SIU Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 3: Review of Cybersecurity

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

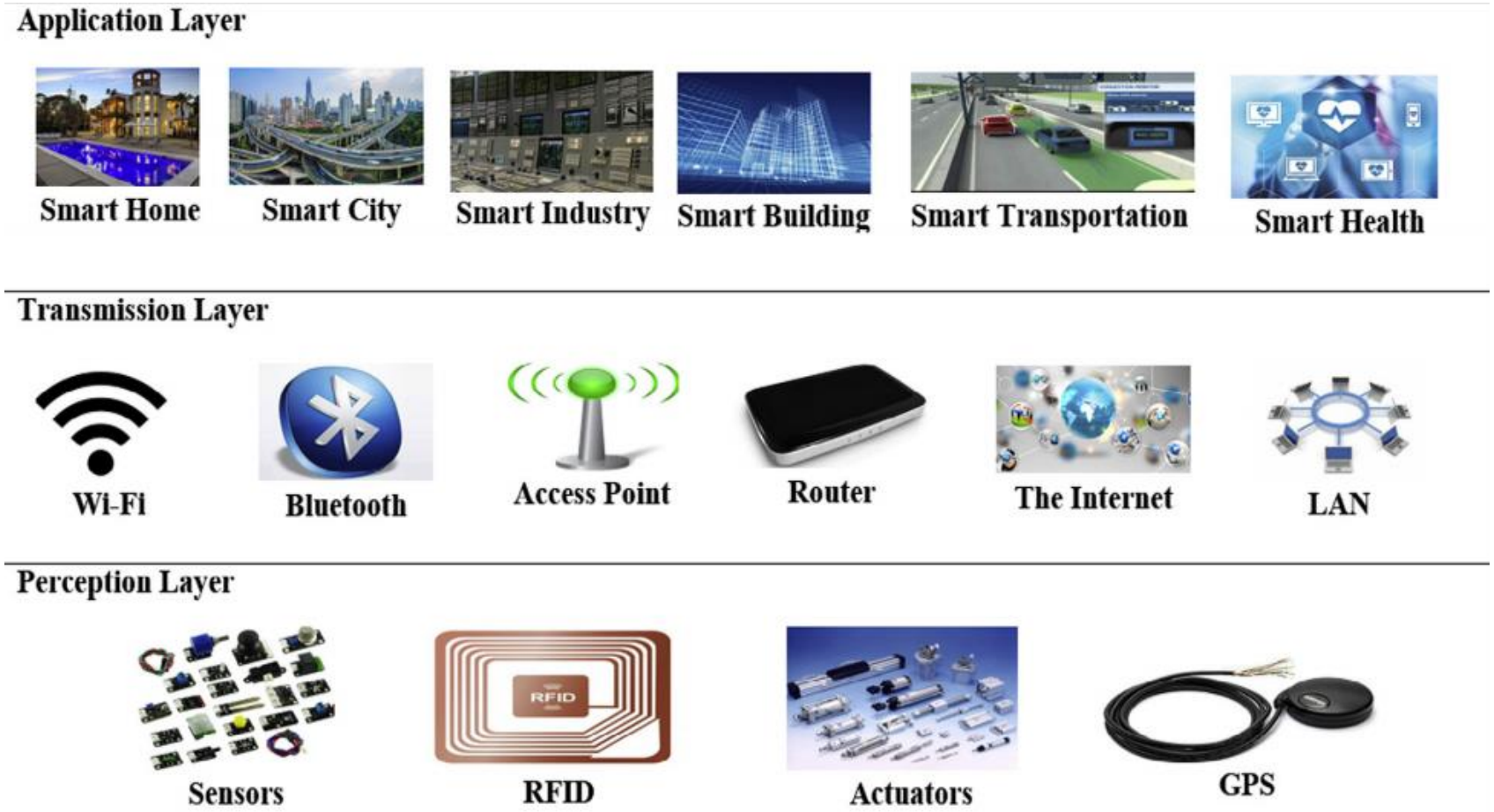
Introduction to Cybersecurity

- Its goals

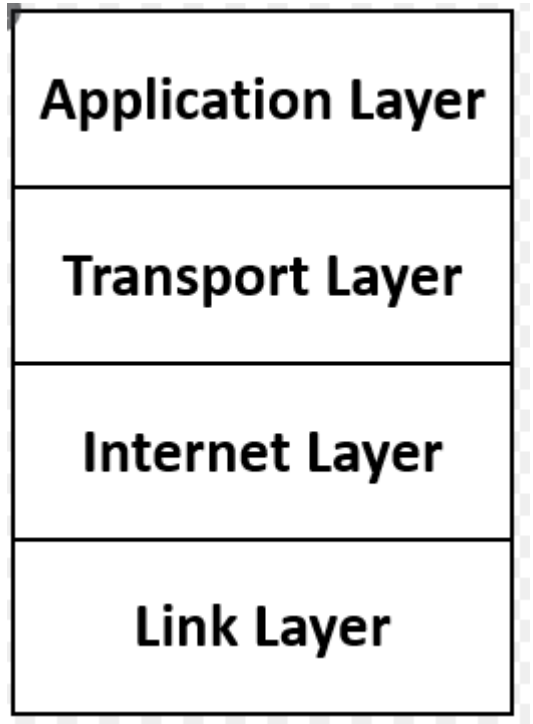
