CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Wireless, IoT, and Cloud Security

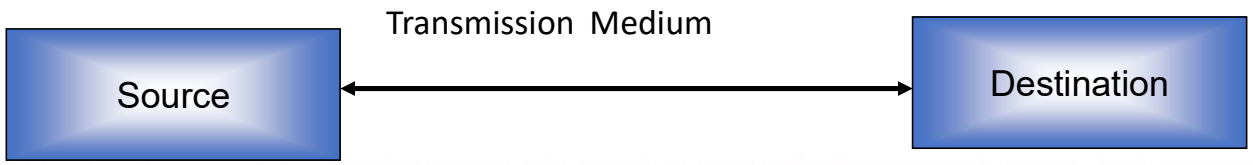
Introduction to Wireless Networks

Video summary

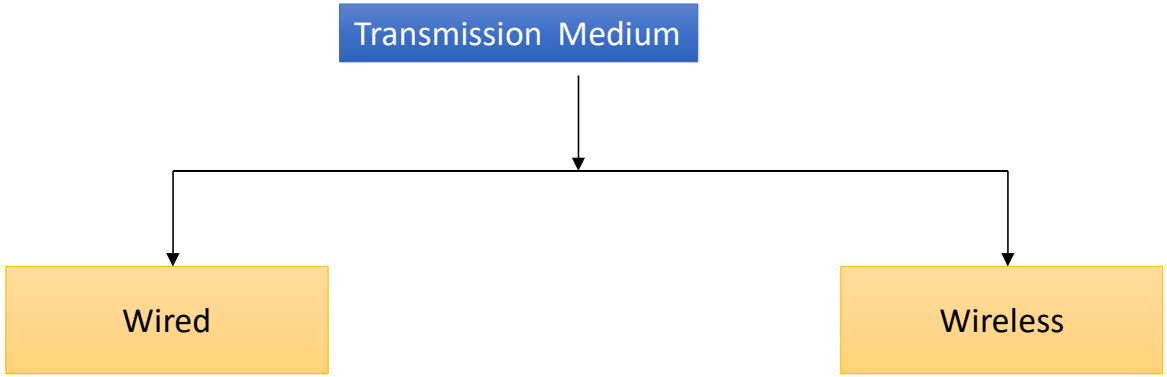
- Basic Communications System Elements
- Wired vs. Wireless
- Wireless Security
- Wireless Network Threats
- Securing Wireless Networks

Basic Communications System Elements

- Source
- Destination
- Transmission Medium



Transmission Medium



Wired vs. Wireless

- Losses
- Mobility
- Security
- Bandwidth
- Cost

Wireless Security

- Key factors contributing to higher security risk of wireless networks compared to wired networks include:
  - **Channel**
    - Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks
    - Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols

Wireless Security

- Key factors contributing to higher security risk of wireless networks compared to wired networks include:
  - **Mobility**
    - Wireless devices are far more portable and mobile, thus resulting in a number of risks

