CYBER SECURITY AND FORENSICS - I
05201296

Prof. Aniket Paul, Assistant Professor
Faculty of IT & Computer Science

CHAPTER-4

Wireless Networks Security

TOPICS

Overview of wireless technology

Wireless security protocols -Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2

Attacks on wireless networks.

OVERVIEW OF WIRELESS TECHNOLOGY

INTRODUCTION TO WIRELESS NETWORKS

What is a Wireless Network?

A **wireless network** is a type of communication network that allows devices to connect and exchange data **without the need for physical cables**. Instead, it uses **radio waves** or **infrared signals** to transmit data between devices.

Key Advantages of Wireless Networks

- Eliminates the need for physical cables, making it **cost-effective and flexible**.
- Allows **mobility**, enabling users to connect from anywhere within the signal range.
- Easier to **expand** compared to wired networks.

Disadvantages of Wireless Networks

- **Security risks** – More vulnerable to hacking and unauthorized access.
- **Interference issues** – Signal quality can be affected by other devices, walls, or environmental factors.
- **Limited range** – Wireless signals weaken over long distances.

TYPES OF WIRELESS NETWORKS

Wireless networks can be categorized based on **structure and coverage area**.

1) Ad-hoc (Peer-to-Peer) Networks

- Devices communicate **directly** with each other **without a central access point** (AP).
- Common in **temporary** or **small-scale** setups, such as **file sharing between laptops**.
- Example: Bluetooth file transfer between mobile phones.

TYPES OF WIRELESS NETWORKS

2) Infrastructure Wireless Networks

- Uses a **wireless access point (AP)** to manage and facilitate communication.
- Devices connect to the network through the AP, which may be linked to a wired network.
- Common in **corporate environments, public Wi-Fi hotspots, and home networks**.

TYPES OF WIRELESS NETWORKS

📌 Key Differences

Feature	Ad-hoc Network	Infrastructure Network
Central Access Point	❌ No AP, direct connection	✅ Uses AP for communication
Scalability	🚫 Limited	✅ Easily expandable
Security	🔴 Less secure	🟢 More security options available

TYPES OF WIRELESS NETWORKS

3) Wireless Personal Area Network (WPAN)

- Covers a **very short range** (few meters).
- Examples: **Bluetooth, ZigBee, Infrared (IR)**.
- Used for connecting devices like wireless keyboards, headphones, smartwatches.

TYPES OF WIRELESS NETWORKS

4) Wireless Local Area Network (WLAN)

- Covers a **larger area** like **homes, offices, universities**.
- Based on **Wi-Fi (IEEE 802.11)** standards.
- Provides internet access to multiple users.

TYPES OF WIRELESS NETWORKS

5) Wireless Metropolitan Area Network (WMAN)

- Covers a **city-wide area**.
- Example: **WiMAX (Worldwide Interoperability for Microwave Access)**.
- Used for high-speed internet services in cities.

TYPES OF WIRELESS NETWORKS

6) Wireless Wide Area Network (WWAN)

- Covers **long distances**, such as between cities or countries.
- Uses **cellular networks (3G, 4G, 5G)** for communication.
- Example: Mobile broadband internet.

TYPES OF WIRELESS NETWORKS

📌 Comparison of Wireless Network Types

Network Type	Coverage Area	Examples
WPAN	Few meters	Bluetooth, Infrared
WLAN	Up to 100m	Wi-Fi (802.11)
WMAN	Several kilometers	WiMAX
WWAN	Countrywide/Global	3G, 4G, 5G

WIRELESS TECHNOLOGIES OVERVIEW

Evolution of Wireless Technology	
Wireless technologies have evolved significantly over the years:	
📡 1G (First Generation)	Analog communication.
	Used for **voice-only calls**.
	No data transmission capabilities.
📡 2G (Second Generation)	Introduced **digital communication**.
	Allowed **SMS (Short Message Service)**.
	Technologies: **GSM (Global System for Mobile Communication)**, **CDMA (Code Division Multiple Access)**.

WIRELESS TECHNOLOGIES OVERVIEW

📡 2.5G (GPRS/EDGE)

Enhanced **data transmission rates** over 2G.

Introduced **GPRS (General Packet Radio Service)** and **EDGE (Enhanced Data rates for GSM Evolution)**.

