FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

Department of Computer Science

# CSE 4820: Wireless and Mobile Security

## 1. Preliminaries

**Dr. Abdullah Aydeger**
**Location: Harris Inst #310**
**Email: aaydeger@fit.edu**

# Outline

Background: Computer Networks

Background: Cybersecurity Basics

# Computer Networks

Connects two or more computing devices

- Computers, phones, IoT

Various ***protocols*** between different device set

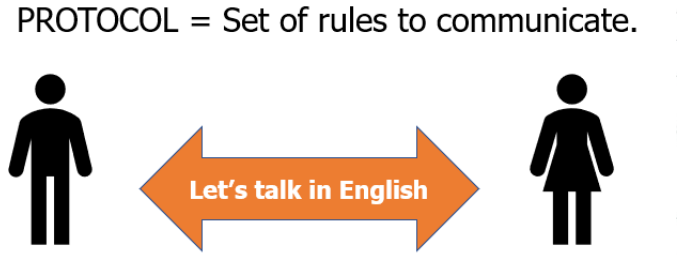
- Protocol define the rules of how they interact

Example daily uses:

- Virtual classrooms, messaging, emails, social media posts, etc.

# Protocols

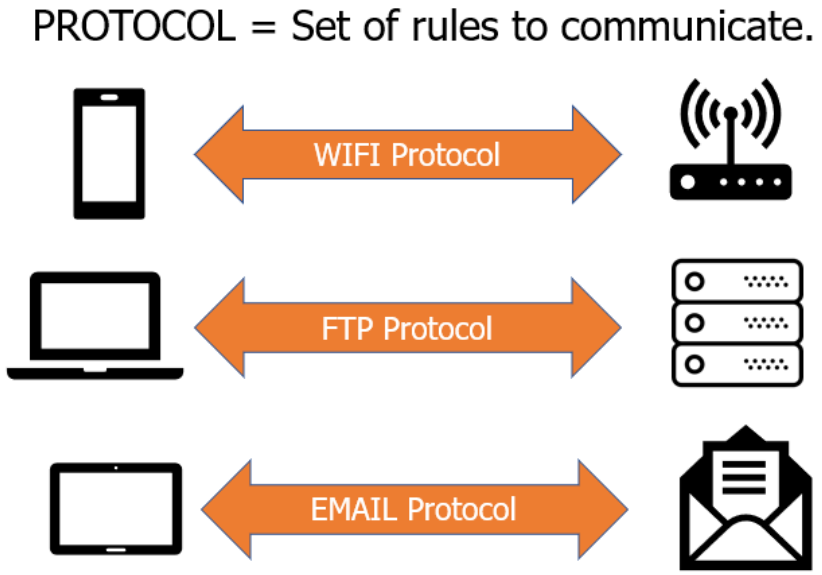
- "The official procedure or system of rules governing affairs of state or diplomatic occasions"




- A communication protocol:
  - System of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity
  - Defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods

# Communication Protocols

- Each protocol defines different set of:
  - Format of messages
  - Order
  - Actions
  - Security?
- Protocol runs on multiple nodes, and implements certain functionality of a single layer
  - Works through packet header



# How to Design Network Protocols

- Internet has billions of devices
- How to manage the different devices to talk to each other
- How to deal with maintenance, scalability, accountability of them?

- Solution: Divide and control

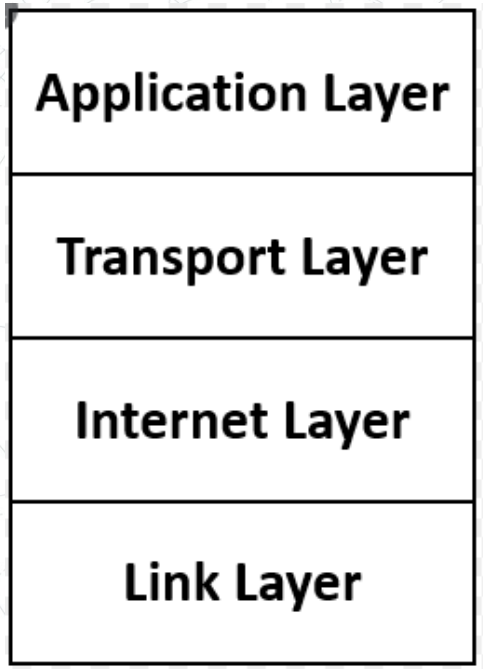
# Layering

- A way of abstracting and organizing functionality
  - Without specifying implementation details
- Eases maintenance, updating of system
- Provides scalability

- => Leads to design protocol stack by creating different layers for different tasks