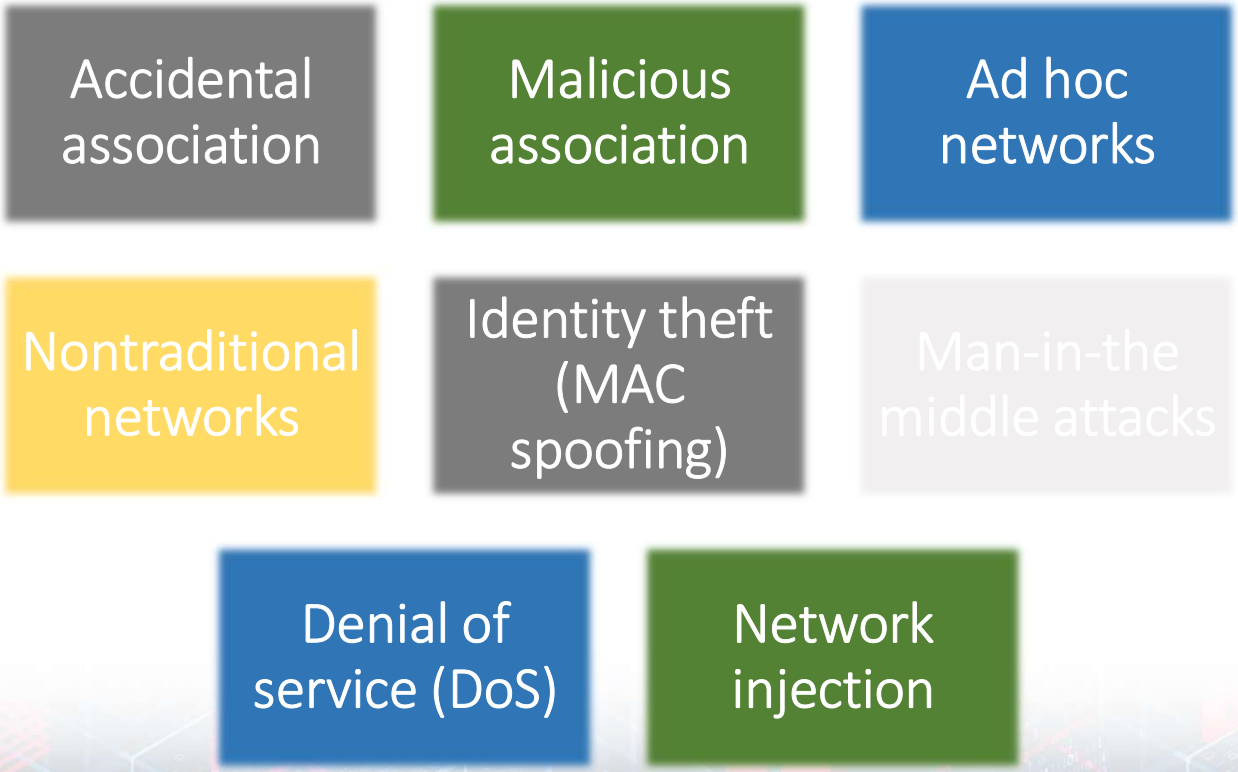
Wireless Security

- Key factors contributing to higher security risk of wireless networks compared to wired networks include:
  - **Resources**
    - Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware
    - Limited energy

Wireless Security

- Key factors contributing to higher security risk of wireless networks compared to wired networks include:
  - **Accessibility**
    - Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations, thus greatly increasing their vulnerability to physical attacks

Wireless Network Threats



Wireless Network Threats

Accidental association

A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network. Although the security breach is accidental, it nevertheless exposes resources of one LAN to the accidental user.

Wireless Network Threats

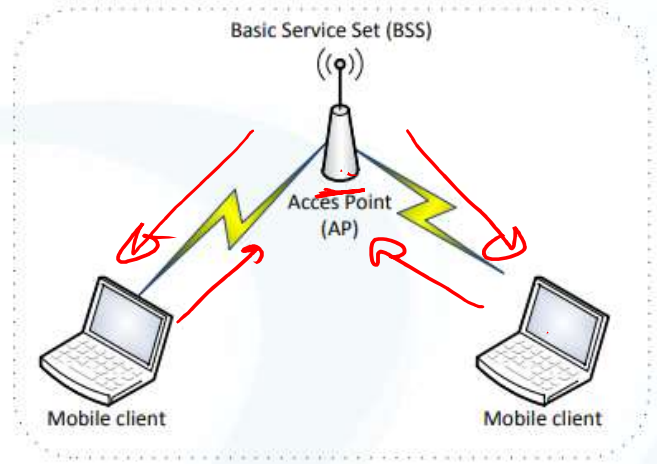
Malicious association

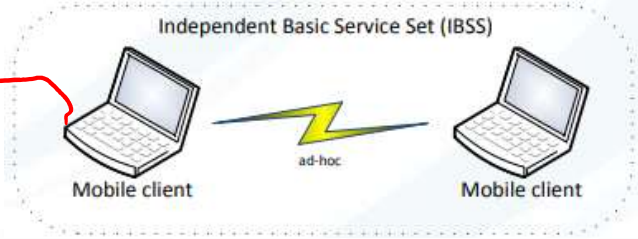
In this situation, a wireless device (Access Point) is configured to appear to be a legitimate access point, enabling the operator of this AP to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point.

Wireless Network Threats

Ad hoc networks

These are peer-to-peer networks between wireless computers with no access point between them. Such networks can pose a security threat due to a lack of a central point of control.





Ad hoc.

Wireless Network Threats

Non-traditional networks

Non-traditional networks and links, such as personal network Bluetooth devices, barcode readers, and handheld devices pose a security risk both in terms of eavesdropping and spoofing.

Wireless Network Threats

Identity theft (MAC spoofing)

This occurs when an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges.