Introduction to Cyberattacks

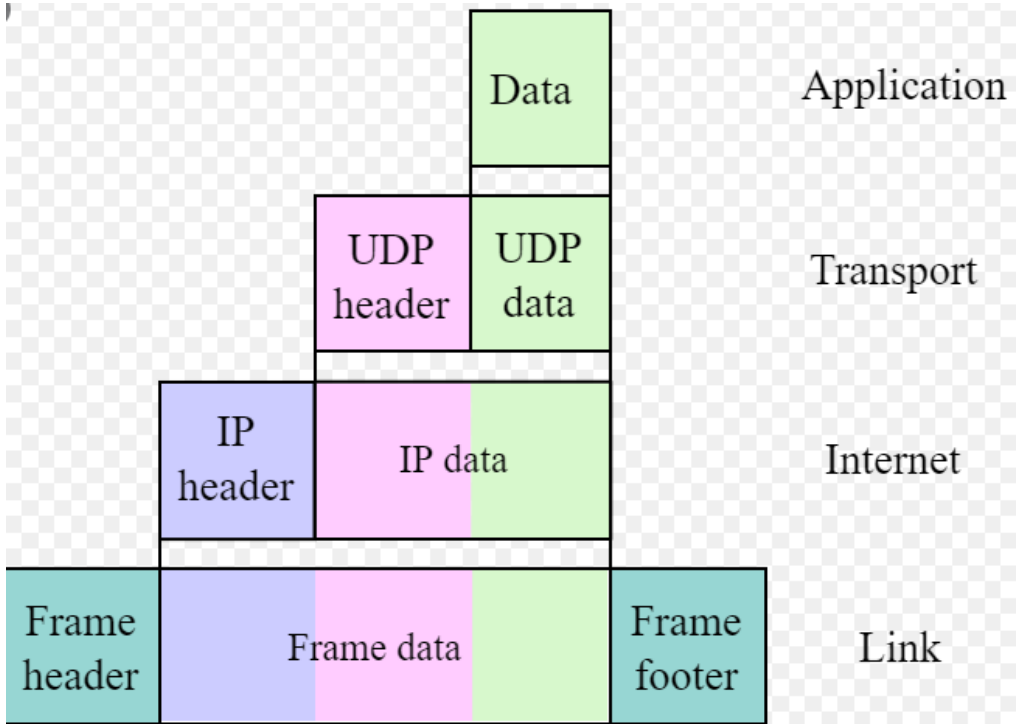
- Some attack examples

Recall: CPS Architecture



Recall: Computer Networks





Cybersecurity (Computer Security)

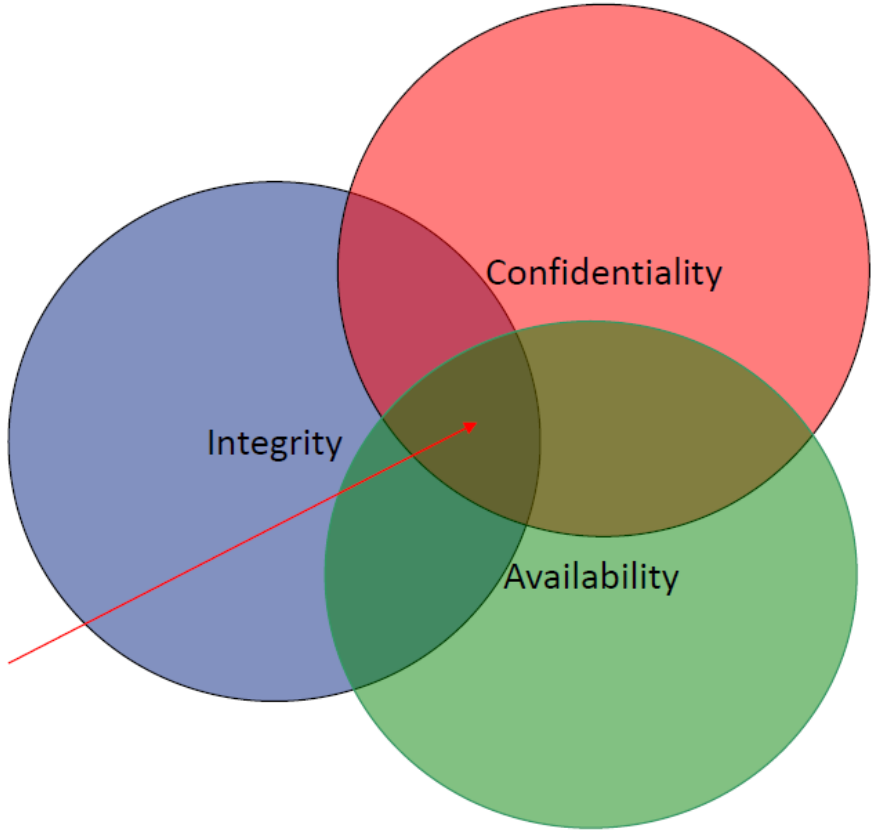
NIST definition:

