Wireless and Short-Range Threats

Dr Ayman El Hajjar

CyBOK Mapping

The lecture maps to the following CyBOK Knowledge Areas:

Full Coverage:

- **Infrastructure Security → Network Security**
- **Infrastructure Security → Physical Layer and Telecommunications Security**

Partly Covered:

- **Infrastructure Security → Cyber-Physical Systems Security**
- **Systems Security → Authentication, Authorisation & Accountability**
- **Infrastructure Security → Applied Cryptography**

Outline

- Wireless Security Foundations
- WiFi Security Threats
- Bluetooth Security Threats
- Low-Power and Proximity Protocols
- Wireless Disruption Attacks

Wireless Security Foundations

Why Wireless is Vulnerable

Wireless communication extends the **attack surface** beyond **physical network boundaries**.

- **Broadcast Medium:** Signals can be received by nearby devices, not only the intended receiver
- **Physical Layer Exposure:** Attackers may observe, interfere with, or disrupt radio communication
- **Shared Spectrum:** Multiple systems often operate in the same frequency bands
- **Dynamic Connectivity:** Devices move, disconnect, reconnect, and interact with changing networks

Safety-relevant use: wireless links may carry **sensor data**, **commands**, **alerts**, or **monitoring information**.

How We Analyse Wireless Attacks

Attack Analysis

Each attack can be understood through its target, mechanism, security impact and safety relevance.

- **Target:** What part of the wireless system is attacked?
- **Mechanism:** How does the attacker exploit the weakness?
- **Security Impact:** Which property is affected: confidentiality, integrity, availability, or authentication?
- **Safety Relevance:** What happens if the affected link carries commands, alerts, readings, or status?

Attack detail matters because safety impact depends on what the wireless link controls or reports.

WiFi Security Threats

WiFi Security Evolution

WiFi security has evolved to improve **authentication**, **encryption**, and resistance to **common wireless attacks**.

- **WEP**
  - Early protection mechanism based on RC4
  - Weak key management and repeated IVs made it insecure
- **WPA**
  - Transitional improvement introduced before WPA2
  - Used TKIP to address some weaknesses in WEP
- **WPA2**
  - Uses stronger AES-based protection through CCMP
  - Still affected by weak passwords and protocol-level issues
- **WPA3**
  - Introduces SAE to improve protection against offline password guessing
  - Provides stronger protection for modern wireless networks

Common WiFi Security Threats

WiFi threats exploit **exposed radio communication**, **weak authentication**, **management traffic**, and trust in **nearby access points**.

- **Eavesdropping:** Capturing wireless traffic transmitted over the air
- **Weak Password Attacks:** Capturing authentication material and testing passphrases offline
- **Management Frame Attacks:** Forging deauthentication or disassociation frames to disrupt connections
- **Rogue Access Points:** Creating fake or unauthorised access points to attract users or devices
- **Protocol Flaws:** Exploiting weaknesses in WiFi security protocols or implementations

Legacy and Common WiFi Weaknesses

Older WiFi mechanisms remain useful for understanding how **weak design choices** lead to **practical attacks**.

- **WEP Key Recovery:** Weak IV handling and RC4 usage allow practical recovery of the network key
- **Replay Attacks:** Captured frames can be reused to generate traffic or trigger repeated actions
- **Packet Injection:** Attackers can inject crafted frames when protocol protections are weak
- **Weak Compatibility Mechanisms:** Compatibility allows transition but may retain security weaknesses

WiFi Attack: Deauthentication

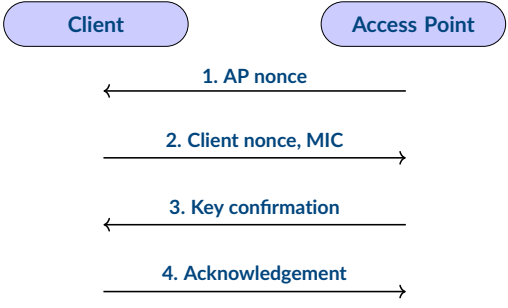
Deauthentication frames are management frames used to terminate a **WiFi client connection**.

- **Attack Mechanism:** Attacker forges deauthentication frames to disconnect a client
- **Main Effect:** The client is forced to disconnect and attempt to reconnect
- **Use in Attacks:** Supports denial of service or handshake capture during reconnection
- **Weakness:** Legacy management frames were not always protected against spoofing

In safety-relevant systems, use **Protected Management Frames** where supported and monitor repeated **deauthentication patterns**.

WPA2 Attack: Handshake Capture

In **WPA2-Personal**, the **4-way handshake** derives session keys from the shared **passphrase** and exchanged **nonces**.



