October 1, 2024

"Can You Hear Me Now?"

Foundations of Cybersecurity - CYBS 3213

Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute

Tulsa
SCHUSTERMAN CENTER

Checking In

- Last week we looked at the question, “Do You Trust Me?” (Secure Network Design, Network Trust, Least Privileges, Firewalls)
- And since our last meeting, you have taken the second quiz.
- What were the muddiest points of the lecture on trust? We will review the quiz Thursday, but what are your thoughts o the quiz?

https://youtu.be/cCHKGUUxpbE?si=sWSsHIXJsB_Hr-U4

https://youtu.be/7EizBXeN0Is?si=fv9yU8Rg4-xDbq2P

Wireless Communications

- Transmission of voice and data without cable or wires. Instead, it uses electromagnetic signals.

- **Wi-Fi** (often used in WLANs): Provides high-speed internet access with limited range.
- **Bluetooth**: designed for short-range communication.
- **Cellular Networks** (2G, 3G, 4G, 5G): Used by mobile devices to connect to internet.

Wireless Communications

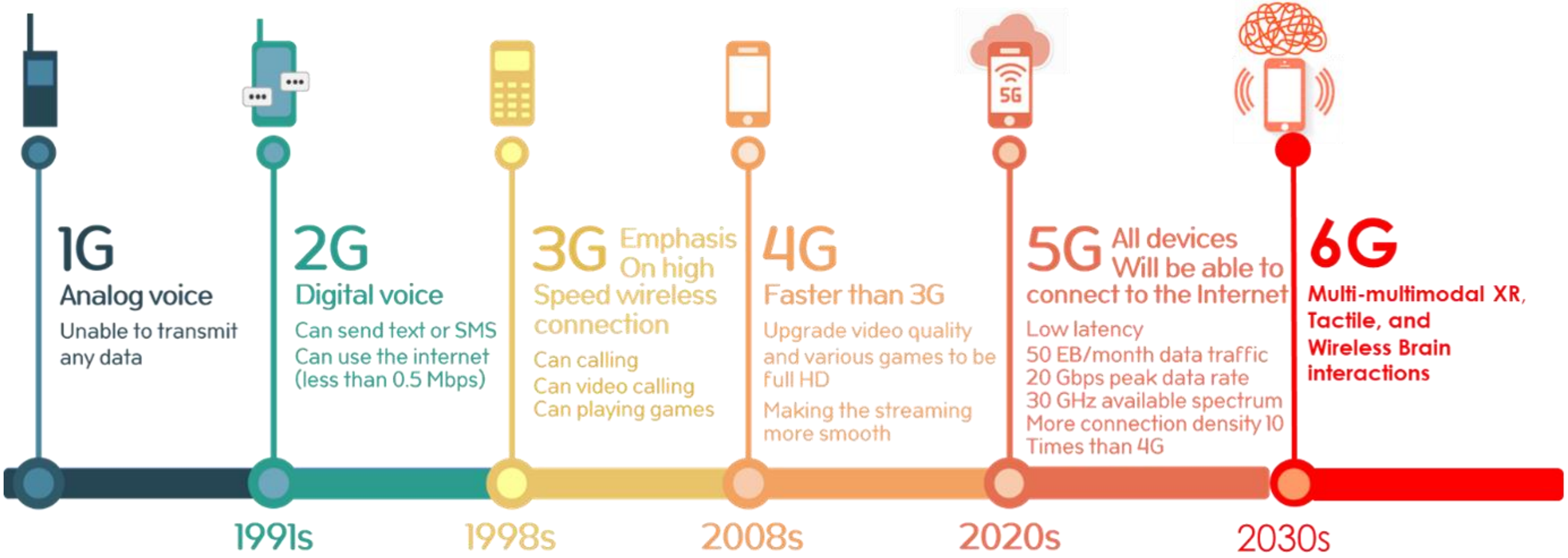
- A wireless network uses devise that send and receive data over radio frequences (RF).

- **Frequency:** Measured in hertz (Hz), it is the number of cycles per second. The higher the frequency, the faster the data (5 GHz).
- **Wavelength:** Measured in meters, it is the distance over which the wave repeats (2.4GHz vs 5 GHz). But higher means shorter distance.