- "The protection afforded to an automated information system in order to attain the applicable objectives of preserving integrity, availability, and confidentiality of information system resources"
  - Hardware, software, information, data, telecommunications, etc.

Cybersecurity goals

CIA Triad:

- Confidentiality
- Integrity
- Availability



Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Data Confidentiality:

- Private or confidential information is not revealed to unauthorized individuals

Privacy:

- Users control what information about them can be
- Collected
- Stored
- By whom

Integrity

Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Data Integrity

- Information and programs are changed only in specified and authorized manner

System Integrity

- System performs intended function free from unauthorized system manipulation

Availability

Ensuring timely and reliable access to and use of information

Actions by an attacker do not prevent users from having access to use of the system

- Enable access to data and resources
- Timely response
- Fair resource allocation

Some Additional Required Concepts

Authenticity

- Being able to be verified and trusted
- Confidence in the validity of a message (originator)

Accountability

- Actions of an entity can be traced to it
- Tracing a security breach to a responsible party

Examples

Confidentiality

- Student grades
- Available only to student, parents, employer

Integrity

- Patient information e.g., allergies
- Can lead to loss of human life

Availability

- Web service
- Unavailability can lead to financial loss

Cyber attack

The Internet Engineering Task Force defines attack as:

- An assault on system security that derives from an intelligent threat, i.e., 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

Cyber attack: any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems

Potential Impacts of Cyber attacks

They can disrupt phone and computer networks or paralyze systems, making data unavailable, failure of military equipment and breaches of national security secrets

Significant impacts for the business;

- The loss of customer trust
- Data theft
- Potential revenue losses
- Intellectual property theft

$221,836.80 cost per attack;

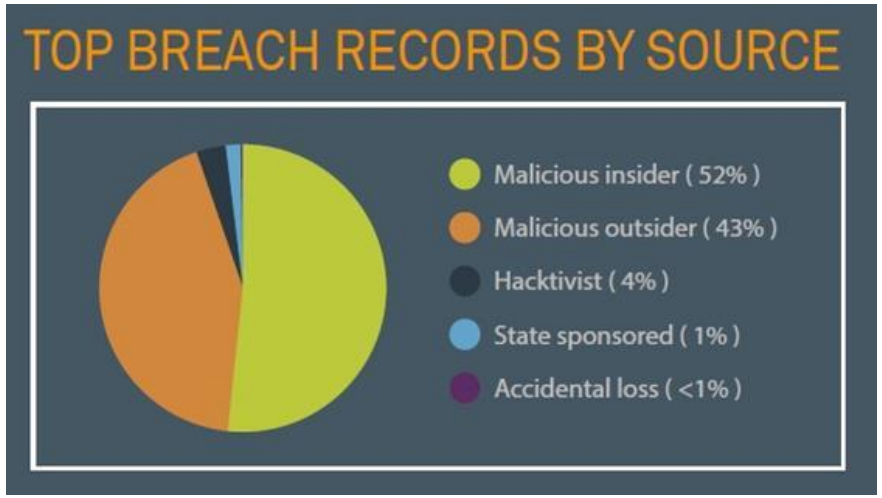
- The cost of downtime associated with internet service an

hour outages caused by DDoS attacks in 2018

Type of Cyberattacks: Attacker's Location

Insider vs. Outsider Attacks:

- An inside attack is an attack initiated by an entity inside the security perimeter (an "insider"),
  - An entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization
- An outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider")



Type of Cyberattacks: Attacker's Behavior

Active vs. Passive Attacks:

- An active attack attempts to alter system resources or affect their operation
  - Involve some modification of the data stream or the creation of a false stream
- A passive attack attempts to learn or make use of information from the system but does not affect system resources
  - Eavesdropping, monitoring, etc.

