اونيبرسيتي مليسيا ڤهڠ السلطان عبدالله
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

Data & Network Security

Chapter 6 – Wireless Security

Outline

6.1 Introduction to Wireless Concept

6.2 Wireless Security

6.3 Wireless Threat

6.4 Wireless Installation

Learning Outcome

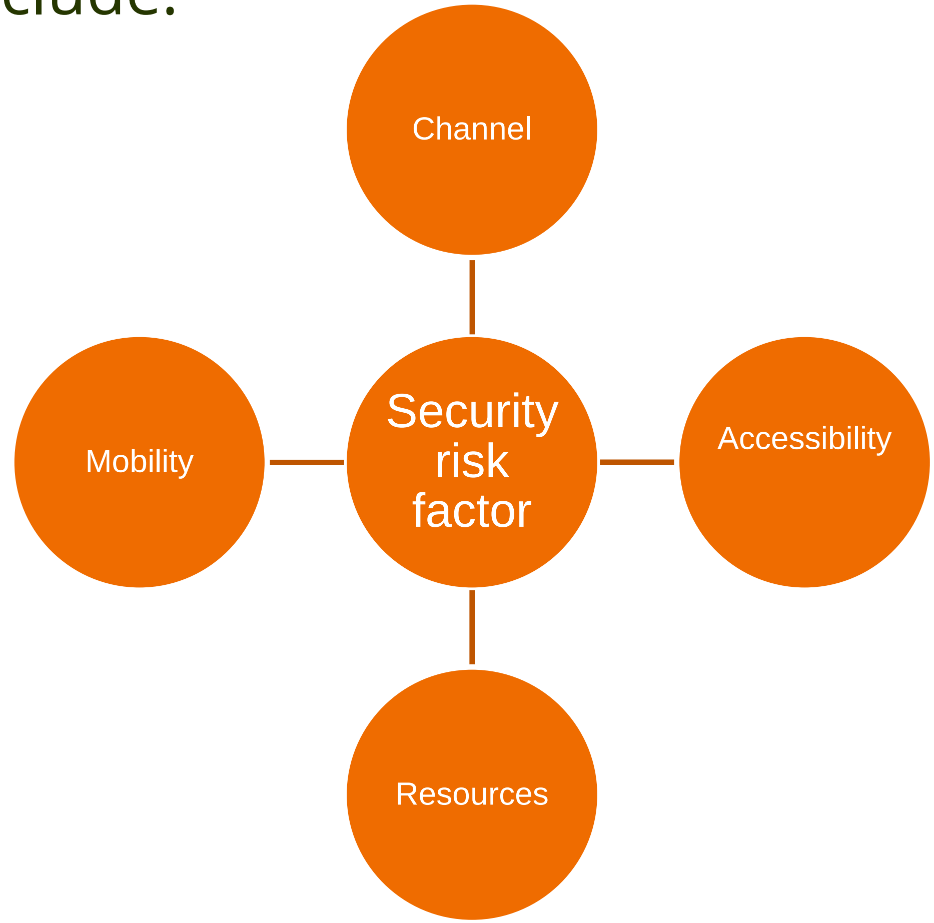
At the end of this chapter, the students are able to:

- Understand the concept of wireless networks.
- Apply the basic authentication process.
- Determine the type of wireless threats and issues.
- Apply any mechanism to defend the wireless network.

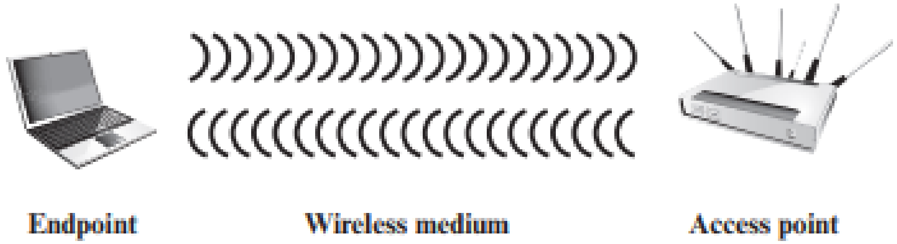
6.1 Introduction to Wireless Concept

Introduction to Wireless Concept

- Key factors contributing to the higher security risk of wireless networks compared to wired networks include:



Overview…



- The main standard for Wireless Local Area Network (WLAN) – 802.11 family of standards (802.11x [ax,ac,a,b,g,n]).
- Signals travel a few tens to hundreds of meters
- Ethernet (wired) uses physical transmission media – copper wire, and optical cable.
- WLANs use radio transmission – to spread signals widely without any cabling (wireless).

WHY, WHAT, HOW, WHO

- Why is wireless invented and used?
- Advantages?
- Disadvantages?

Wireless LAN 802.11 Overview

- In 1990, the IEEE 802 Committee formed a new working group, IEEE 802.11, with a charter to develop a protocol and transmission specifications for wireless LANs (WLANs).