Wi-Fi Connectivity

- Institute of Electrical and Electronics Engineers (IEEE)
  - 802.11n (Wi-Fi 4) – 2009
  - 802.11ac (Wi-Fi 5) – 2013
  - 802.11ax (Wi-Fi 6) - 2019

- Wi-Fi Alliance
  - Wi-Fi is Wi-Fi Alliance's certification indicating a WLAN product meets an IEEE technical standard.



1G
Analog voice
Unable to transmit any data

2G
Digital voice
Can send text or SMS
Can use the internet (less than 0.5 Mbps)

3G Emphasis On high Speed wireless connection
Can calling
Can video calling
Can playing games

4G
Faster than 3G
Upgrade video quality and various games to be full HD
Making the streaming more smooth

5G All devices Will be able to connect to the Internet
Low latency
50 EB/month data traffic
20 Gbps peak data rate
30 GHz available spectrum
More connection density 10 Times than 4G

6G
Multi-multimodal XR, Tactile, and Wireless Brain interactions

1991s
1998s
2008s
2020s
2030s

Wireless Communication

https://www.interdigital.com/post/sensing-an-evolution-how-interdigitals-work-in-multimodal-communications-brings-us-closer-to-haptic-and-emotional-wireless-internet

Difference Between Wi-Fi and Cellular Networks?

Wi-Fi

- Wi-Fi Generations (like 802.11ac or Wi-Fi 6) are used for local networks, providing internet connectivity in smaller areas with higher speeds and typically lower cost. Devices connect to the internet by communicating with a router, which is usually connected to a broadband or fiber internet service.

Cellular

- Cellular Network Generations (like 4G, 5G) provide wide-area coverage for mobile devices, offering more mobility but often at higher costs and potentially slower speeds than the latest Wi-Fi standards.
- GSM – Global System for Mobile
- CDMA – Code Division Multiple Access (3G)
- LTE – Long-term Evolution (4G)
- Fifth Gen – 5G

WLAN Security Standards

- Subset of network security that involves designing, implementing, and ensuring security.
- Strategies are designed to preserve the <u>confidentiality, integrity, and availability</u> of wireless networks and their resources.

- WEP, WPA, WPA2, and the latest WPA3 are the four types of wireless network security protocols.
- <u>Wired Equivalent Privacy (WEP) </u>– 1997; very vulnerable security.
- <u>Wi-Fi Protected Access (WPA)</u> – 2003; uses Temporal Key Integrity Protocol (TKIP) encryption (insecure).
  - WPA – Personal (for home) – what's the password?
  - WPA – Enterprise (uses RADIUS) – individual pwds.
- <u>WPA2</u> – 2004; most popular; uses Advanced Encryption Standard (AES) encryption (highly secure).
- <u>WPA3</u> – 2018; greater protection against brute force.
  - Personal; Enterprise; Enhanced Open
  - Compatibility issues with older equipment