Passive Attacks

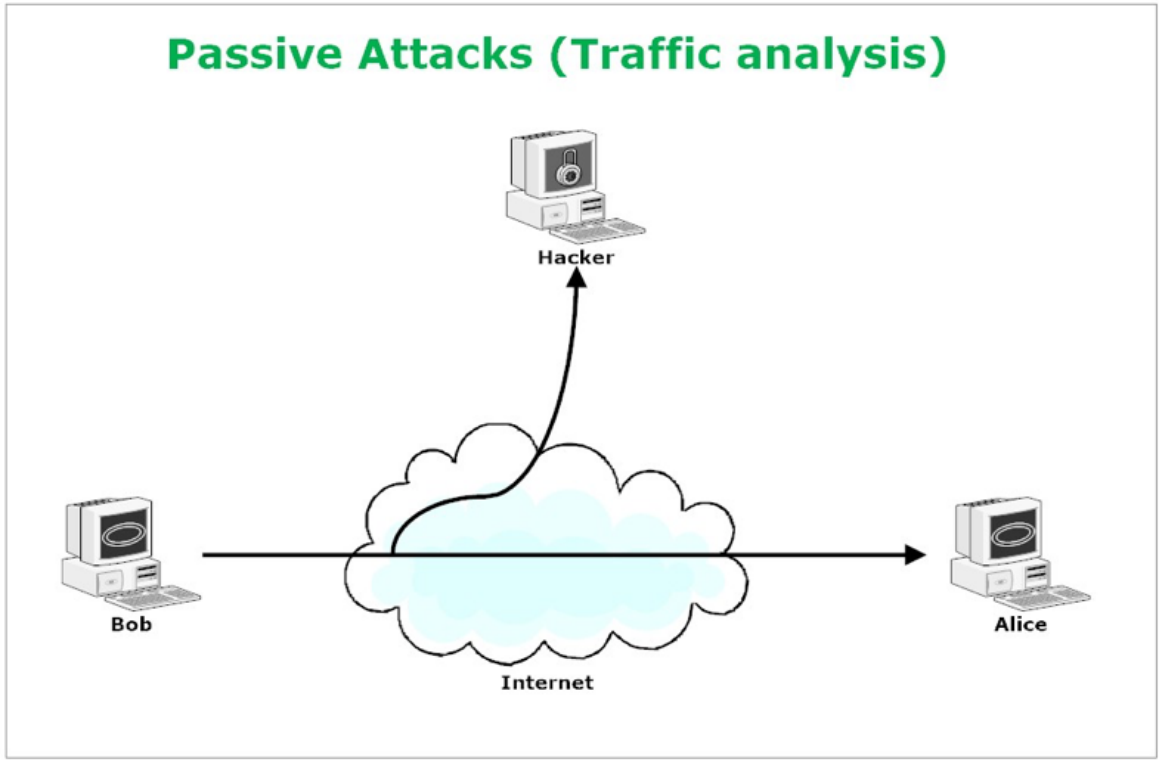
Computer and network surveillance

Network

- Wiretapping
- Fiber tapping
- Port scan

Host

- Keystroke logging
- Backdoor



Active Attacks

Denial-of-service (DoS) attack

- Distributed Denial of service (DDoS) attack

Spoofing

Network based:

- Man-in-the-middle

Host based:

- Buffer overflow
- Format string attack

Some Common Attack Types

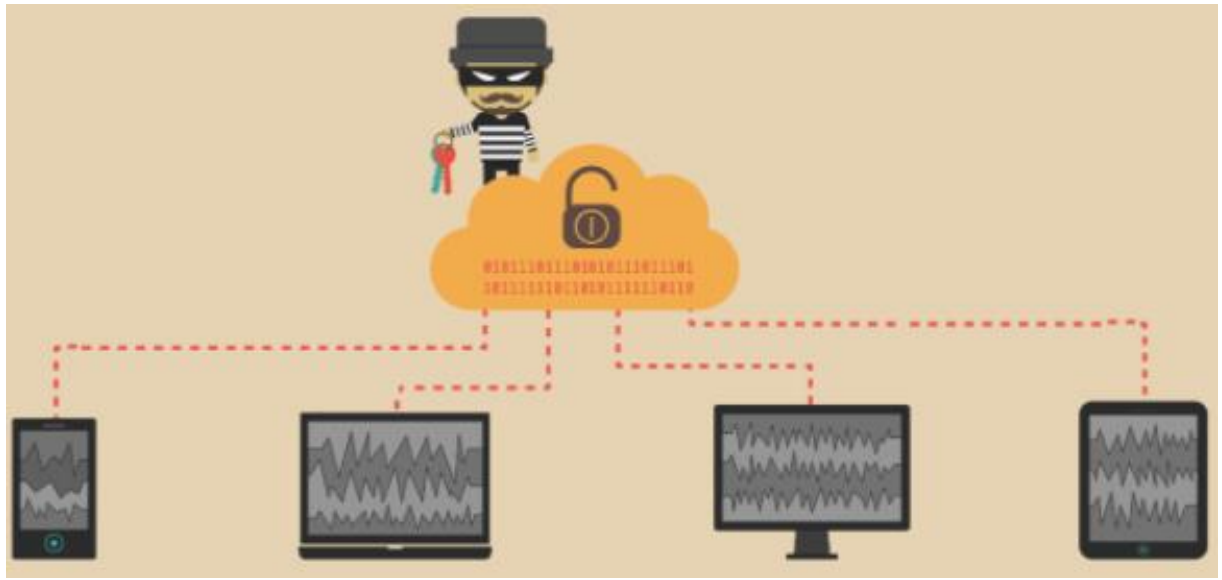
Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

