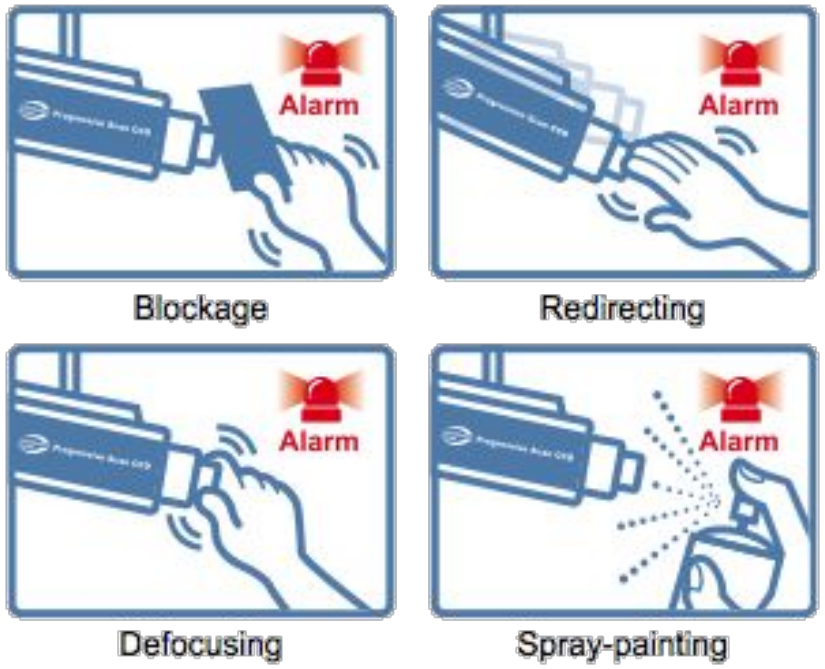
Key Components of Physical Security in Cybersecurity (continued)

4. Intrusion Detection Systems
   a. Sensors, alarms, and tamper-detection mechanisms
   b. Alerts personnel to unauthorized access attempts or breaches in real-time.

5. Hardware Security
   a. Securing endpoints, servers, network equipment
   b. Prevents tampering, theft, or manipulation of physical devices that could compromise digital systems.

6. Personnel Security
   a. Employee ID verification, background checks, training
   b. Ensures that staff are trustworthy and aware of the importance of physical and digital security practices.

Image Credit



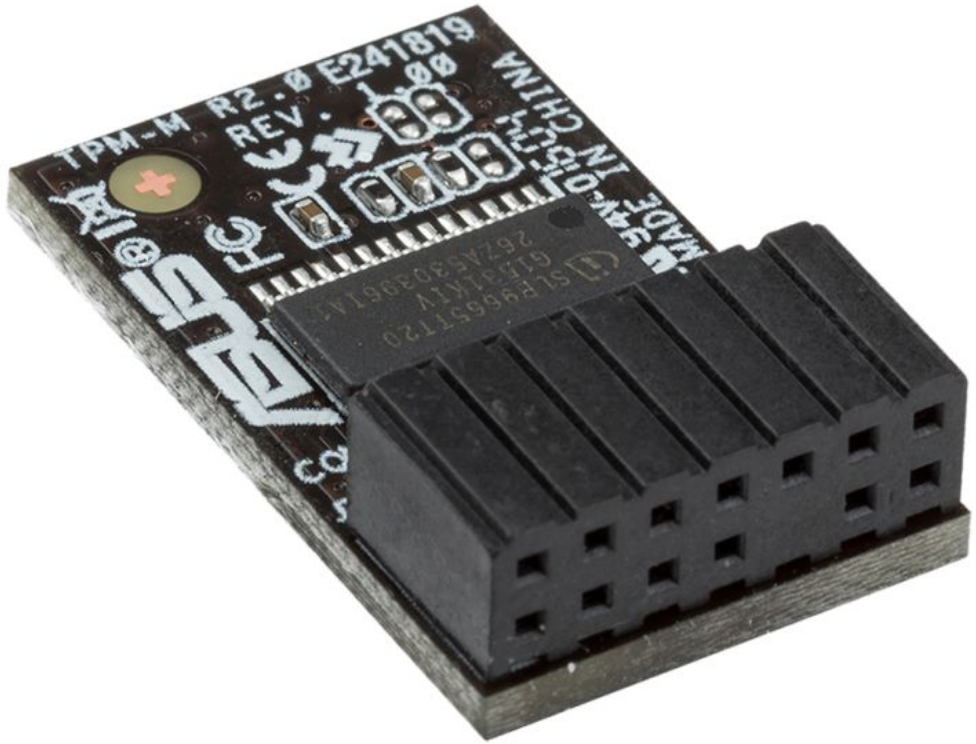


Image Credit

https://camera-sdk.com/p_6821-how-to-implement-tampering-detection-in-c-sharp.html

https://www.pcmag.com/explainers/what-is-a-tpm-and-why-do-i-need-one-for-windows-11

KALAMAZOO COLLEGE

Debate Team (not really)

We are going to be moving around for this activity and choosing sides!

You are to look at the prompt, and choose **whether you agree or disagree!** The agree students will be on one side, and the disagree students will be on the other.

- Your group should discuss 1 reason you want to share with the class.
- These teams will each share, then afterwards members can chose to **stay or go to the other side.**
- *This is intended to be **fun**, please be respectful!

Image Credit

Physical security is more important than cybersecurity in protecting an organization's critical assets.

Biometric access controls (fingerprints, facial recognition) are essential for securing physical assets, even if they come with privacy concerns.

CCTV surveillance cameras should be implemented in all areas of an organization, including employee workspaces, to prevent physical security breaches

Remote work makes it impossible to secure physical assets effectively, especially in a world where employees use personal devices for work.

Advanced physical security technologies, like smart locks and facial recognition, provide a false sense of security and distract from more important cybersecurity measures.

Questions?