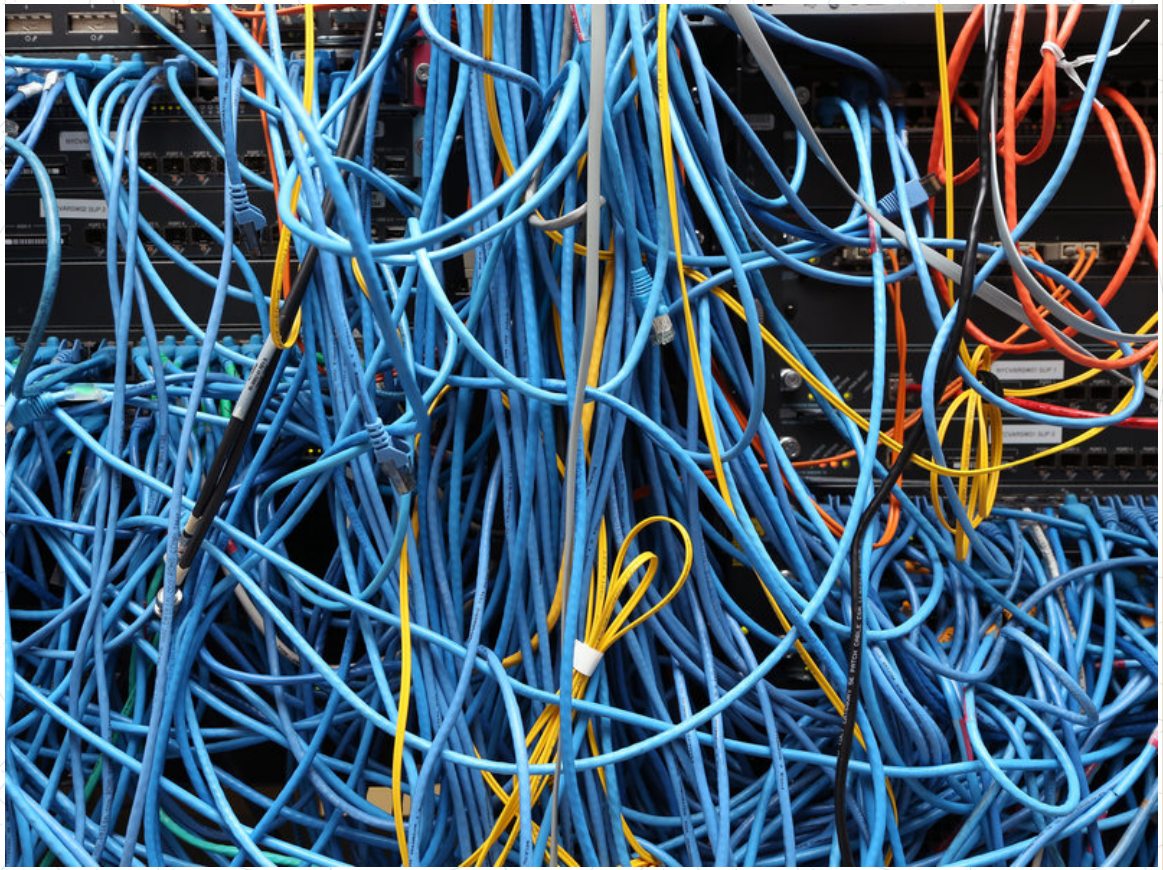
# Network Protocols

- **Application Layers:** End-user applications
- **Transport Layer:** Data transfer from end to end
- **Internet (Network) Layer:** Routing of data from source to destination
- **Link (Physical) Layer:** Physical media carrying the data



# Link Layer

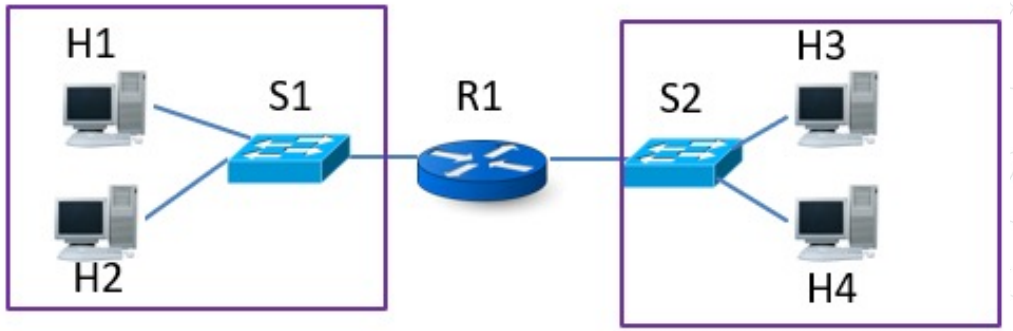
- Link = Medium + Adapters
- Enable host-to-host communication within a single local area network (LAN)



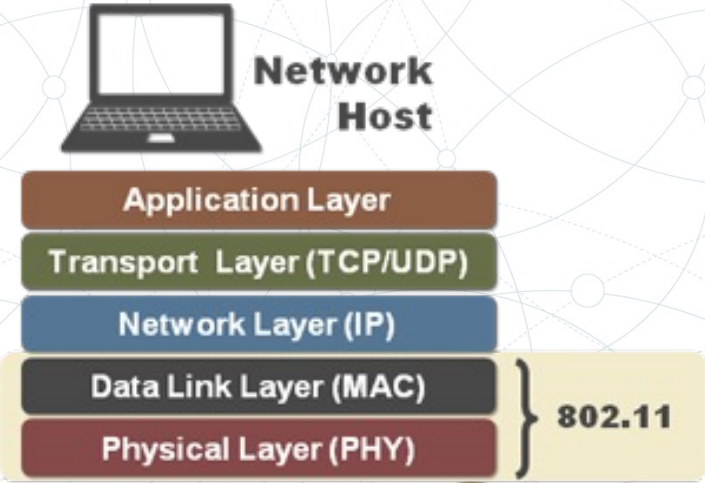
# Some "Link" Examples

# Some "Network Adapters"


# Network Layer

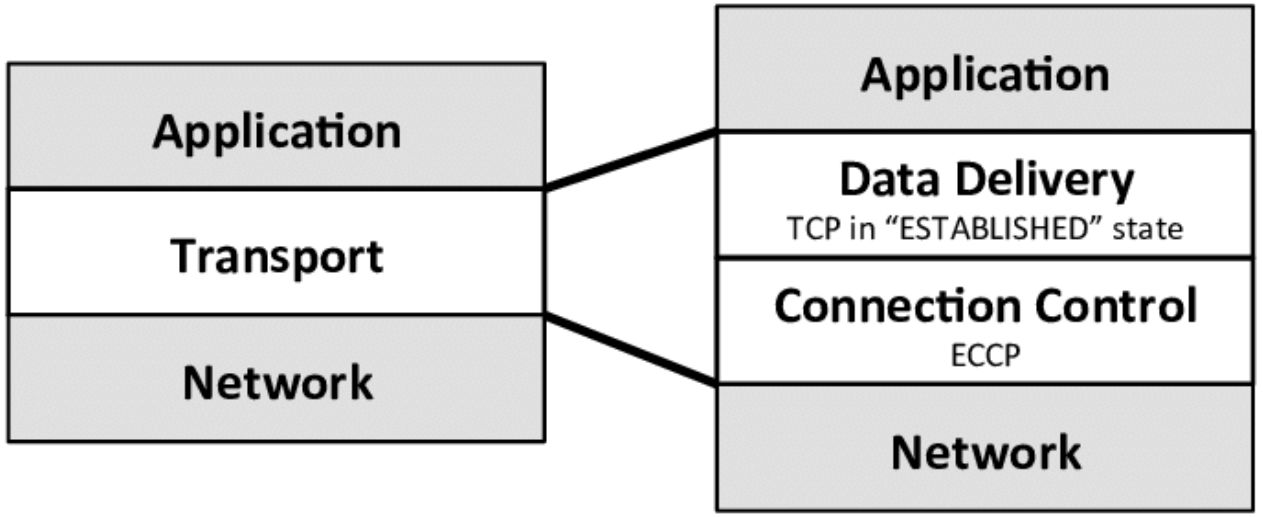



- Connecting networks
  - Forwarding: move from one port to another
  - Routing: calculate the route it should take to arrive destination
- Internet Protocol (IP): IP addresses
  - IPv4, e.g. 157.23.54.201
  - IPv6, e.g. 3002:0db8:85a3:ffff:0000:8a2e:0370:7114



# Transport Layer

- Layer 1 & 2 deal with forwarding packets from one place to another
  - Mechanisms for finding paths, locating destination, etc.
- Layer 3 provides two extra functionality on top of forwarding