Man-in-the-middle (MitM) attack

Phishing and spear phishing attacks

SQL injection attack

Malware attack

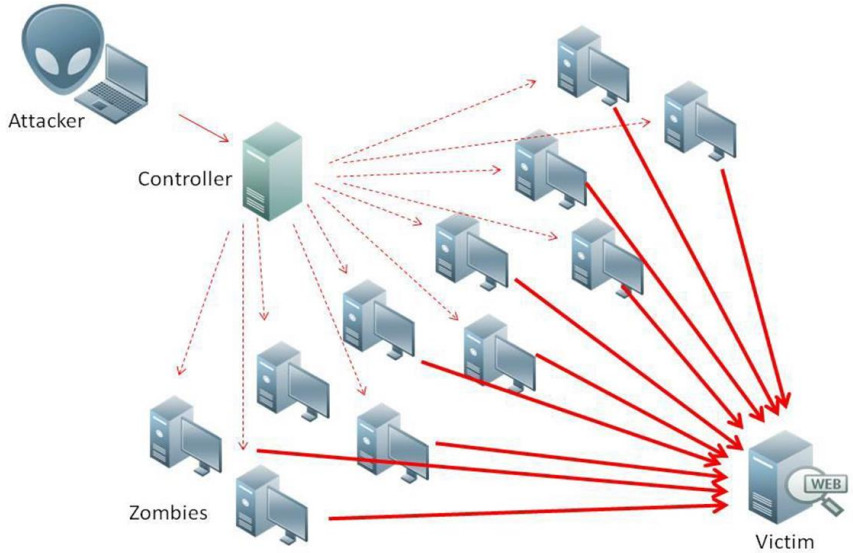


DoS and DDoS

DoS attack overwhelms a system's resources so that it cannot respond to service requests

DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker

- TCP SYN flood attack, etc.

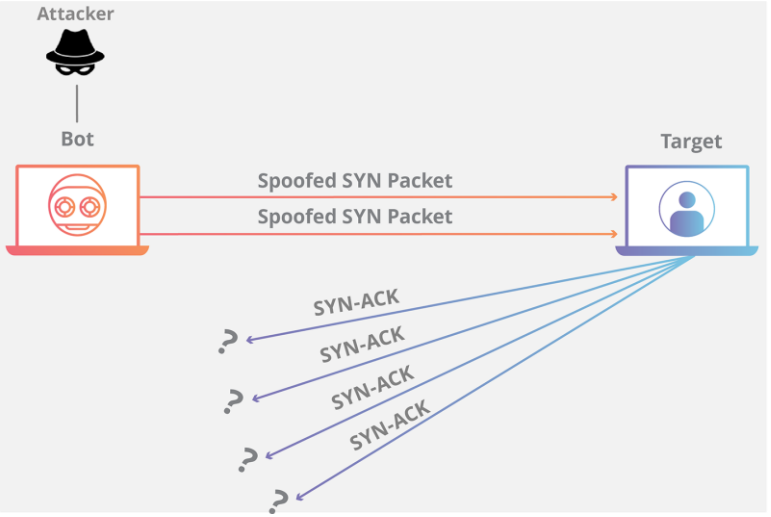


TCP SYN flood attack

Exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake

The attacker's device floods the target system's small in-process queue with connection requests, but it does not respond when the target system replies to those requests