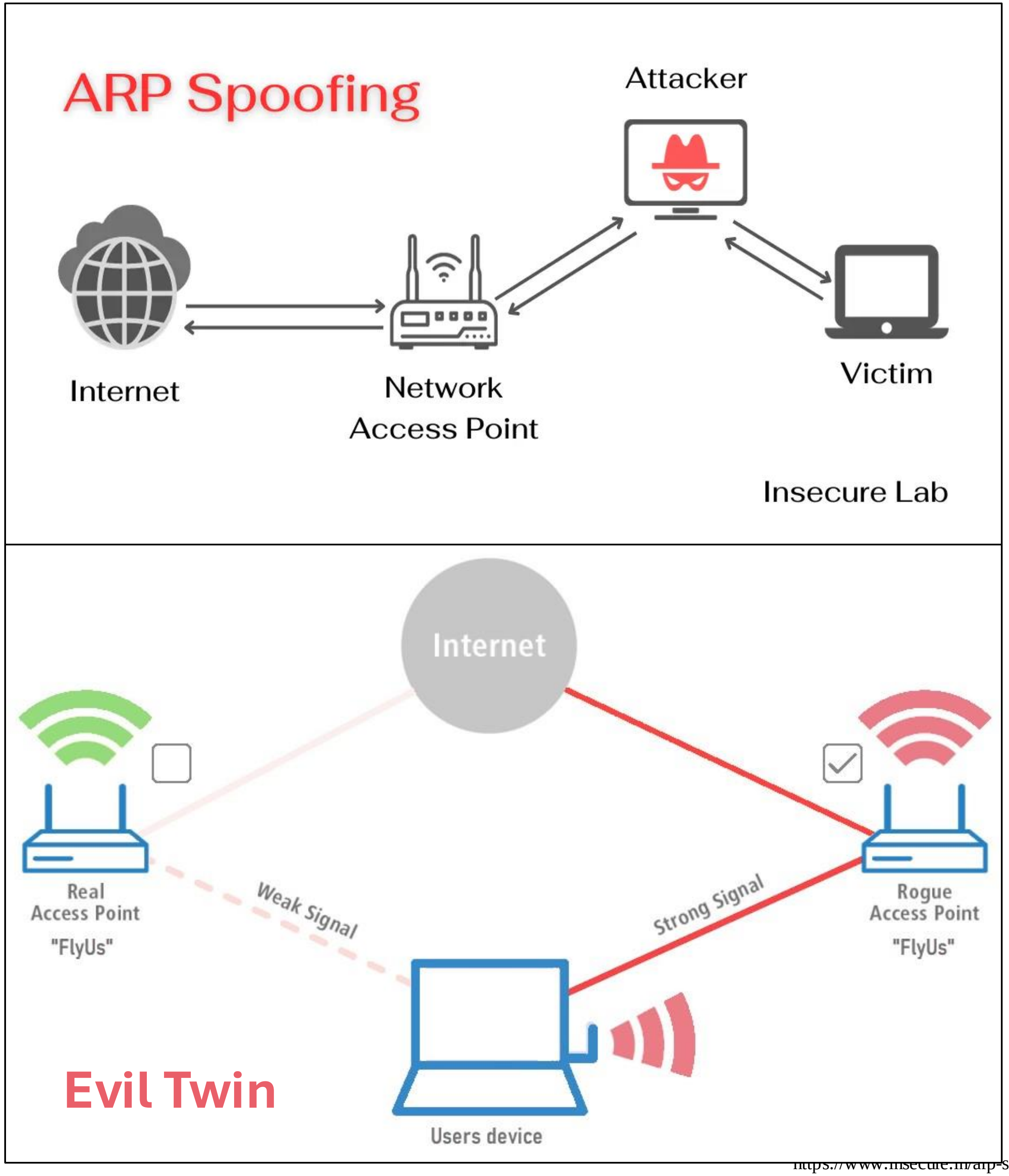
https://youtu.be/l71GBlds0Rs?si=v0Slo1UWIktKcxJa

WLAN Authentication

- Pre-shared key (PSK) is a shared password used for device authentication. Provides authentication.
- Extensible Authentication Protocol (EAP) is an authentication framework that allows various methods (like passwords, digital certificates, or tokens) to be used.
- IEEE 802.1X is an IEEE standard for port-based access control.
- Remote Authentication Dial-In User Service (RADIUS) is a networking protocol for centralized authentication, authorization, and accounting (AAA) services.
- Terminal Access Controller Access-Control System Plus (TACACS+) is a proprietary networking protocol developed by Cisco for centralized authentication, authorization, accounting, and auditing (AAAA) services

Attack!

- Passive attacks - attacker is within range of a wireless network to eavesdrop; most common is packet sniffing (DNS spoofing; malware)
- Active attacks – rogue access points (“Free Wi-Fi”) (MitM; Evil Twin; ARP spoofing).



https://www.insecure.in/arp-spoofing

https://youtu.be/1OVTmrXGHyU?si=iUwycEzTbSH5LhiO

Wireless Technologies: Bluetooth, RFID, NFC

Bluetooth:

1. Use Case: Short-range communication (up to 30 feet)
2. Security Risks:
   a. Bluejacking: Sending unsolicited messages to nearby Bluetooth devices.
   b. Bluesnarfing: Gaining unauthorized access to data on a Bluetooth-enabled device.