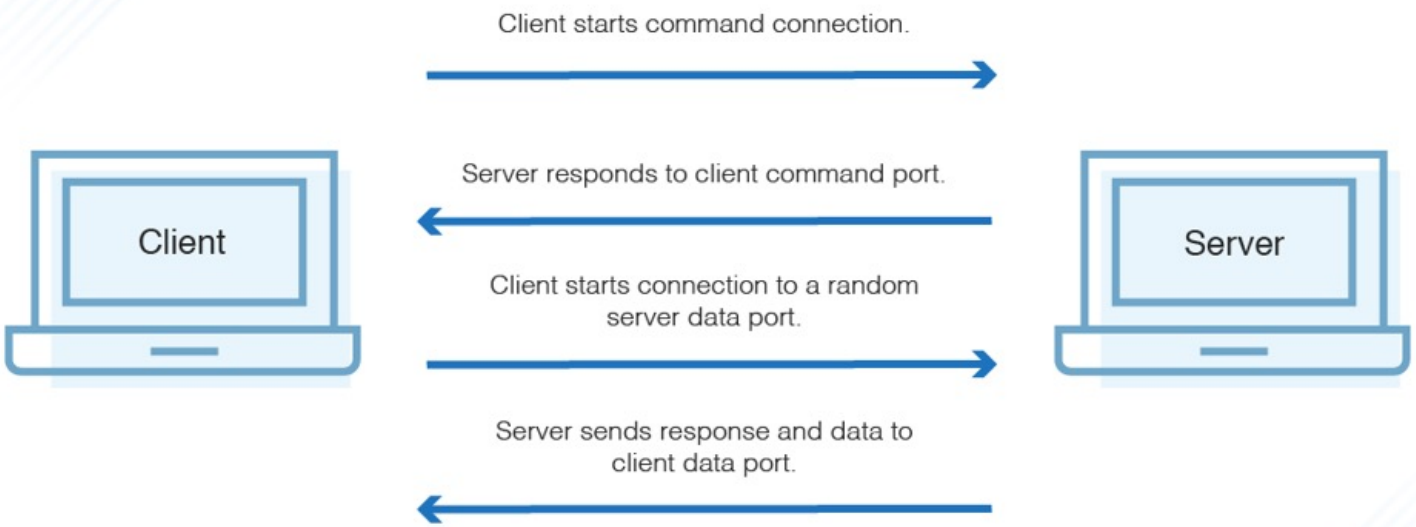


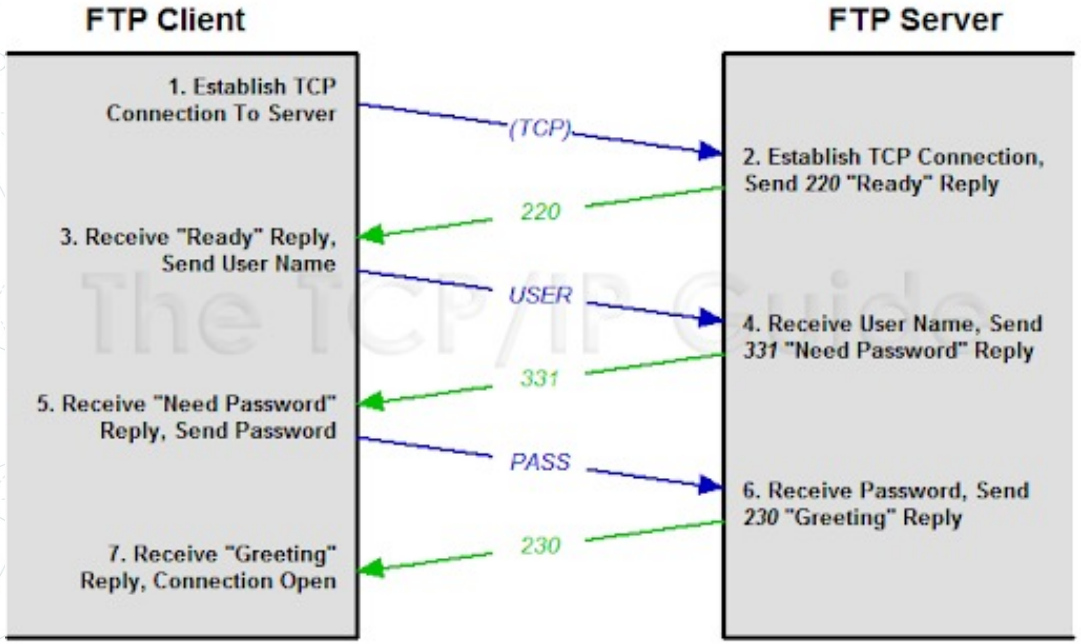
# Application Layer

- It defines:
  - types of messages exchanged,
    - request, response
  - message syntax:
    - what fields in messages & how fields are delineated
  - message semantics
    - meaning of information in fields
  - *rules* for when and how processes send & respond to messages

- Open protocols:
  - defined in RFCs
  - allows for interoperability
  - e.g., HTTP
- Proprietary protocols:
  - e.g., Zoom, Skype