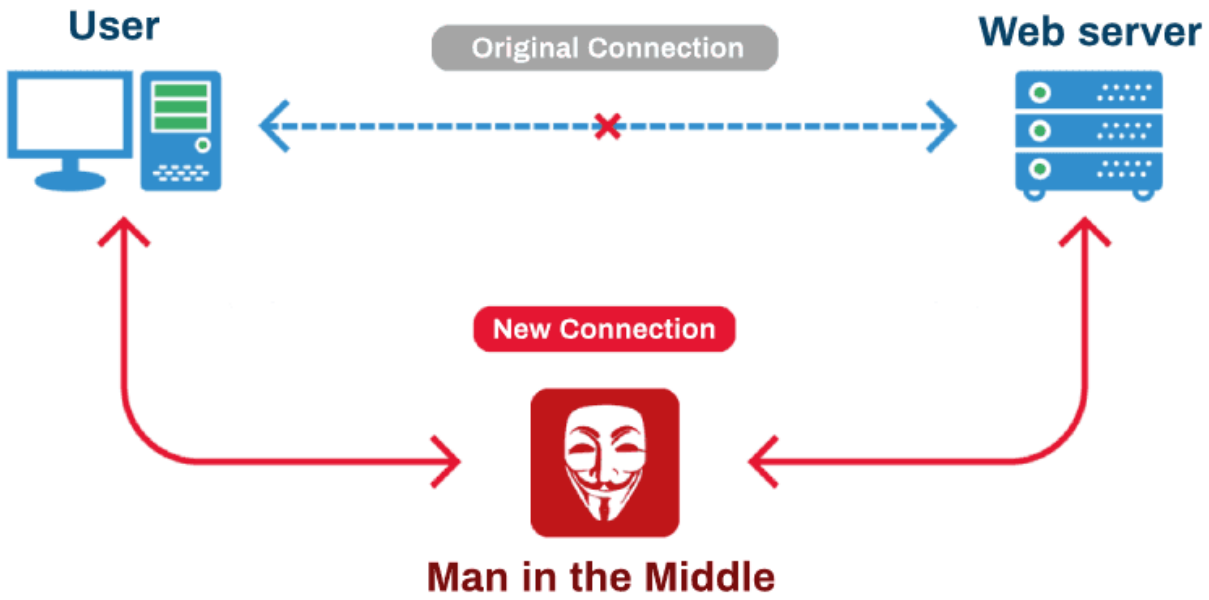
- This causes the target system to time out while waiting for the response from the attacker's device, which makes the system crash or become unusable when the connection queue fills up