RFID (Radio Frequency Identification):

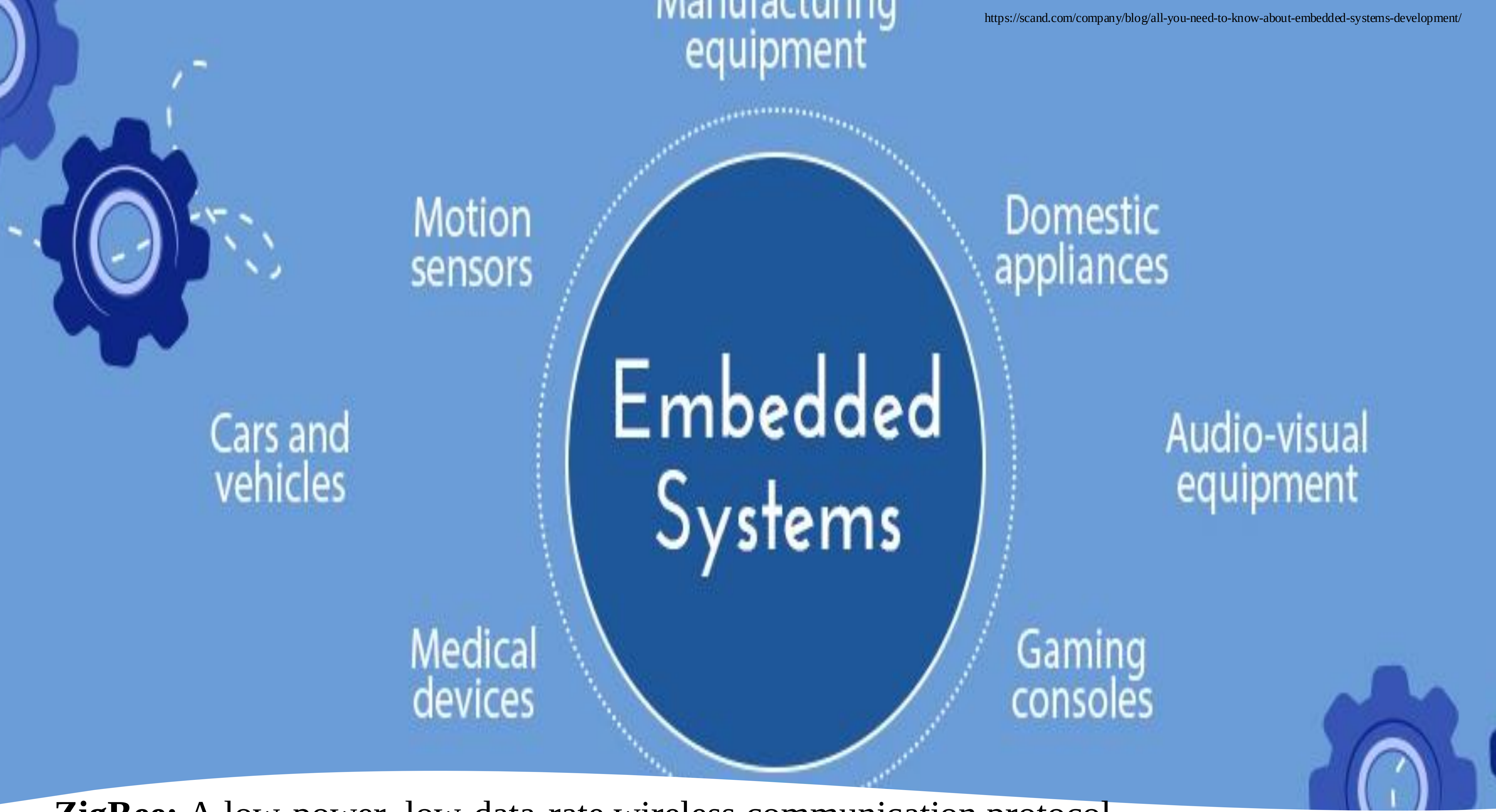
1. Use Case: Uses electromagnetic fields to automatically identify and track tags attached to objects. Used in access control (e.g., keycards), inventory management, and pet identification.
2. Security Consideration: Without encryption, RFID tags can be cloned or spoofed.

NFC (Near-Field Communication):

1. Use Case: Used for contactless payments (e.g., Apple Pay, Google Pay) and data exchanges

What Are Embedded Systems?

- The connection between embedded systems and wireless communication lies in the integration of wireless technologies into devices to enable connectivity, data exchange, and control over a network without the need for physical connections.
- An embedded system is a specialized computer system within a larger device, consisting of a processor, memory, and input/output components. It is designed to perform a specific task with dedicated hardware and software.



https://scand.com/company/blog/all-you-need-to-know-about-embedded-systems-development/

ZigBee: A low-power, low-data-rate wireless communication protocol.