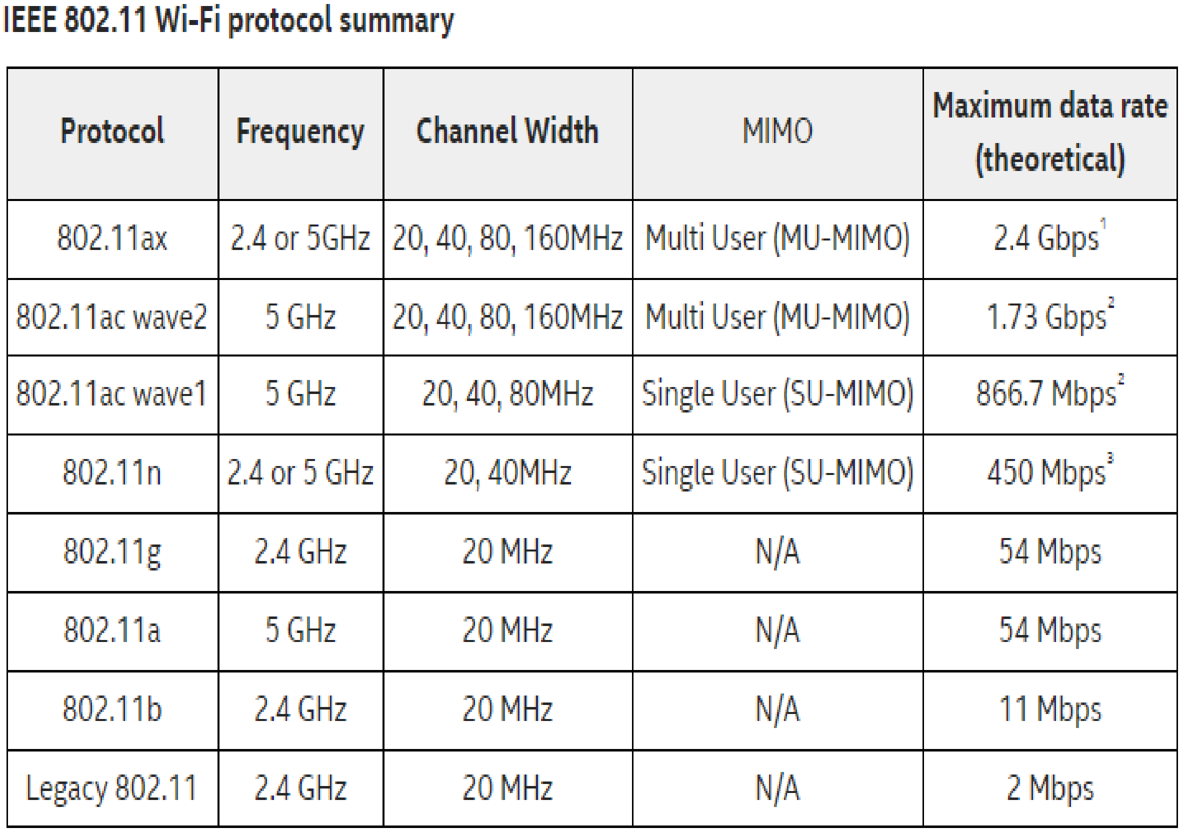
- The first 802.11 standard to gain broad industry acceptance was 802.11b.

- This organization, subsequently renamed the Wi-Fi (Wireless Fidelity) Alliance, created a test suite to certify interoperability for 802.11b products. The term used for certified 802.11b products is *Wi-Fi*.

- Wi-Fi certification has been extended to 802.11g products.

WIFI PROTOCOLS, NAMES AND VARIANTS

- 11be (2023-2024) - Next Generation (Wi-Fi 7) ...
- 11ax (2021) - Highest Speed (Wi-Fi 6) ...
- 11ac (2012) - High Speed (Wi-Fi 5) ...
- 11n (2009) - High Speed (Wi-Fi 4) ...
- 11g (2003) - Medium Speed (Wi-Fi 3) ...
- 11a (1999) - Medium Speed (Wi-Fi 2) ...
- 11b (1999) - Slow Speed (Wi-Fi 1) ...
- Original Spec (1997)



IEEE 802.11 Wi-Fi protocol summary

Protocol	Frequency	Channel Width	MIMO	Maximum data rate (theoretical)
802.11ax	2.4 or 5GHz	20, 40, 80, 160MHz	Multi User (MU-MIMO)	2.4 Gbps[1]
802.11ac wave2	5 GHz	20, 40, 80, 160MHz	Multi User (MU-MIMO)	1.73 Gbps[2]
802.11ac wave1	5 GHz	20, 40, 80MHz	Single User (SU-MIMO)	866.7 Mbps[2]
802.11n	2.4 or 5 GHz	20, 40MHz	Single User (SU-MIMO)	450 Mbps[3]
802.11g	2.4 GHz	20 MHz	N/A	54 Mbps
802.11a	5 GHz	20 MHz	N/A	54 Mbps
802.11b	2.4 GHz	20 MHz	N/A	11 Mbps
Legacy 802.11	2.4 GHz	20 MHz	N/A	2 Mbps