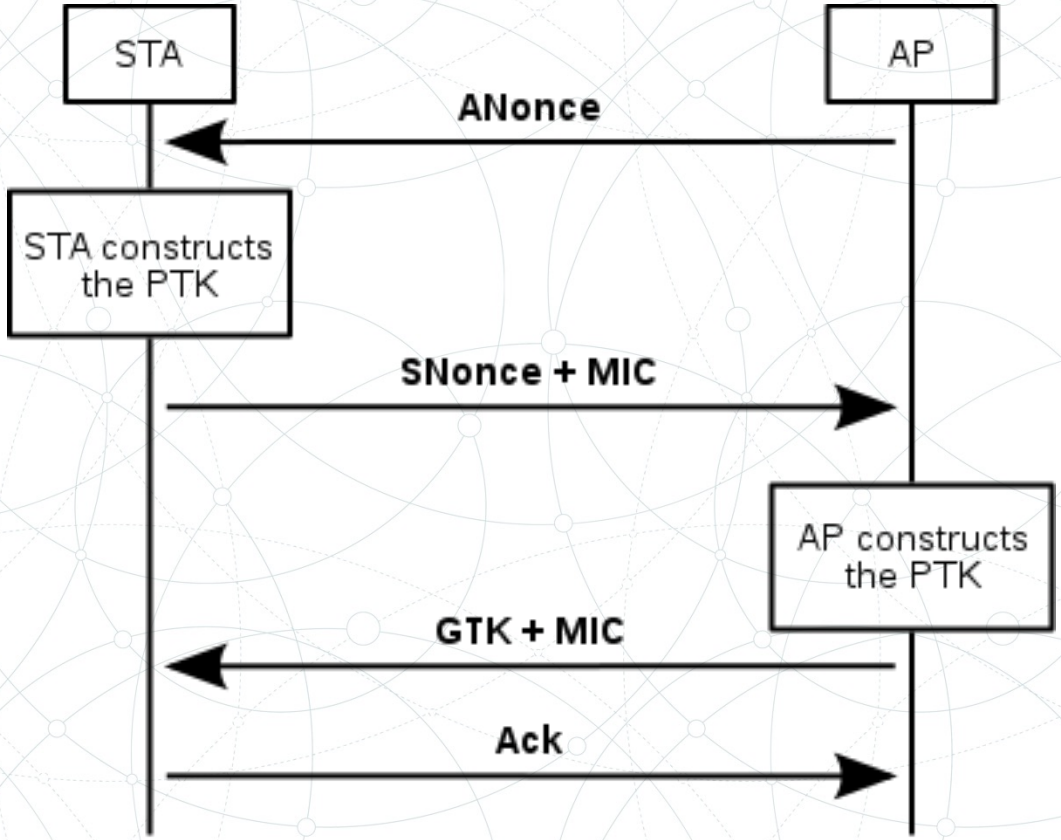
# File Transfer Protocol (FTP) Steps



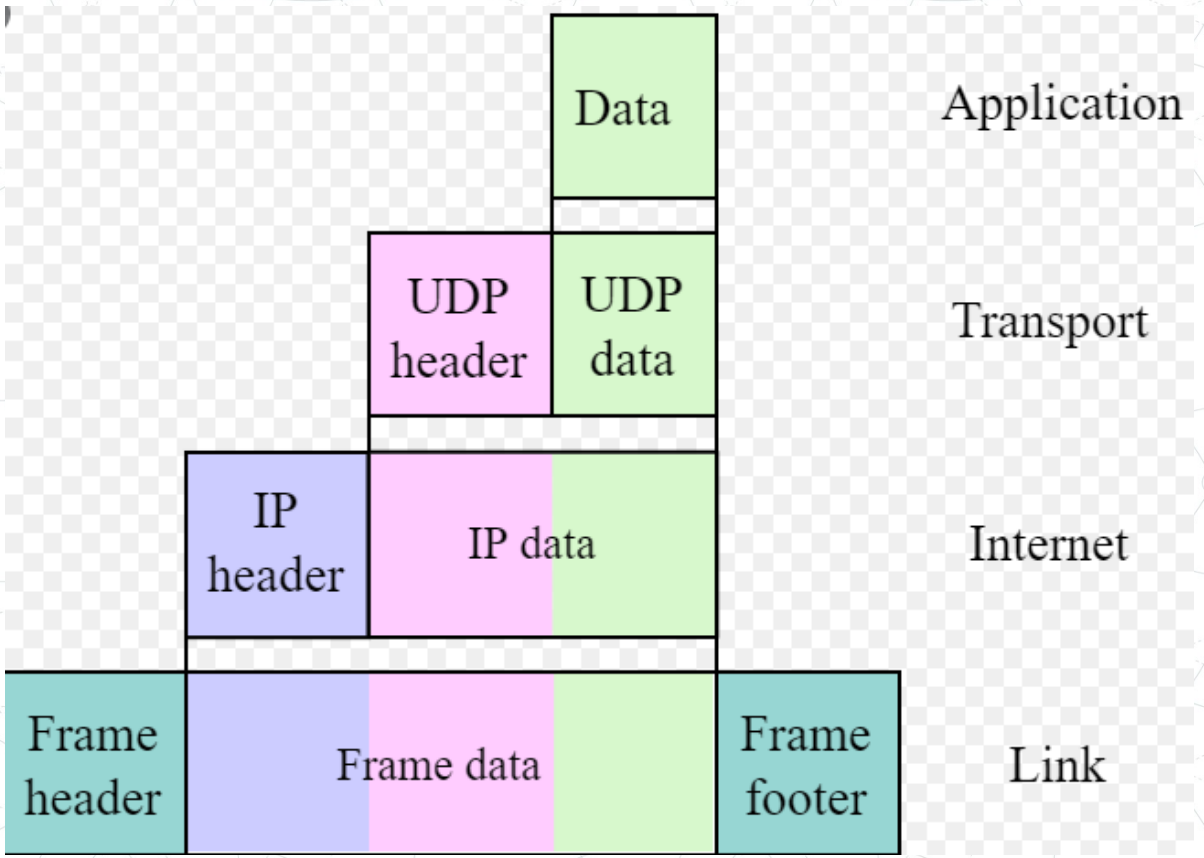

https://datatracker.ietf.org/doc/html/rfc959

# WiFi (IEEE 802.11)



# Data Communication via Networks

- Application data; user input
- Transport layer adds its header
  - TCP or UDP
- Internet layer adds
  - IP header (or ICMP)
- Link Layer adds extra info
  - Such as error correction, etc.



# Data in Layers

- Full data communicated:

```
Frame 5438: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
    Interface id: 0 (\Device\NPF_{[redacted]-2B8C-40B9-BA81-[redacted]})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 17, 2021 21:35:53.945308000 Central Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1629254153.945308000 seconds
    [Time delta from previous captured frame: 0.004450000 seconds]
    [Time delta from previous displayed frame: 0.004450000 seconds]
    [Time since reference or first frame: 38.141095000 seconds]
    Frame Number: 5438
    Frame Length: 94 bytes (752 bits)
    Capture Length: 94 bytes (752 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ssl]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
```

# Data in Layers

- Data in physical layer (or MAC layer):

```
Ethernet II, Src: D-LinkIn_e9:[redacted] (c0:a0:bb:e9:[redacted]), Dst: 06:39:a5:[redacted] (06:39:[redacted])
  > Destination: 06:39:a5:[redacted] (06:[redacted])
  > Source: D-LinkIn_e9:91:de (c0:a0:bb:e9:[redacted])
    Type: IPv4 (0x0800)
```

- Data in network layer

```
Internet Protocol Version 4, Src: 157.[redacted], Dst: 192.168.[redacted]
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 80
    Identification: 0x6214 (25108)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 88
    Protocol: TCP (6)
    Header checksum: 0x5f88 [validation disabled]
    [Header checksum status: Unverified]
    Source: 157.2[redacted]
    Destination: 192.168.[redacted]
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

# Data in Layers

- Data in transmission layer:

```
Transmission Control Protocol, Src Port: 443, Dst Port: 53226, Seq: 1815, Ack: 5217, Len: 40
   Source Port: 443
   Destination Port: 53226
   [Stream index: 20]
   [TCP Segment Len: 40]
   Sequence number: 1815    (relative sequence number)
   [Next sequence number: 1855    (relative sequence number)]
   Acknowledgment number: 5217    (relative ack number)
   Header Length: 20 bytes
 > Flags: 0x018 (PSH, ACK)
   Window size value: 369
   [Calculated window size: 94464]
   [Window size scaling factor: 256]
   Checksum: 0xe2c0 [unverified]
   [Checksum Status: Unverified]
   Urgent pointer: 0
 > [SEQ/ACK analysis]
```

- Data in application layer (encrypted):

```
Secure Sockets Layer
 v TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 35
      Encrypted Application Data: 40264ebace1718dcd3a9513764ed6d2664d01ce2118a54d3...
```

# Wifi Packet Example

```
 24 1.567097                    Apple_98:f0:6f…  802.…   39 Acknowledgement, Flags=........C
```

```
> Frame 24: 39 bytes on wire (312 bits), 39 bytes captured (312 bits) on interface unknown, id 0
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Acknowledgement, Flags: ........C
```