📡 3G (Third Generation)

Faster **internet browsing** and **video calling**.

Used technologies like **UMTS (Universal Mobile Telecommunications System)** and **W-CDMA**.

WIRELESS TECHNOLOGIES OVERVIEW

📡 4G (Fourth Generation)
High-speed broadband internet.
Allowed streaming services (YouTube, Netflix).
Technologies: **LTE (Long-Term Evolution)**.
📡 5G (Fifth Generation) – Emerging Technology
Ultra-fast speeds, lower latency, supports IoT (Internet of Things).
Used for **autonomous vehicles, smart cities, remote surgeries**.

WIRELESS TECHNOLOGIES OVERVIEW

Wi-Fi Standards (IEEE 802.11)

Wi-Fi is based on **802.11** standards developed by **IEEE**.
Different versions include:

Wi-Fi Standard	Frequency	Speed
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4/5 GHz	600 Mbps
802.11ac	5 GHz	1 Gbps+
802.11ax (Wi-Fi 6)	2.4/5 GHz	10 Gbps

WIRELESS SECURITY PROTOCOLS

INTRODUCTION TO WIRELESS SECURITY

Why is Wireless Security Important?

Wireless networks are more **vulnerable** to attacks than wired networks because:

- **Open transmission** – Data travels through the air and can be intercepted.
- **Unauthorized access** – Attackers can connect to an unprotected Wi-Fi network.
- **Eavesdropping** – Hackers can use packet sniffing tools to steal data.

To **secure wireless networks**, encryption is used to **protect communication** between devices and prevent unauthorized access.

What is Encryption?

Encryption is the process of **converting readable data (plaintext)** by scrambling it **into an unreadable format (ciphertext)** to prevent unauthorized access

- Only authorized users with the **decryption key** can access the original data.
- Encryption protects sensitive information like **passwords, personal details, and financial transactions**.

WIRELESS SECURITY PROTOCOLS

To secure Wi-Fi networks, different encryption standards have been developed over the years.

1) Wired Equivalent Privacy (WEP)

- **Introduced**: 1997
- **Key Size**: 64-bit or 128-bit
- **Weakness**: Easily hacked using modern tools

WEP was the **first encryption standard** for wireless networks. It was designed to provide security similar to **wired networks**, but it has serious flaws:

- Uses **static encryption keys**, which can be cracked easily.
- Vulnerable to **replay attacks** and **packet sniffing**.
- Can be broken in minutes using tools like **Aircrack-ng**.

💡 **Why is WEP still in use?**
Some **old devices** only support WEP, which is why it still exists in some networks. However, **it is no longer recommended** for securing Wi-Fi.

WIRELESS SECURITY PROTOCOLS

2) Wi-Fi Protected Access (WPA)

Introduced: 2003

- **Key Size**: 256-bit
- **More secure than WEP**

To address WEP's security flaws, the **Wi-Fi Alliance** introduced **WPA (Wi-Fi Protected Access)**:

- Uses **dynamic encryption keys**, making it harder to crack.
- Introduced **Message Integrity Checks (MIC)** to detect altered data packets.
- Supports **WPA-PSK (Pre-Shared Key)** for home networks.

WPA Weaknesses:

- **Still vulnerable** to brute-force attacks.
- Uses **TKIP (Temporal Key Integrity Protocol)**, which has some security flaws.

WIRELESS SECURITY PROTOCOLS

3) Wi-Fi Protected Access 2 (WPA2)

- **Introduced**: 2006
- **Key Size**: 256-bit
- **Stronger encryption than WPA**

WPA2 is an **improvement over WPA**, with better encryption:

- Uses **AES (Advanced Encryption Standard)** instead of TKIP.
- Introduced **CCMP (Counter Mode with CBC-MAC Protocol)** for stronger security.
- Resistant to most known attacks.

WPA2 Weaknesses:

- Vulnerable to **KRACK (Key Reinstallation Attack)**, where attackers exploit weaknesses in the **four-way handshake** process.
- WPA2 networks can still be hacked if weak passwords are used.

Solution: Use **strong passwords** and enable **WPA3 (if supported by devices)**.