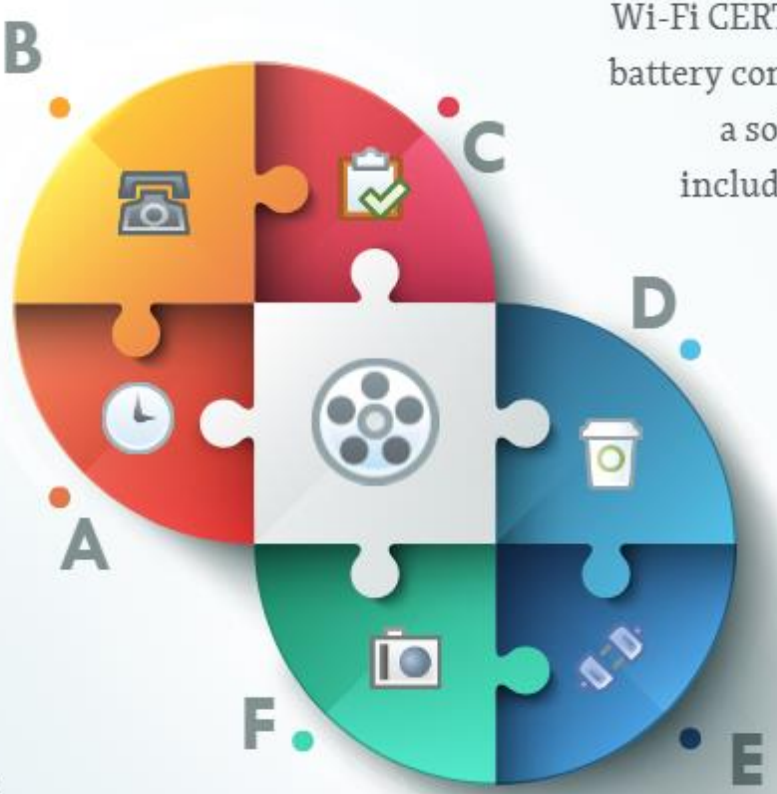
Source: https://www.intel.com/content/www/us/en/support/articles/000005725/wireless/legacy-intel-wireless-products.html

Wi-Fi 6 is the next generation wireless Wi-Fi based on the latest **802.11ax technology**. The technology will still be called 802.11ax, but the devices that are compatible with the new standard will be called Wi-Fi 6 compatible.

Wi-Fi CERTIFIED 6 networks enable lower battery consumption in devices, making it a solid choice for any environment, including smart home and Internet of Things (IoT) uses.

Wi-Fi 6 is rated to support transfer speeds of up to 10 Gb/s.

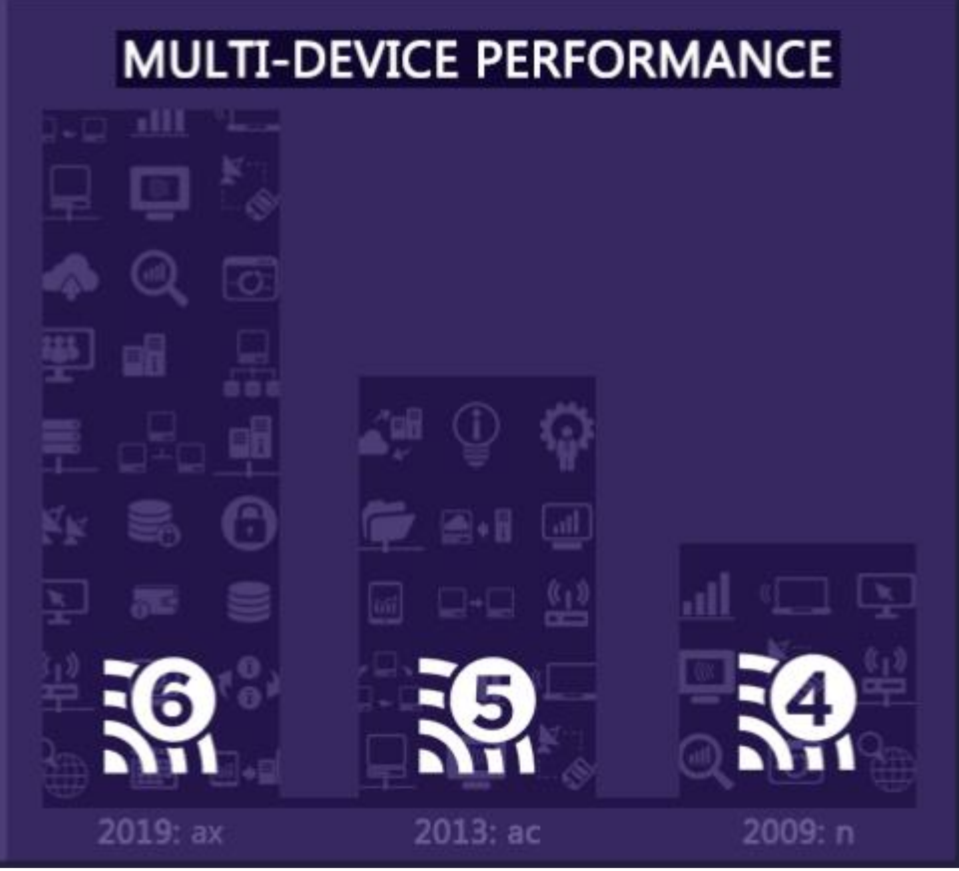
IEEE 802.11ax standard, enables next generation Wi-Fi connectivity providing the capacity, coverage, and performance required by users—even in environments with many connected devices such as stadiums and other public venues.