```
v Frame 24: 39 bytes on wire (312 bits), 39 bytes captured (312 bits) on interface unknown, id 0
  > Interface id: 0 (unknown)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jul 10, 2012 00:12:59.887086000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1341893579.887086000 seconds
    [Time delta from previous captured frame: 0.000005000 seconds]
    [Time delta from previous displayed frame: 0.000005000 seconds]
    [Time since reference or first frame: 1.567097000 seconds]
    Frame Number: 24
    Frame Length: 39 bytes (312 bits)
    Capture Length: 39 bytes (312 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
```

# Wifi Packet Example

```
Radiotap Header v0, Length 25
    Header revision: 0
    Header pad: 0
    Header length: 25
  > Present flags
    MAC timestamp: 2443214761
  > Flags: 0x12
    Data Rate: 24.0 Mb/s
    Channel frequency: 2462 [BG 11]
  > Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
    Antenna signal: -55 dBm
    Antenna noise: -91 dBm
    Antenna: 0
```

```
802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Proprietary mode: None (0)
    Data rate: 24.0 Mb/s
    Channel: 11
    Frequency: 2462MHz
    Signal strength (dBm): -55 dBm
    Noise level (dBm): -91 dBm
    Signal/noise ratio (dB): 36 dB
    TSF timestamp: 2443214761
  > [Duration: 28µs]
```