- **Attack:** Capture the handshake during connection or reconnection
- **Offline Guessing:** Test candidate passphrases against the captured MIC
- **Weakness:** Short or predictable passwords can be cracked offline

In safety-relevant systems, use **strong passphrases** or **enterprise authentication** to protect wireless access.

WiFi Attack: Evil Twin Access Point

An **evil twin** is a **rogue access point** that imitates a **legitimate WiFi network** to attract users or devices.

- **Attack Setup:** Attacker creates a fake access point with a familiar SSID
- **User Connection:** Devices may connect automatically or users may select the fake network
- **Traffic Exposure:** Attacker may observe, redirect, or manipulate network traffic
- **Security Risk:** Users may disclose credentials or interact with malicious services

In safety-relevant systems, secure wireless communication depends on **cryptography**, **protocol design**, and **correct implementation**.

WPA2-Enterprise Attack: Rogue Access Point

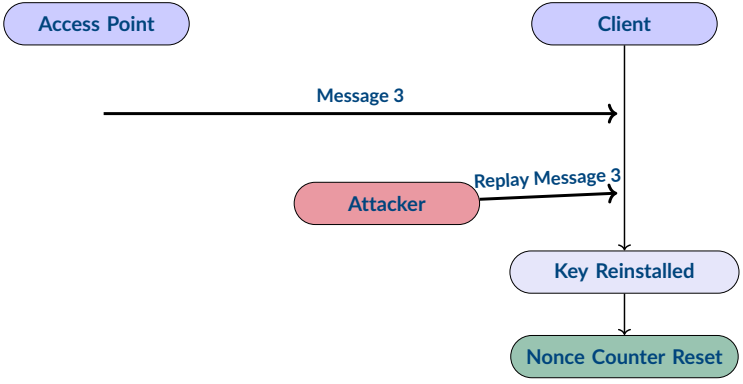
WPA2-Enterprise uses 802.1X and EAP to authenticate users through an authentication server, rather than relying on a shared WiFi passphrase.

- **Attack Setup:** Attacker creates a rogue access point using the same enterprise SSID
- **User Authentication:** Devices may authenticate if certificate validation is weak or ignored
- **Credential Exposure:** Captured authentication material may support offline password guessing

In safety-relevant systems, validate **server certificates** and use stronger **EAP methods** such as **EAP-TLS**.

WPA2 Attack: KRACK

KRACK exploits vulnerable **WPA2 clients** that **reinstall** an already-used key after a **retransmitted handshake message**.



KRACK: Security Implications

Security Impact

- Does not require guessing the WiFi password
- Exploits protocol state handling
- Can weaken confidentiality and integrity
- Depends on vulnerable client behaviour

What It Shows

- Strong encryption is not enough on its own
- Handshake messages must be handled correctly
- Key reuse and nonce reuse can break security assumptions
- Protocol implementation matters as much as protocol design

In safety-relevant systems, secure wireless communication depends on **cryptography**, **protocol design**, and **correct implementation**.

Bluetooth Security Threats

Bluetooth Security Evolution

Bluetooth security has evolved across versions to improve **pairing**, **authentication**, **encryption**, and **privacy protection**.

- **Early Bluetooth:** PIN-based pairing and weaker authentication assumptions
- **Secure Simple Pairing:** Improved pairing for Bluetooth Classic devices
- **Bluetooth Low Energy:** Low-power design for sensors, wearables, and IoT
- **LE Secure Connections:** Stronger BLE pairing using elliptic-curve key exchange
- **Modern Bluetooth:** Stronger privacy and security, but implementation weaknesses remain

Security depends on **version**, **pairing mode**, **device configuration**, and **implementation quality**.

Bluetooth Architecture

Bluetooth includes different communication modes with different power, performance, and security characteristics.

- **Bluetooth Classic:** Used for audio, peripherals, and continuous connections
- **Bluetooth Low Energy:** Used for sensors, wearables, medical devices, and IoT
- **Security Models:** Pairing, encryption, and privacy differ across Classic/BLE
- **Dual-Mode Devices:** Dual-mode support increases compatibility complexity
- **Attack Feasibility:** Depends on version, device role, pairing mode, and implementation behaviour

Bluetooth attacks often exploit gaps between **supported features**, **configured security**, and **implementation behaviour**.

Common Bluetooth Security Threats

Bluetooth threats exploit **short-range discovery**, **pairing**, **authentication**, and **implementation weaknesses**.

- **Device Discovery:** Exposes nearby devices and services to potential attackers
- **Weak Pairing:** Poor pairing choices can allow impersonation or interception
- **Eavesdropping:** Attackers may capture traffic when encryption or pairing is weak
- **Man-in-the-Middle:** Attackers may position themselves between paired devices
- **Implementation Flaws:** Vulnerabilities in Bluetooth stacks can expose devices remotely
- **Tracking:** BLE advertising can reveal device presence, movement, or behaviour

Bluetooth Pairing

Bluetooth pairing establishes shared keys so devices can authenticate and encrypt later communication.