What is WiFi6?

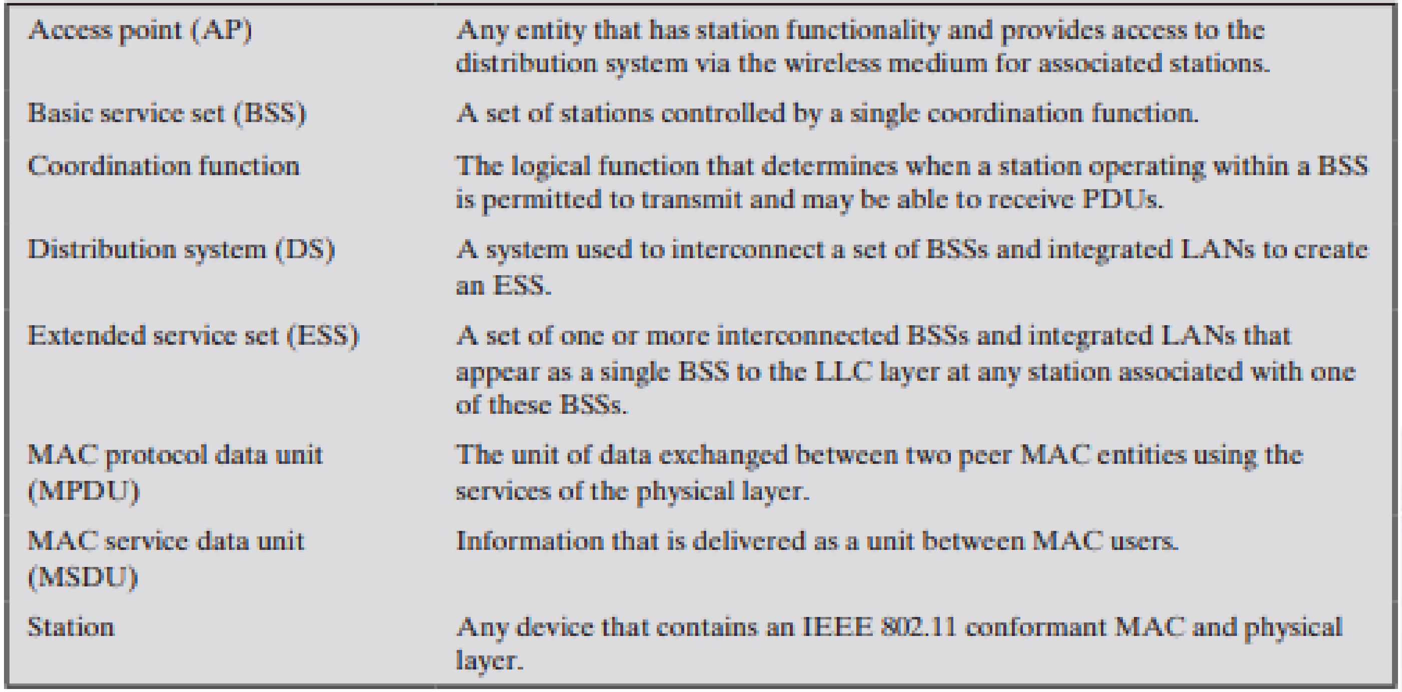
Wi-Fi GENERATIONS

Wi-Fi Generation	Sample User Interface Icon
Wi-Fi 6	6
Wi-Fi 5	5
Wi-Fi 4	4

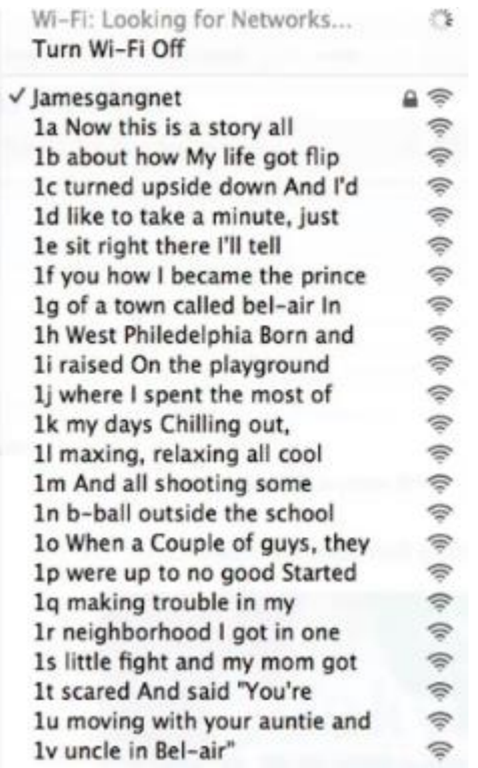


IEEE 802.11 Terminology

Table 7.1 IEEE 802.11 Terminology



Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

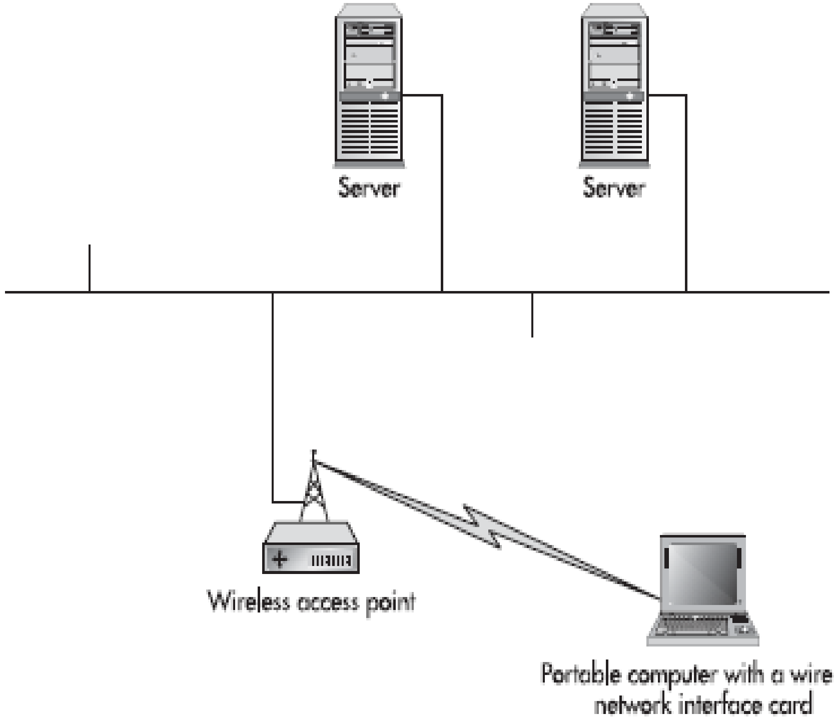


Wi-Fi: Looking for Networks...
Turn Wi-Fi Off

✓ Jamesgangnet
1a Now this is a story all
1b about how My life got flip
1c turned upside down And I'd
1d like to take a minute, just
1e sit right there I'll tell
1f you how I became the prince
1g of a town called bel-air In
1h West Philedelphia Born and
1i raised On the playground
1j where I spent the most of
1k my days Chilling out,
1l maxing, relaxing all cool
1m And all shooting some
1n b-ball outside the school
1o When a Couple of guys, they
1p were up to no good Started
1q making trouble in my
1r neighborhood I got in one
1s little fight and my mom got
1t scared And said "You're
1u moving with your auntie and
1v uncle in Bel-air"

Basic Operation

- Consists of
  - Main wired network
  - Access points (APs)
  - Wireless stations



Typical wireless network architecture

Basic Operation

- ## Main Wired Network
  - WLAN connected to the site's main wired LAN.
  - Assume that the LAN is Ethernet.
  - Main Ethernet LAN is needed because most wireless devices are client machines and the servers they connected to are located on the Ethernet LAN.
- ## Access Points (APs)
  - Wireless access point – serves several functions.
  - A bridge between the main wired LAN and wireless LAN. Bridges are devices that connect two LANs of different technology.
  - 802.3 (Ethernet) and 802.11 (Wireless)
  - Access point controls the wireless stations. Example -> it tells stations what signal power to use when they transmit
- ## Wireless Stations
  - Mobile Smart Phone
  - Laptop

6.2 Wireless Security

Wireless Security

Four security approaches:

1. WEP (Wired Equivalent Privacy)
2. WPA (Wi-Fi Protected Access)
3. WPA2 (Wi-Fi Protected Access II)
4. WPA3 (Wi-Fi Protected Access III)

WPA also has two generations named Enterprise and Personal.