```
IEEE 802.11 Acknowledgement, Flags: ........C
    Type/Subtype: Acknowledgement (0x001d)
  > Frame Control Field: 0xd400
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Apple_98:f0:6f (00:17:f2:98:f0:6f)
    Frame check sequence: 0x716ea6c7 [unverified]
    [FCS Status: Unverified]
```

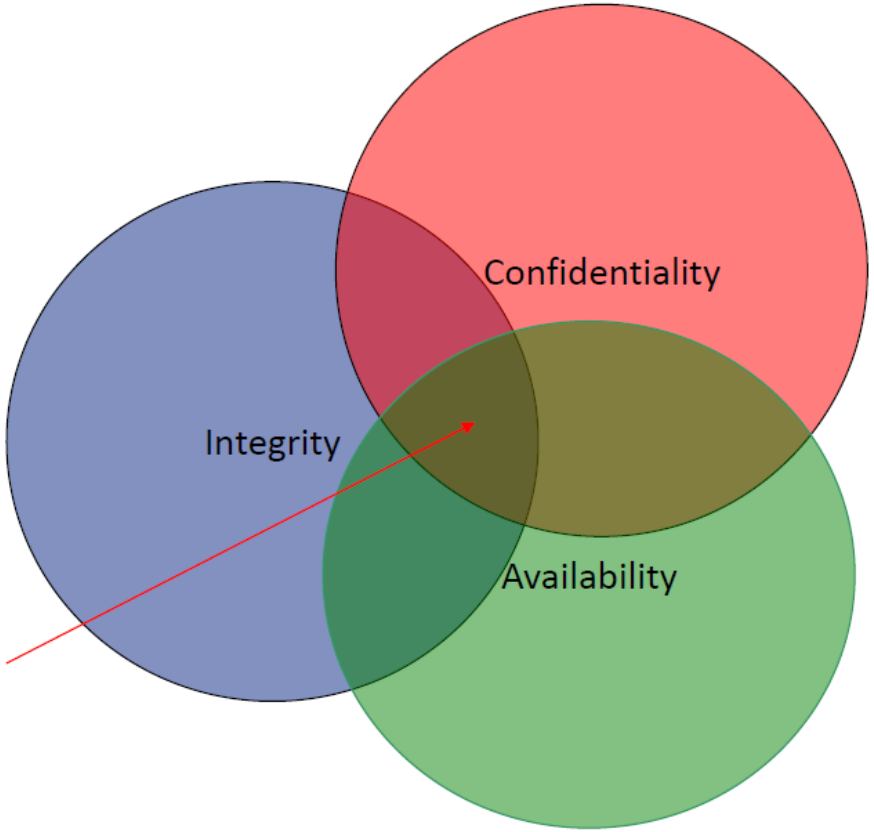
# Background: Cybersecurity Basics


FLORIDA TECH

# 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

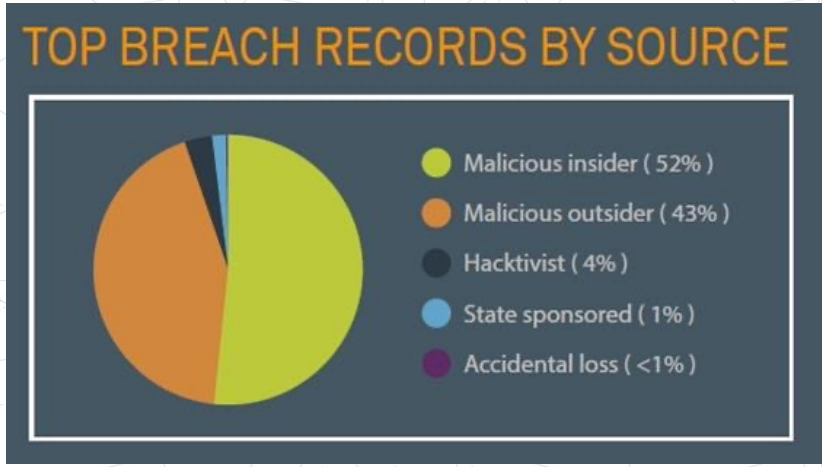
- Ensuring timely and reliable access to and use of information
- Actions by an attacker do not prevent users from having access to use of the system
  - Enable access to data and resources
  - Timely response
  - Fair resource allocation