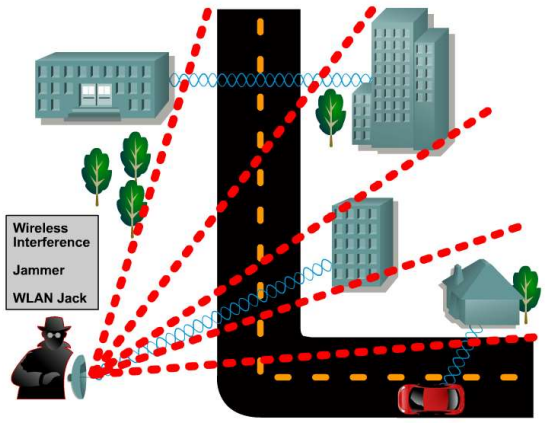
Wireless Network Threats

Man-in-the middle attacks

This attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device. Wireless networks are particularly vulnerable to such attacks.

Wireless Network Threats

Denial of service (DoS)



In the context of a wireless network, a DoS attack occurs when an attacker continually bombards a wireless access point or some other accessible wireless port with various protocol messages designed to consume system resources. The wireless environment lends itself to this type of attack, because it is so easy for the attacker to direct multiple wireless messages at the target.

2.4 GHZ

2.1 GHZ

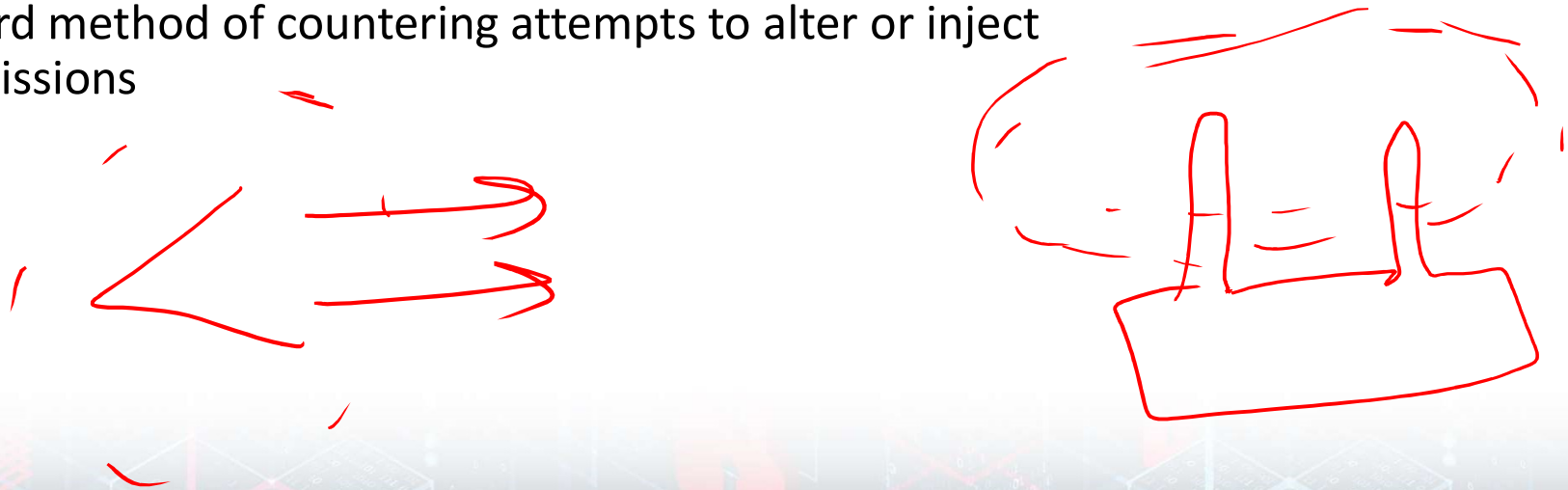
Wireless Network Threats

Network injection

A network injection attack targets wireless access points that are exposed to non-filtered network traffic, such as routing protocol messages or network management messages. An example of such an attack is one in which bogus reconfiguration commands are used to affect routers and switches to degrade network performance.

Securing Wireless Transmissions

- Countermeasures for eavesdropping:
  - Signal-hiding techniques
  - Encryption
- The use of encryption and authentication protocols is the standard method of countering attempts to alter or inject transmissions



Video summary

- Basic Communications System Elements
- Wired vs. Wireless
- Wireless Security
- Wireless Network Threats
- Securing Wireless Networks