Cont…

- Wired Equivalent Privacy (WEP) algorithm
  - 802.11 privacy
- Wi-Fi Protected Access (WPA)
  - set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard
- Robust Security Network (RSN)
  - final form of the 802.11i standard
- Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program

WEP (Wired Equivalent Privacy)

- The specification of a protocol, along with the chosen key length (if variable) is known as a *cipher suite*. The options for the confidentiality and integrity cipher suite are:

- ENCRYPTION: WEP, with either a 40-bit or 104-bit key,

- PASSPHRASE: Key 1-4 Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9". It should be 10 hex or 5 ASCII characters in length for 40/64-bit encryption and 26 hex or 13 ASCII characters in length for 104/128-bit encryption.

WPA/WPA2 Personal

- WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard.

- **Encryption**:
  - TKIP (Temporal Key Integrity Protocol)
  - AES (Advanced Encryption Standard)
- **Pre-Shared Key (PSK)**:
  - A key of 8-63 characters

WPA3 will **protect against dictionary attacks** by implementing a new key exchange protocol.

Smart bulbs, wireless appliances, smart speakers, and other screen-free gadgets make everyday tasks just a little bit easier, but connecting them to Wi-Fi can be a Sisyphean task. WPA3 streamlines the process.

WPA3 defines a new handshake that "**will deliver robust protections** even when users choose passwords that fall short of typical complexity recommendations".

In other words, even if you're using a **weak password**, the WPA3 standard will protect against brute-force attacks

WPA3 Protocol

WPA3-Personal

Includes optional 192-bit minimum strength security mode, aligned with the Commercial National Security Algorithm (CNSA) Suite from the Committee on National Security Systems. This was a request by the US government.

Uses 128-bit encryption

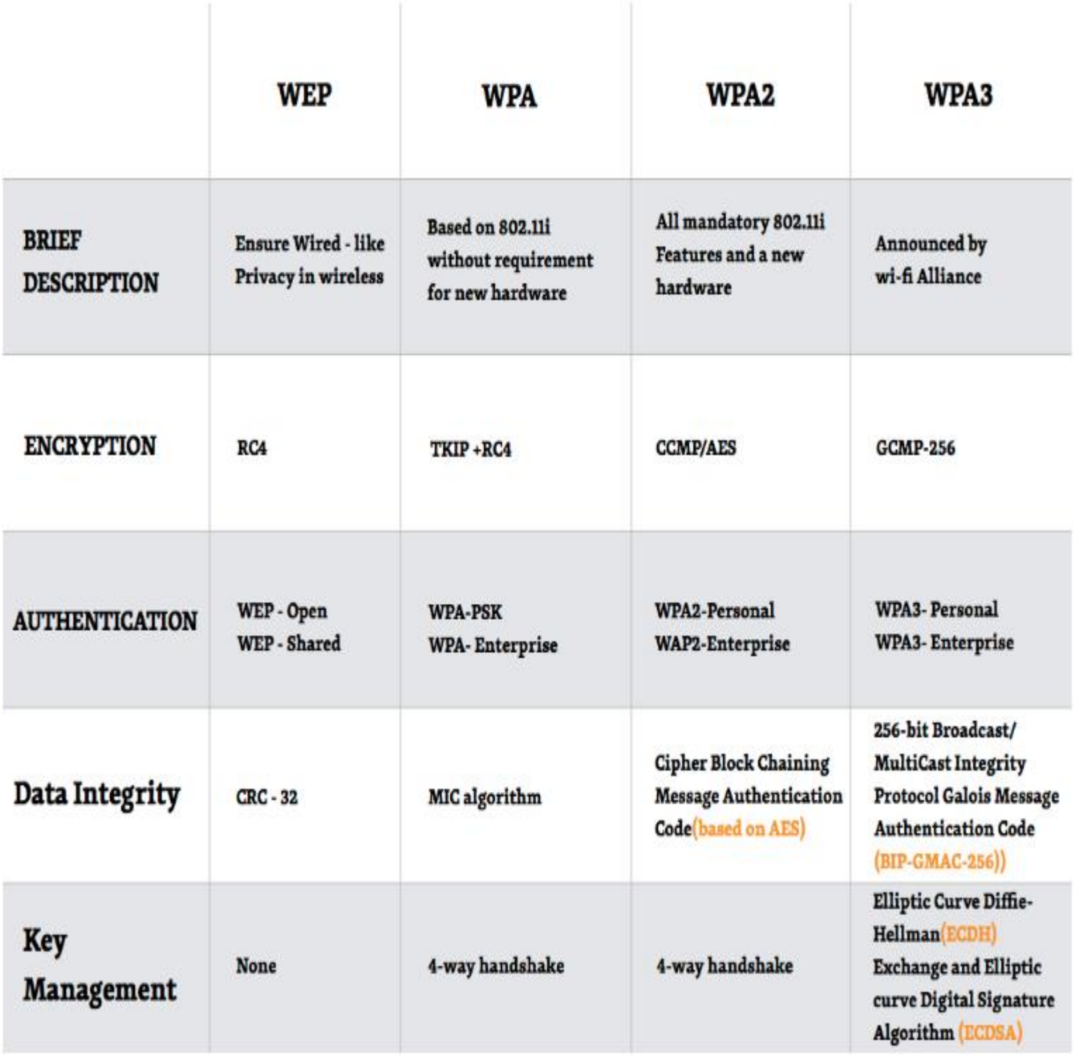
Makes use of a Simultaneous Authentication of Equals (SAE) handshake which protects against brute force attacks