- **Pairing Goal:** Establish trust between two nearby Bluetooth devices
- **Key Establishment:** Devices negotiate or derive keys used for later communication
- **Authentication Strength:** Depends on the pairing method and user interaction
- **Weak Pairing:** Limited or absent user verification can expose devices to impersonation or MITM
- **Security Impact:** A weak pairing process can undermine later encryption

Pairing is a critical point where Bluetooth security can be weakened before normal communication begins.

Bluetooth Attack: Weak Pairing and MITM

Weak Bluetooth pairing occurs when devices establish trust without strong authentication of the peer device.

- **Attack Target:** Pairing with limited user verification, such as Just Works
- **MITM Position:** Attacker relays pairing messages between two nearby devices
- **Authentication Gap:** Devices may establish keys without confirming the peer
- **Security Impact:** Encrypted communication may be exposed or controlled

Safety-relevant use: paired devices may exchange **readings**, **commands**, **alerts**, or **status data**.

BLE Advertising, Discovery, and Tracking

BLE devices use **advertising packets** to announce their presence before or between connections.

- **Advertising:** Devices broadcast identifiers, services, or connection information
- **Discovery:** Nearby scanners can observe devices without pairing
- **Privacy Exposure:** Names, UUIDs, or stable identifiers can reveal device type or presence
- **Tracking Risk:** Repeated observations can support location or movement tracking
- **Data Exposure:** Poor implementations may expose sensitive values before encryption

In safety-relevant systems, advertising data may expose **device presence**, **roles**, or **operational context**.

Bluetooth Vulnerability: BlueBorne

BlueBorne refers to Bluetooth stack vulnerabilities that can allow nearby attackers to target affected devices **without pairing**.

- **Attack Surface:** Bluetooth stack on nearby Bluetooth-enabled devices
- **Attack Condition:** Attacker must be within Bluetooth radio range
- **Main Weakness:** Implementation flaws in Bluetooth protocol handling
- **Security Impact:** May support device compromise, data exposure, or network pivoting

In safety-relevant systems, affected Bluetooth links may carry **commands**, **readings**, **alerts**, or **device status**.

Bluetooth Vulnerability: KNOB and BIAS

KNOB and **BIAS** show how Bluetooth security can be weakened by flaws in key negotiation and authentication assumptions.

- **KNOB:** Forces weaker encryption key negotiation in vulnerable Bluetooth Classic connections
- **BIAS:** Allows impersonation of a paired device under vulnerable authentication handling
- **Attack Surface:** Bluetooth Classic pairing, key negotiation, and reconnection
- **Security Impact:** May weaken confidentiality, authentication, or device trust

In safety-relevant systems, protocol-level weaknesses may persist even when devices appear paired and encrypted, while affected links may carry **commands**, **readings**, **alerts**, or **status**.

Low-Power and Proximity Protocols

Low-Power and Proximity Protocols

Low-power and proximity protocols support **constrained devices**, **short-range interaction**, and **IoT communication**.

- **Zigbee:** Low-power mesh networking for sensors, automation, and IoT devices
- **Z-Wave:** Smart-home mesh networking using controllers, devices, and inclusion processes
- **Thread:** IPv6-based low-power mesh networking for IoT environments
- **NFC/RFID:** Proximity communication for tags, access systems, and short-range exchange
- **LoRaWAN:** Long-range low-power communication for telemetry and remote sensing

In safety-relevant systems, constrained links may carry **sensor readings**, **commands**, **alarms**, or **status**.

Common Low-Power and Proximity Threats

Low-power and proximity protocols expose threats around **joining**, **identity**, **replay**, **relay**, and **radio disruption**.

- **Weak Joining:** Devices may join using insecure or poorly protected processes
- **Key Exposure:** Shared or default keys can expose multiple devices
- **Replay Attacks:** Captured messages may be reused without freshness checks
- **Relay Attacks:** Proximity assumptions may be bypassed by forwarding messages
- **Device Spoofing:** Attackers may imitate sensors, tags, or controllers
- **Radio Disruption:** Low-power links may be vulnerable to interference

In safety-relevant systems, these links may carry **measurements**, **commands**, **alarms**, or **state changes**.

6LoWPAN Threat Surface

6LoWPAN brings **IP networking** into constrained wireless systems, creating threats around identity, fragmentation, routing and gateway trust.

- **Fragmentation Abuse:** Malformed fragments may disrupt reassembly or exhaust memory
- **Node Spoofing:** Attackers may imitate constrained devices
- **Replay:** Captured packets may be reused without freshness checks
- **Routing Disruption:** Compromised nodes may affect forwarding
- **Border Router Risk:** The gateway becomes a key trust boundary

In safety-relevant systems, affected 6LoWPAN links may delay, alter, or block **measurements**, **commands**, **alerts**, or **state updates**.