WPA VS. WPA2: KEY DIFFERENCES

Feature	WPA	WPA2
Encryption Algorithm	TKIP	AES
Security Level	Moderate	High
Vulnerable to Attacks	Yes	Less vulnerable
Introduced	2003	2006

ATTACKS ON WIRELESS NETWORKS

INTRODUCTION TO WIRELESS NETWORK ATTACKS

Wireless networks are convenient and widely used, but they are also more vulnerable to attacks than wired networks. Since wireless signals travel through the air, attackers can intercept or manipulate them without needing physical access.

Why Are Wireless Networks Targeted?

- **Open transmission medium** – Unlike wired networks, data can be intercepted over the air.
- **Weak security settings** – Many users still rely on outdated protocols like WEP.
- **Easy access** – Attackers can exploit open Wi-Fi hotspots and misconfigured networks.

Wireless attacks range from **passive eavesdropping** (listening to network traffic) to **active manipulation** (altering or injecting data into the network).

COMMON ATTACKS ON WIRELESS NETWORKS

1. Packet Sniffing

Attackers use specialized tools to capture and analyze network traffic. Since many protocols transmit data in plaintext, an attacker can steal sensitive information like usernames, passwords, and credit card details.

How It Works:

- Sniffers like **Wireshark** capture network packets.
- If the traffic is unencrypted, the attacker can read and extract information.
- Login credentials sent over HTTP or unencrypted protocols can be stolen.

Mitigation:

- Use **WPA2/WPA3 encryption** to secure data transmission.
- Prefer **HTTPS, VPNs, and encrypted messaging apps** to protect communication.

COMMON ATTACKS ON WIRELESS NETWORKS

2. Rogue Access Points (APs)

A rogue AP is an unauthorized wireless access point connected to a network, either by an attacker or an unaware employee. Attackers can use rogue APs to intercept and manipulate network traffic.

How It Works:

- The attacker sets up an AP with a legitimate-sounding SSID.
- Devices automatically connect to it, assuming it's a trusted network.
- Once connected, the attacker can capture and manipulate traffic.

Mitigation:

- Use **network access controls** to prevent unauthorized APs.
- Implement **MAC filtering and authentication** to allow only trusted devices.
- Regularly scan for rogue APs using **wireless intrusion detection systems (WIDS)**.

COMMON ATTACKS ON WIRELESS NETWORKS

3. Jamming (Denial-of-Service Attack)

Jamming is a type of **Denial-of-Service (DoS) attack** that disrupts wireless communication by overwhelming the network with noise or interference.

How It Works:

- Attackers use radio signals to interfere with Wi-Fi frequencies.
- Users experience **slow connections, dropped signals, or complete network failure**.
- Can be accidental (from Bluetooth devices or microwaves) or intentional.

Mitigation:

- Use **spectrum analyzers** to detect jamming sources.
- Increase **Wi-Fi power** or switch to less crowded frequencies.
- Implement **frequency-hopping** to minimize interference.

COMMON ATTACKS ON WIRELESS NETWORKS

4. Evil Twin Attack

An evil twin attack occurs when an attacker sets up a fake wireless access point that looks identical to a legitimate network. Users unknowingly connect to the attacker's AP instead of the real one.

How It Works:

- The attacker sets up a fake Wi-Fi network with the same SSID as a public hotspot.
- Victims connect, assuming it's a trusted network.
- All traffic passes through the attacker's device, allowing them to capture sensitive information.

Mitigation:

- Avoid connecting to **public Wi-Fi networks without verification**.
- Use **VPN services** to encrypt data transmission.
- Enable **wireless client isolation** to prevent direct communication between connected devices.

COMMON ATTACKS ON WIRELESS NETWORKS

4. Evil Twin Attack

An evil twin attack occurs when an attacker sets up a fake wireless access point that looks identical to a legitimate network. Users unknowingly connect to the attacker's AP instead of the real one.

How It Works:

- The attacker sets up a fake Wi-Fi network with the same SSID as a public hotspot.
- Victims connect, assuming it's a trusted network.
- All traffic passes through the attacker's device, allowing them to capture sensitive information.

Mitigation:

- Avoid connecting to **public Wi-Fi networks without verification**.
- Use **VPN services** to encrypt data transmission.
- Enable **wireless client isolation** to prevent direct communication between connected devices.