Incorporates Forward Secrecy means that a new set of encryption keys are generated every time a WPA3 connection is made, so if the initial password is compromised, it won't matter

Bolsters security on public networks

Easily manages connected devices

Allows Natural Password Selection, which the Wi-Fi Alliance claims will make it easier for users to remember passphrases



	WEP	WPA	WPA2	WPA3
BRIEF DESCRIPTION	Ensure Wired - like Privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i Features and a new hardware	Announced by wi-fi Alliance
ENCRYPTION	RC4	TKIP +RC4	CCMP/AES	GCMP-256
AUTHENTICATION	WEP - Open WEP - Shared	WPA-PSK WPA- Enterprise	WPA2-Personal WAP2-Enterprise	WPA3- Personal WPA3- Enterprise
Data Integrity	CRC - 32	MIC algorithm	Cipher Block Chaining Message Authentication Code(based on AES)	256-bit Broadcast/ MultiCast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256))
Key Management	None	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman(ECDH) Exchange and Elliptic curve Digital Signature Algorithm (ECDSA)

6.3 Wireless Threat

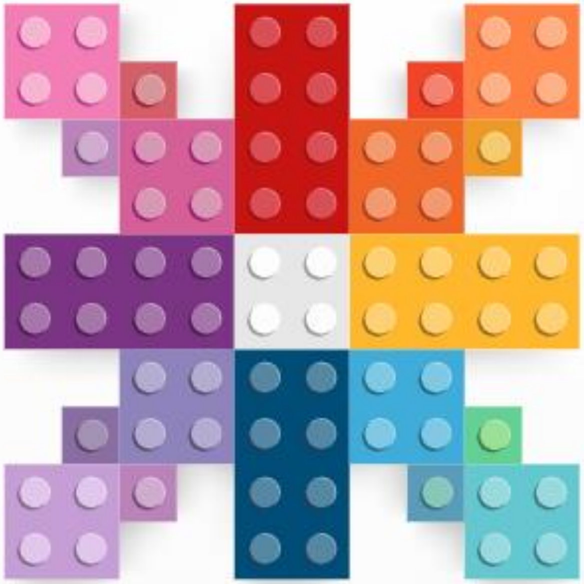
Wireless Threat

- A wireless threat is a threat that uses wireless as an attack vector. The offensive tools like aireplay-ng, aircrack-ng, and mdk3 can be used to run like a flood of de-authentication frames, breaking authentication and exploiting wireless networks.
- They can sniff wireless packet traffic, jam an AP until it is frozen and unavailable, and flood fake beacon tools to imitate a fake AP.
- Another method called wardriving involves attackers searching for wireless networks with vulnerabilities while moving around an area in a moving vehicle. Other names for wardriving are warbiking, warcycling, warwalking and similar use of the same approach but with other modes of transportation.
- Apart from that, a wireless attacker uses a specialized wireless dongle to do signal or packet injection. This dongle is a must-have tool for an attacker because a normal Wi-Fi dongle cannot do packet injection or even sniff wireless traffic other than its traffic.

You will need a **WiFi dongle with chipsets that support packet injection.** The built-in laptop WiFi does not support this.

How To Identify Wifi Adapter Chipset?

Run **airmon-ng**



Chipsets that support monitor mode AND packet injection:

Atheros AR9271

Ralink RT3070

Ralink RT3572

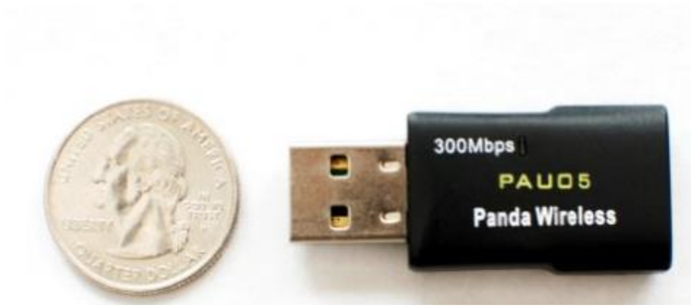
Packet injection and Monitor Mode

Monitor mode is what you use to "sniff" or capture (encrypted) data transmitted by wireless routers and devices nearby. While packet injection is what you use to transmit data to those networks.