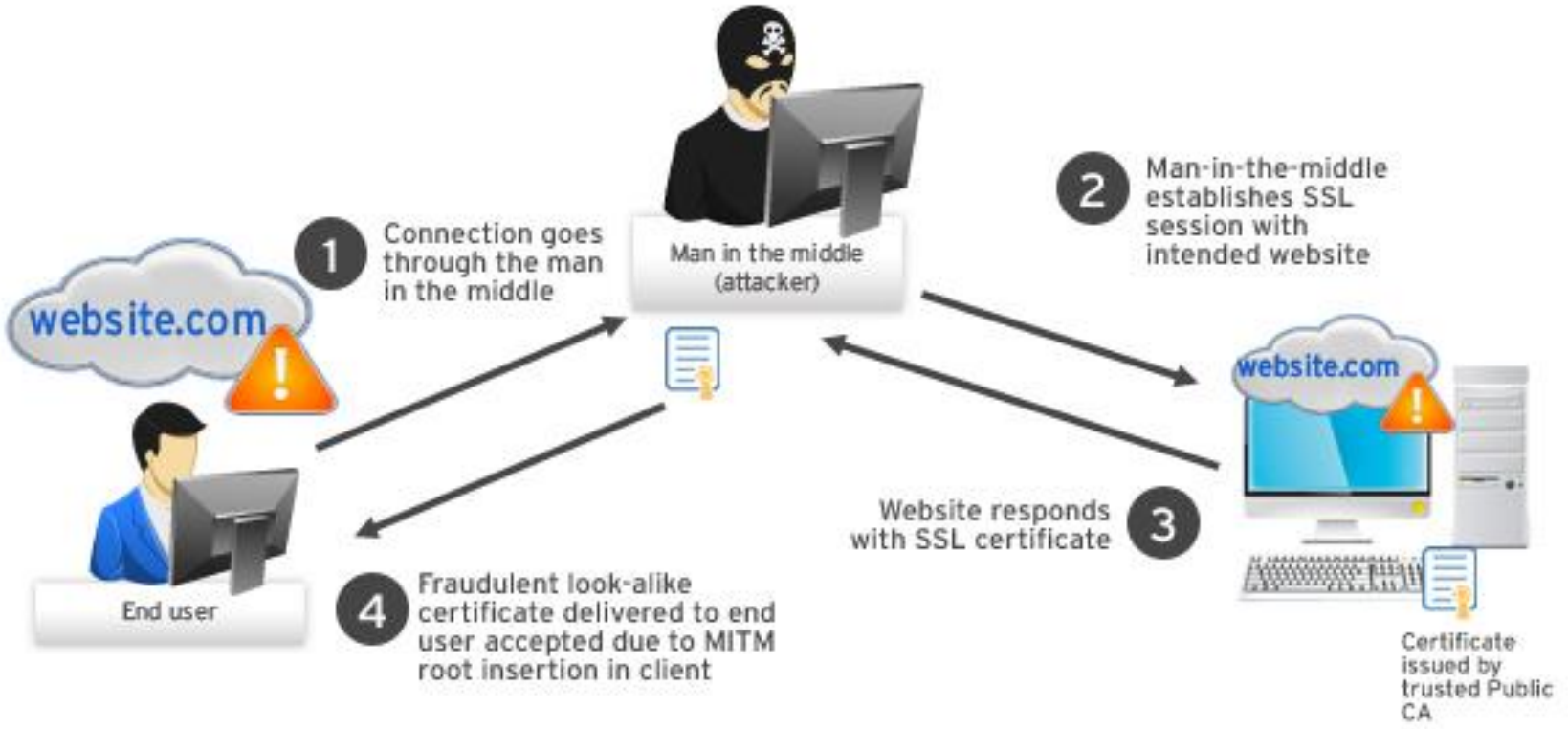
Man-in-the-middle (MitM) attack

A MitM attack occurs when a hacker inserts itself between the communications of a client and a server. Some common MitM attacks:

- Session hijacking
- IP Spoofing
- Replay



MitM: How it works

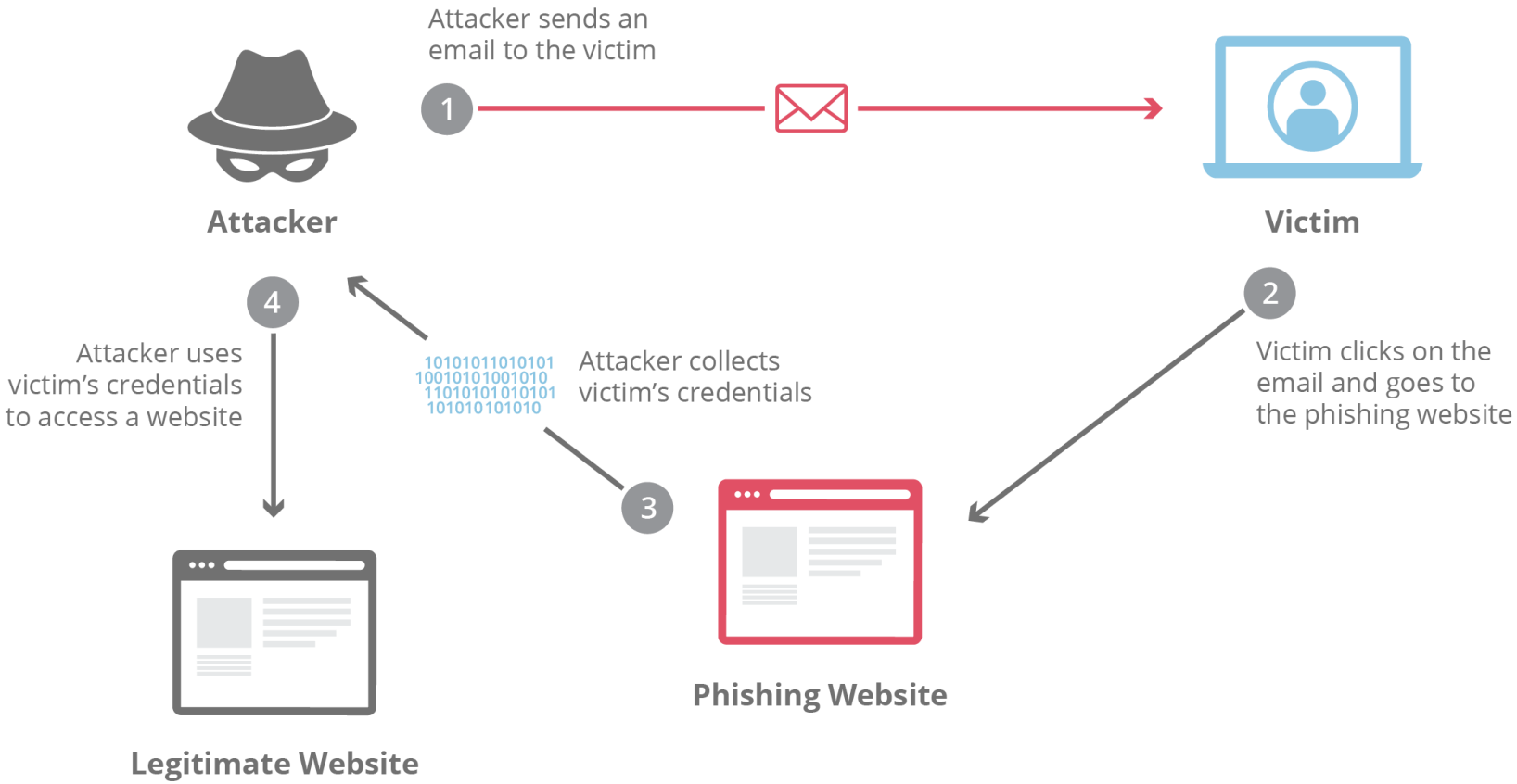


Phishing and spear-phishing attacks

Practice of sending emails which appeared to be from trusted sources with the aim of getting more personal information or appealing users to do something