# 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")

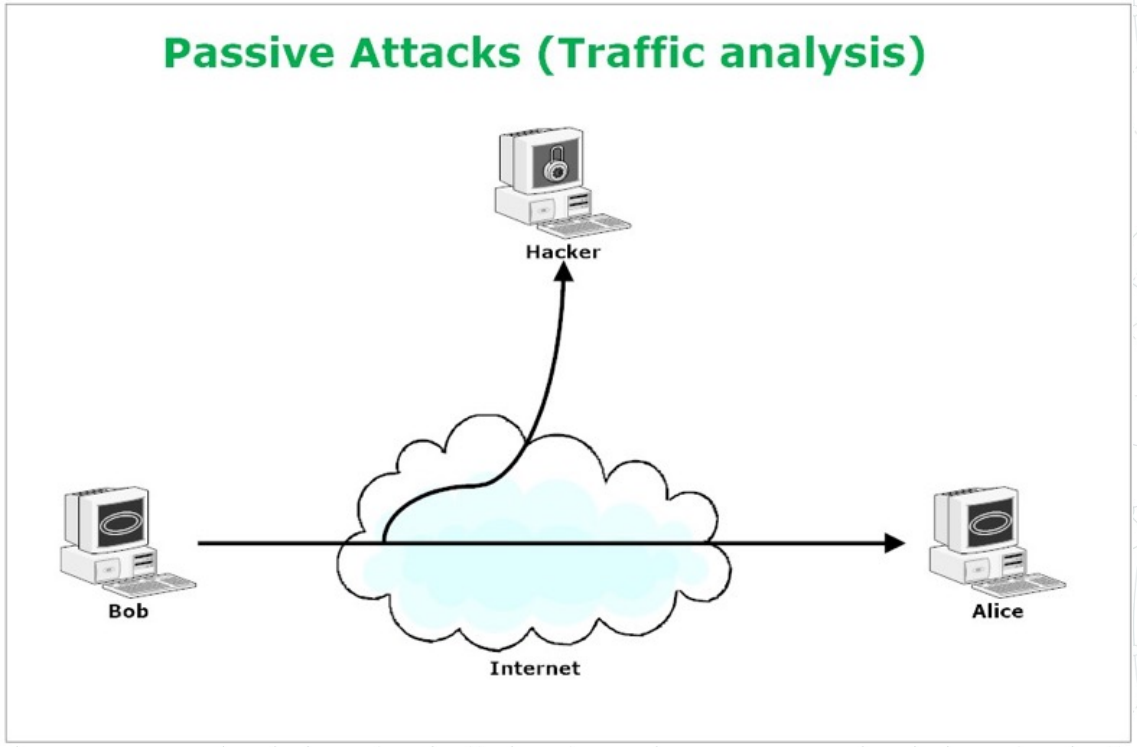


# Type of Cyberattacks: Attacker's Behavior

- 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

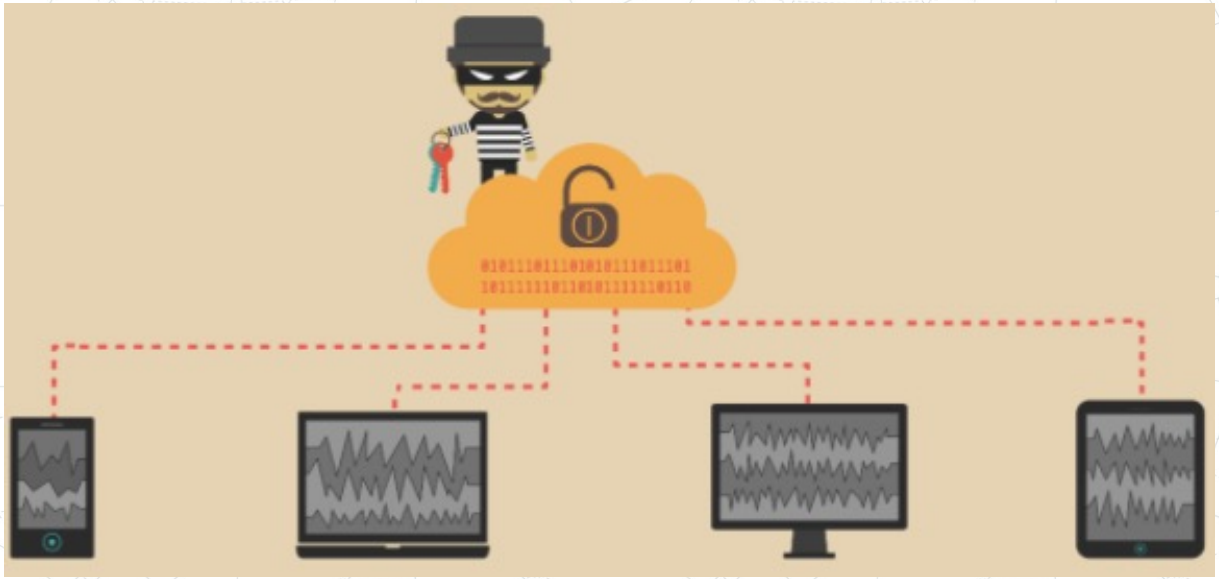


# Active Attacks

- 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

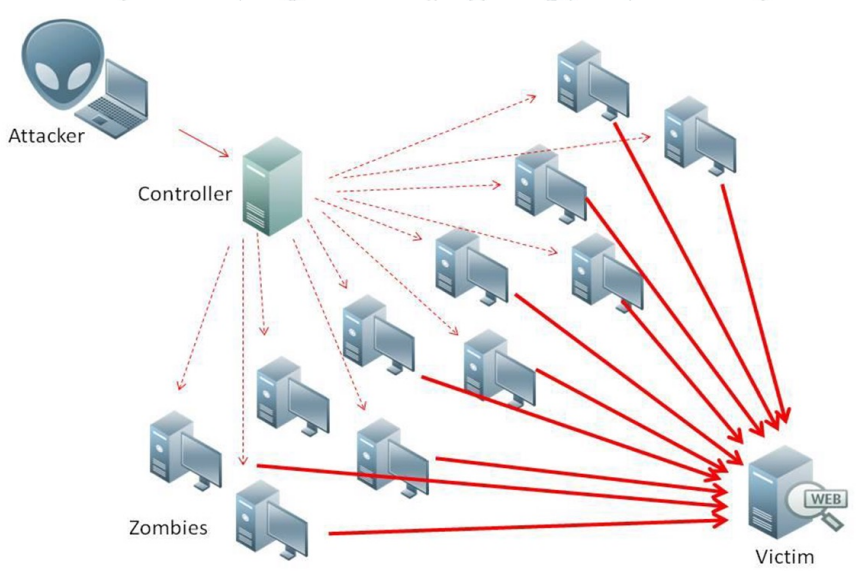
# Some Common Attack Types

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- Malware attack



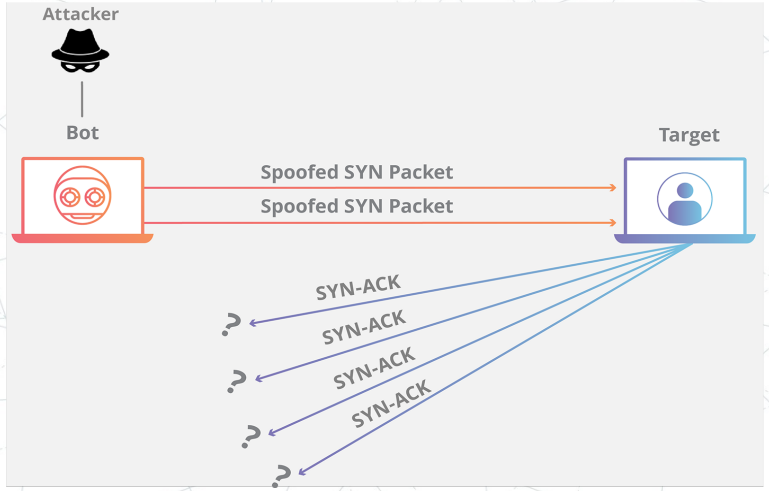
# DoS and DDoS

- 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.



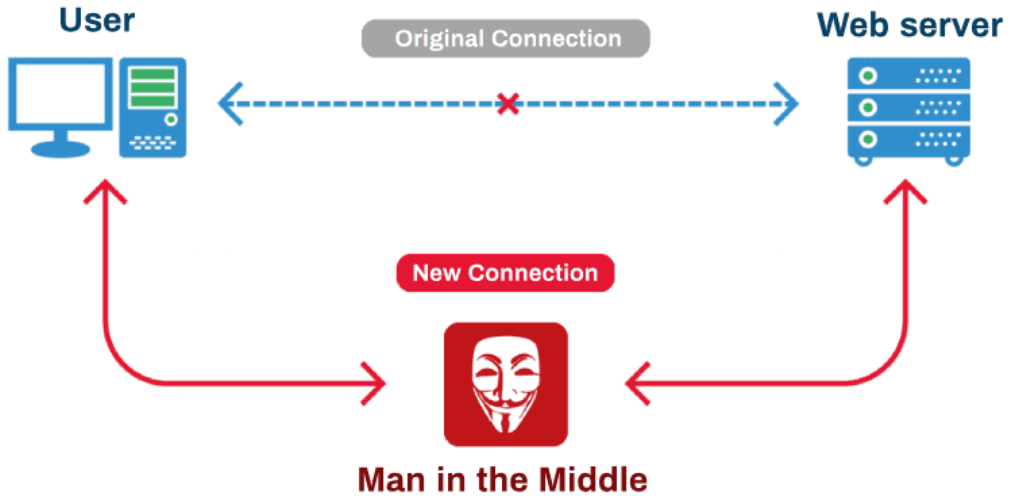
# TCP SYN flood attack

- 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