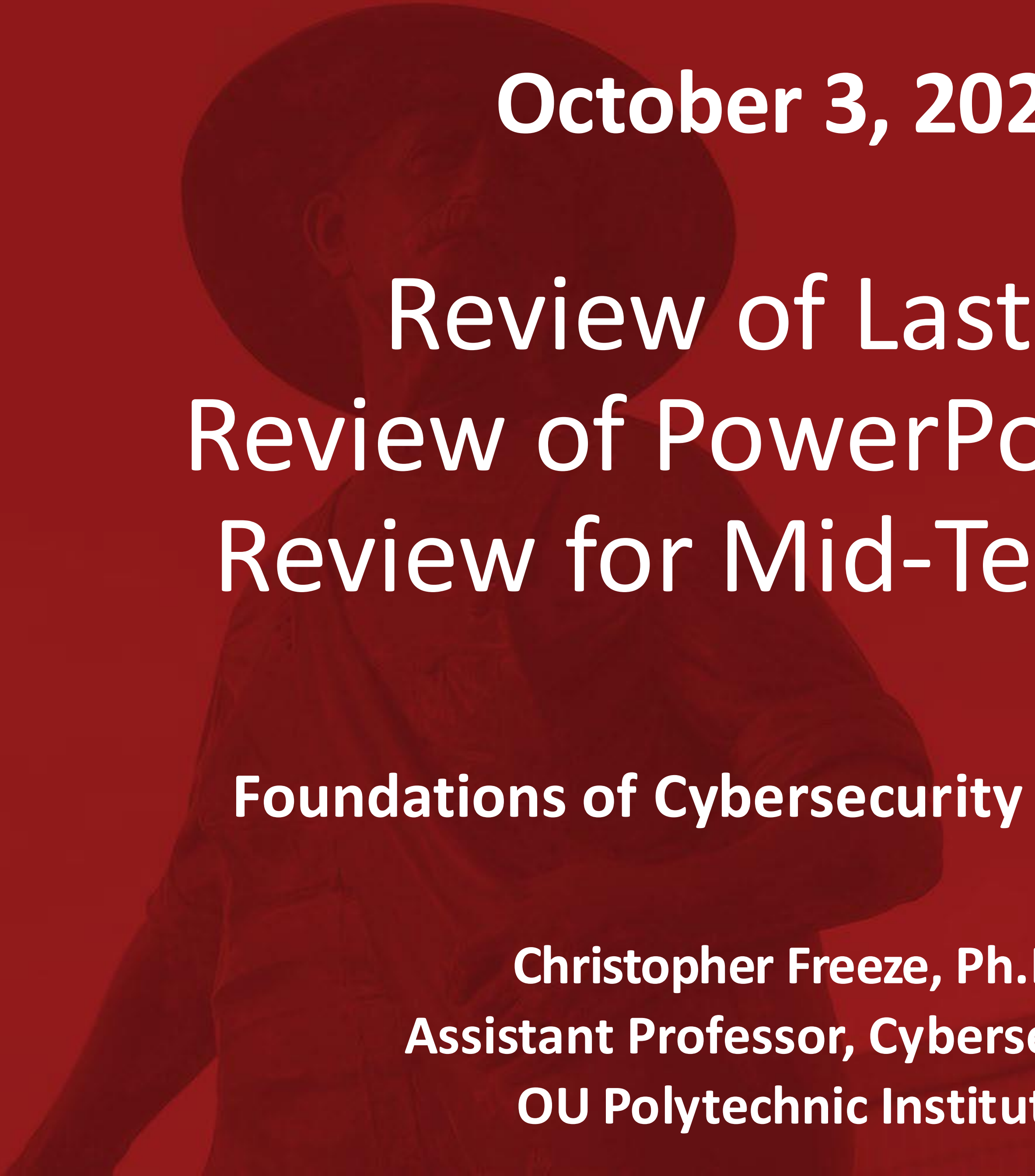
SCADA and ICS

Supervisory Control and Data Acquisition

- Controls operation of electric, water, and similar industrial control systems (ICS).
- Growing reliance on wireless technologies to control, monitor, and manage industrial processes

https://youtu.be/sphvkkybTt0?si=05c9TFYsjLcLiySg

October 3, 2024



Review of Last Quiz
Review of PowerPoint Slides
Review for Mid-Term Exam

Foundations of Cybersecurity - CYBS 3213

Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute

OU Tulsa
SCHUSTERMAN CENTER