- Combines social engineering and technical trickery that could involve an attachment to an email which loaded malware into your device
- The attacker devices link with an illegitimate website that tricks you into downloading malware or offering over your personal information

Phishing attacks: How it is done



SQL Injection Attacks

```
# Define POST variables
uname = request.POST['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd + "'"

# Execute the SQL statement
database.execute(sql)
```

password' OR 1=1

```
SELECT id FROM users WHERE username='username' AND password='password' OR 1=1'
```

Malware attack

Malicious software that's put in your system while not your consent

It will attach itself to legitimate code and propagate; it will lurk in helpful applications or replicate itself across the net.

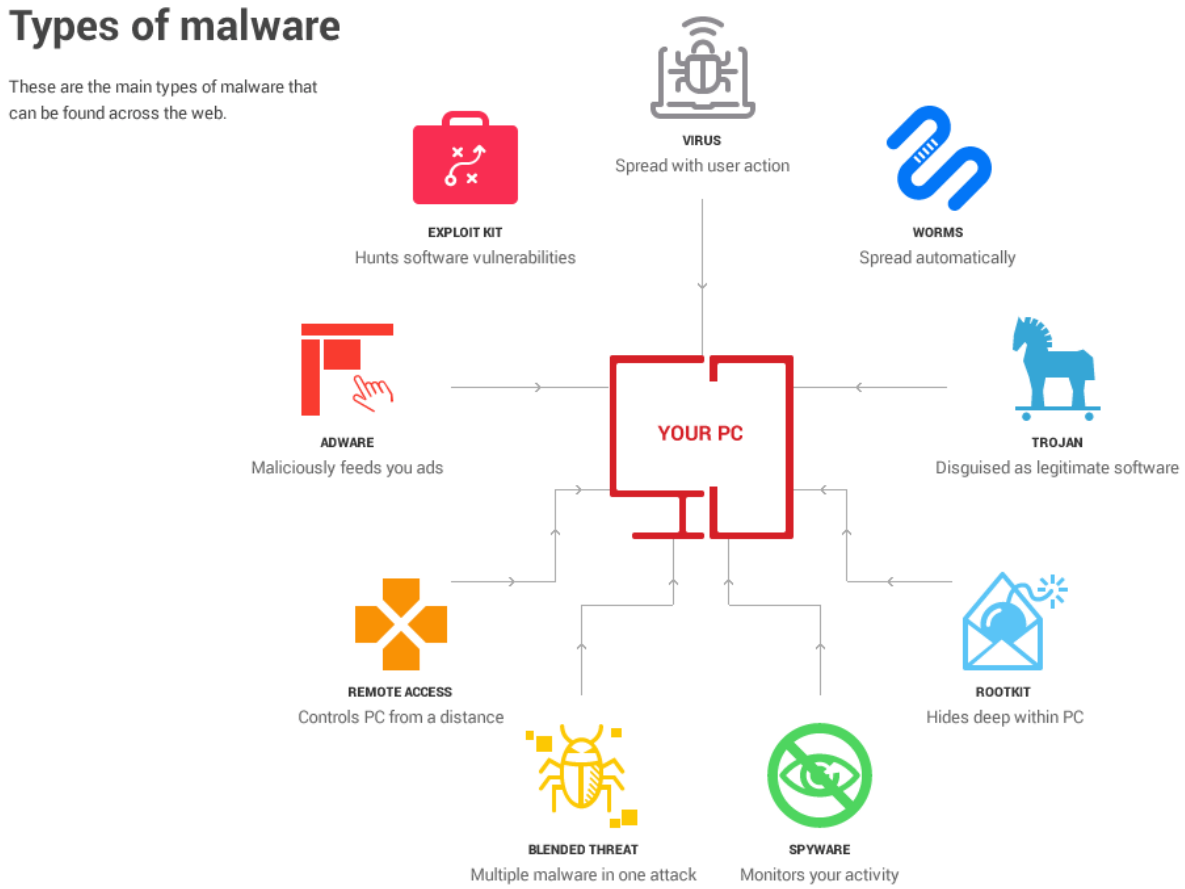
- Examples: viruses, trojans, worms, ransomware, etc.

Types of Malware

Virus

Worms

Trojan



Discussion

Which attack type(s) do you think/believe the most used against CPS?

- DDoS
- SQL Injection
- Phishing
- MiTM
- Malware