Zigbee Attack: Joining and Key Exposure

Zigbee devices may receive network keys during **joining**, making the joining process a critical security point.

- **Attack Target:** Device joining, rejoining, or commissioning
- **Key Exposure:** Network keys may be exposed if joining protection is weak
- **Default Keys:** Shared or predictable keys can weaken multiple devices
- **Device Spoofing:** Attackers may imitate sensors, switches, or controllers
- **Security Impact:** Exposed keys may allow traffic capture, injection, or control

In safety-relevant systems, exposed Zigbee links may affect **sensor readings**, **commands**, **alarms**, or **device state**.

NFC Attack: Relay

NFC relay attacks forward communication between a legitimate reader and token, bypassing the expected **proximity** assumption.

- **Attack Target:** Contactless cards, tags, phones, or access tokens
- **Relay Mechanism:** Messages are forwarded between distant legitimate endpoints
- **Proximity Weakness:** The system assumes the token is physically near the reader
- **Security Impact:** Attackers may trigger unauthorised access or transactions
- **Practical Constraint:** Timing, distance, and protocol checks affect feasibility

In safety-relevant systems, proximity assumptions may protect **access**, **commands**, **identity**, or **authorisation**.

Wireless Disruption Attacks

Wireless Disruption Attacks

Wireless disruption attacks interfere with **radio communication**, reducing the ability of devices to exchange data reliably.

- **Jamming:** Radio interference prevents successful transmission or reception
- **Interference:** Other devices disrupt communication on shared spectrum
- **Congestion:** Excess traffic reduces availability and increases delay
- **Depletion:** Repeated attempts can drain constrained device batteries
- **Denial of Service:** Devices may lose connectivity, delay messages, or miss state

In safety-relevant systems, disrupted wireless links may delay or block **commands**, **alerts**, **measurements**, or **status updates**.

Wireless Attack: Jamming

Jamming disrupts **radio communication** by transmitting interference on the same or nearby frequencies.

- **Attack Target:** Wireless availability at the physical or link layer
- **Attack Method:** Interference prevents receivers from decoding legitimate signals
- **Affected Links:** WiFi, Bluetooth, Zigbee, LoRaWAN, and other radio systems
- **DoS Impact:** Devices may disconnect, delay messages, or fail to report state
- **Attack Scope:** Depends on power, frequency, distance, and environment

In safety-relevant systems, jamming may block **alerts**, **commands**, **measurements**, or **status updates**.

Wireless DoS: Congestion and Depletion

Wireless DoS attacks reduce availability by exhausting **channel capacity**, **device energy**, or **protocol state**.

- **Traffic Flooding:** Excess messages consume bandwidth and processing capacity
- **Connection Abuse:** Repeated connection attempts consume device resources
- **Battery Depletion:** Constrained devices waste energy handling unnecessary traffic
- **Protocol Abuse:** Attackers exploit retries, acknowledgements, or association processes
- **Availability Impact:** Devices may become slow, unreachable, or unstable

In safety-relevant systems, wireless DoS may delay **commands**, **alerts**, **measurements**, or **state updates**.

Summary

- **Wireless Exposure:** Broadcast communication extends the attack surface beyond physical boundaries
- **WiFi Threats:** Attacks may exploit authentication, management frames, rogue access points, or protocol behaviour
- **Bluetooth Threats:** Pairing, discovery, tracking, and stack vulnerabilities affect short-range devices
- **Low-Power Protocols:** Joining, key exposure, relay, replay, and spoofing affect constrained networks
- **Disruption Attacks:** Jamming and DoS can reduce availability across wireless systems

In safety-relevant systems, wireless threats may affect **commands**, **alerts**, **measurements**, or **device state**.

Key References

- NCSC. *Device security principles for manufacturers*. **[Link]**
- NIST. (2012). *Guidelines for Securing Wireless Local Area Networks*. NIST SP 800-153. **[Link]**
- ENISA. (2020). *Guidelines for Securing the Internet of Things*. **[Link]**
- IEEE. *IEEE Std 802.11-2020: Wireless LAN Medium Access Control and Physical Layer Specifications*. **[Link]**
- Bluetooth SIG. *Bluetooth Core Specification 6.3*. **[Link]**
- Connectivity Standards Alliance. *Zigbee Specification*. **[Link]**
- Vanhoef, M., & Piessens, F. (2017). *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*. **[Link]**
- Antonioli, D., et.al. (2019). *The KNOB is Broken*. **[Link]**
- Antonioli, D., et.al. (2020). *BIAS: Bluetooth Impersonation AttackS*. **[Link]**
- Hancke, G. P. (2005). *A Practical Relay Attack on ISO 14443 Proximity Cards*. **[Link]**