  - Causes the target system to time out while waiting for the response from the attacker's device
  - Makes the system crash or become unusable when the connection queue fills up

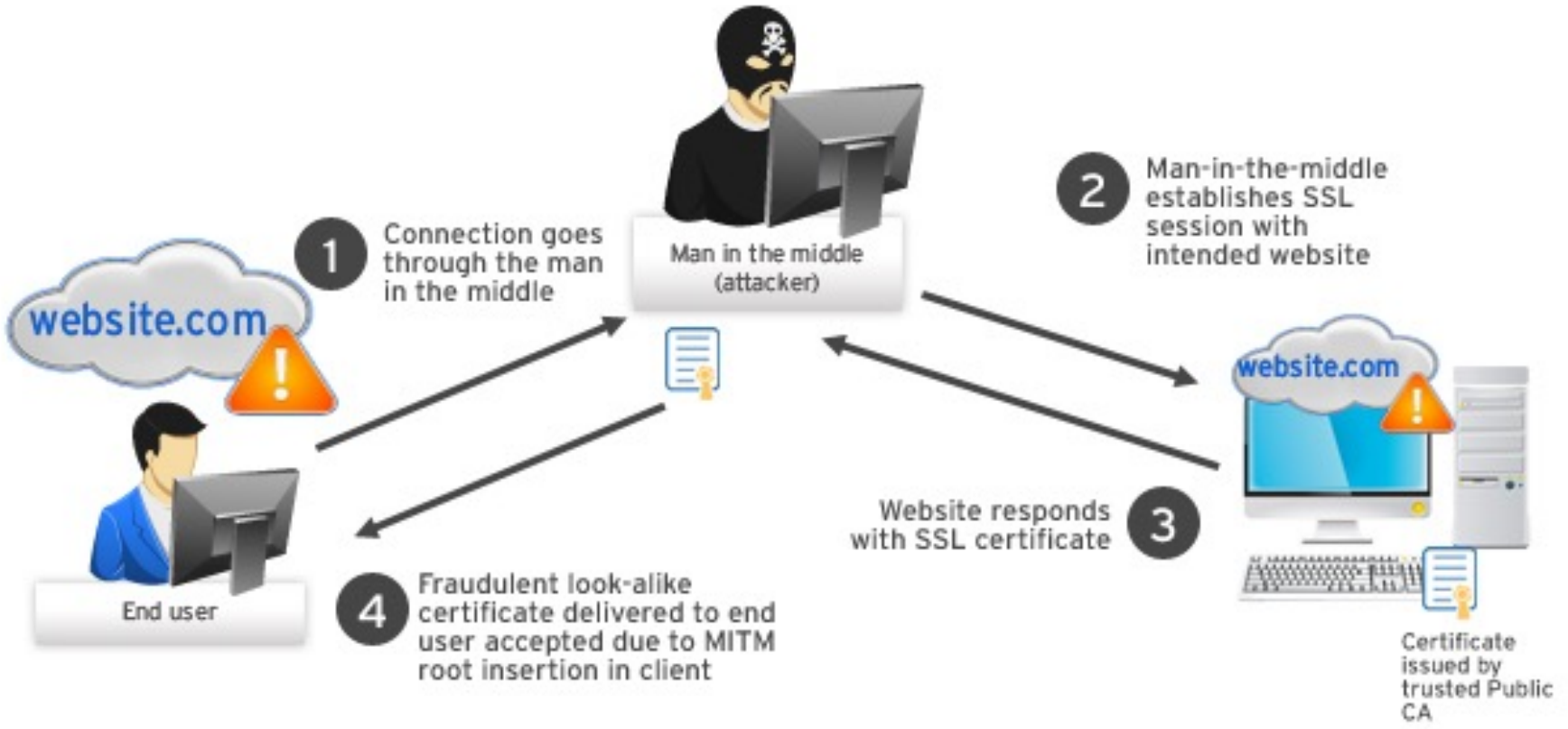


# Man-in-the-middle (MitM) attack

- 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



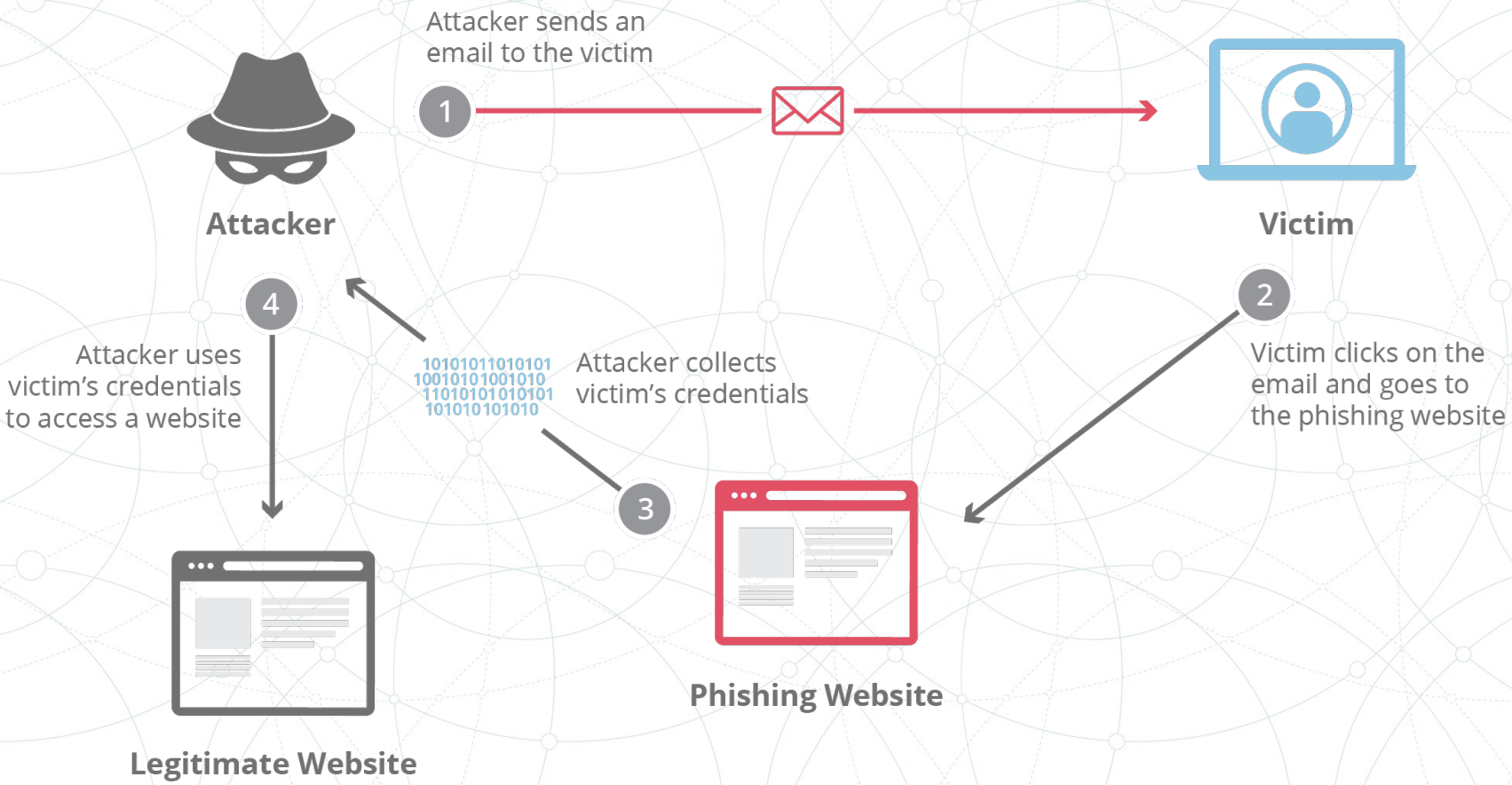
# MitM: How it works



# Phishing 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

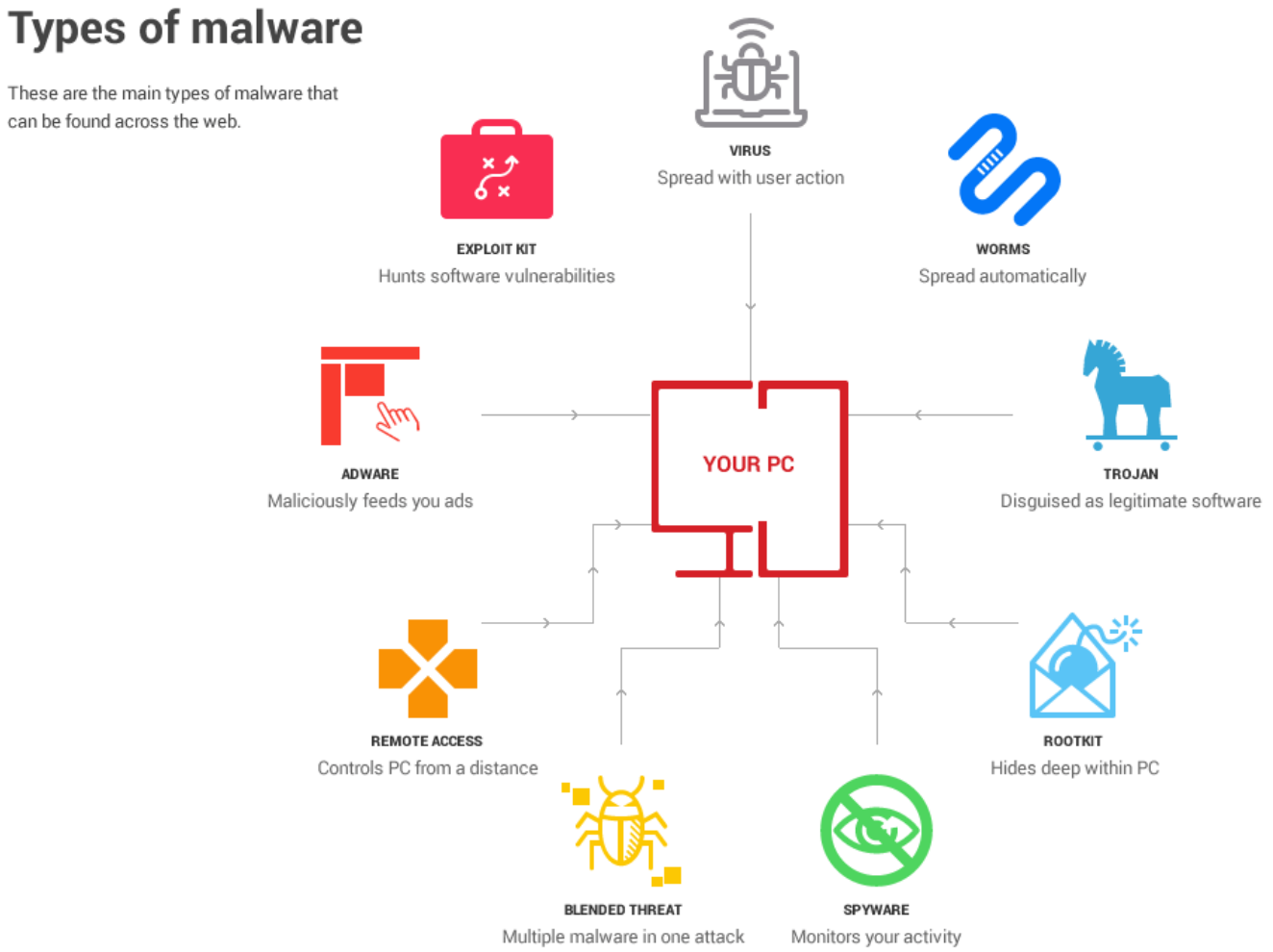


# Malware attack

- 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 the most used against Wifi/Mobile?
  - DDoS
  - Phishing
  - MiTM
  - Malware

FLORIDA TECH

FLORIDA'S STEM UNIVERSITY™

# Thank you. Questions?

Dr. Abdullah Aydeger