WiFi Dongles Required For Hacking

ALFA AWUS036NHA (Atheros AR9271)

Adapter Panda PAU05 USB Wi-Fi



LEGUANG LG-N100

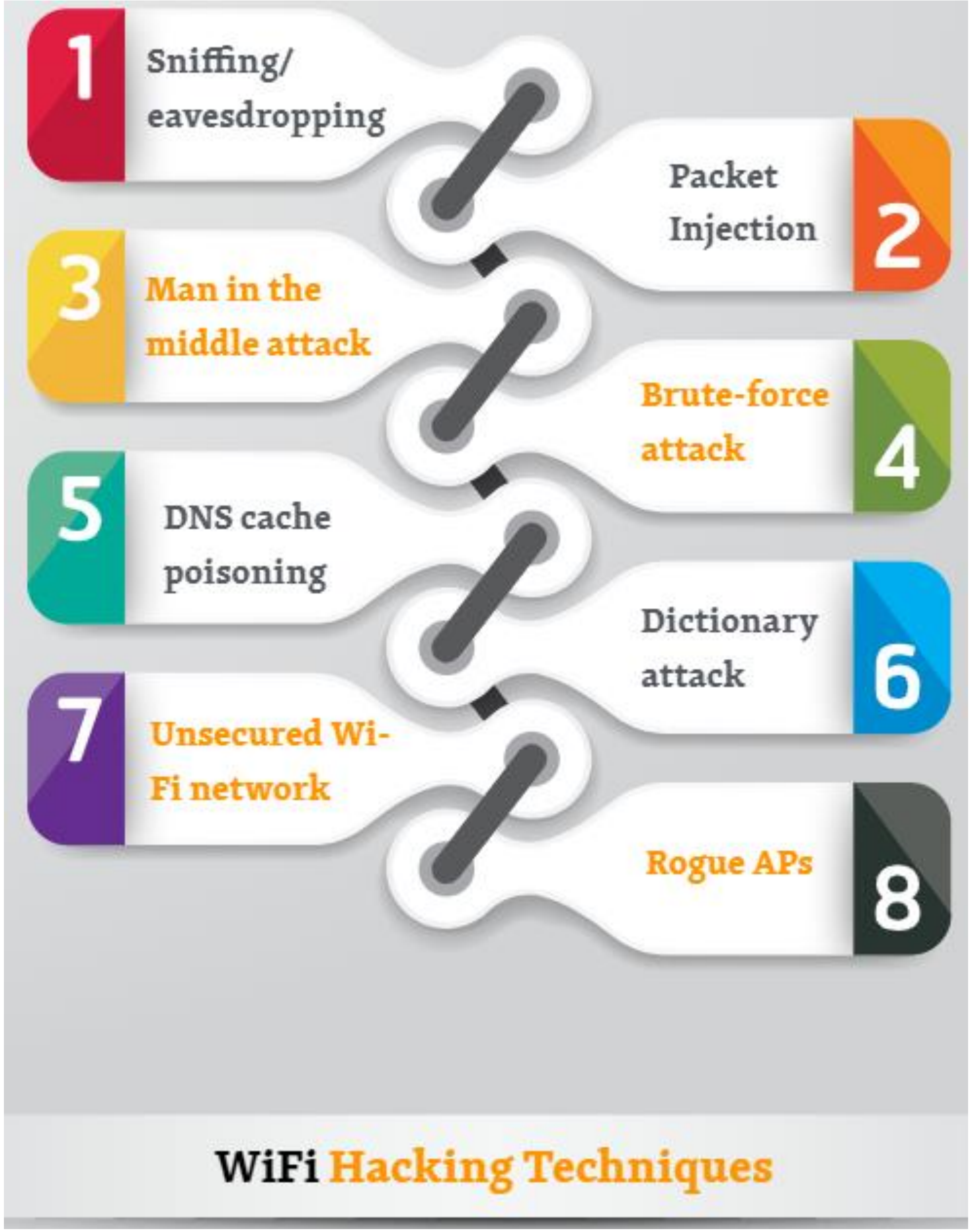
ALFA AWUS036NH
(Ralink RT3070)

Currently, open Wi-Fi networks—the kind you find in airports, hotels, coffee shops, and other public locations—are a security mess.

They're open and allow anyone to connect, traffic sent over them isn't encrypted at all. **It doesn't matter whether you have to sign in on web page after you join the network**—everything sent over the connection is sent in plain text that people can intercept.

The rise of **encrypted HTTPS** connections on the web have improved things, but people could still see which websites you were connecting to and view the content of HTTP pages.

Privacy on Public Wi-Fi Networks



1
Sniffing/ eavesdropping
2
Packet Injection
3
Man in the middle attack
4
Brute-force attack
5
DNS cache poisoning
6
Dictionary attack
7
Unsecured Wi-Fi network
8
Rogue APs
WiFi Hacking Techniques

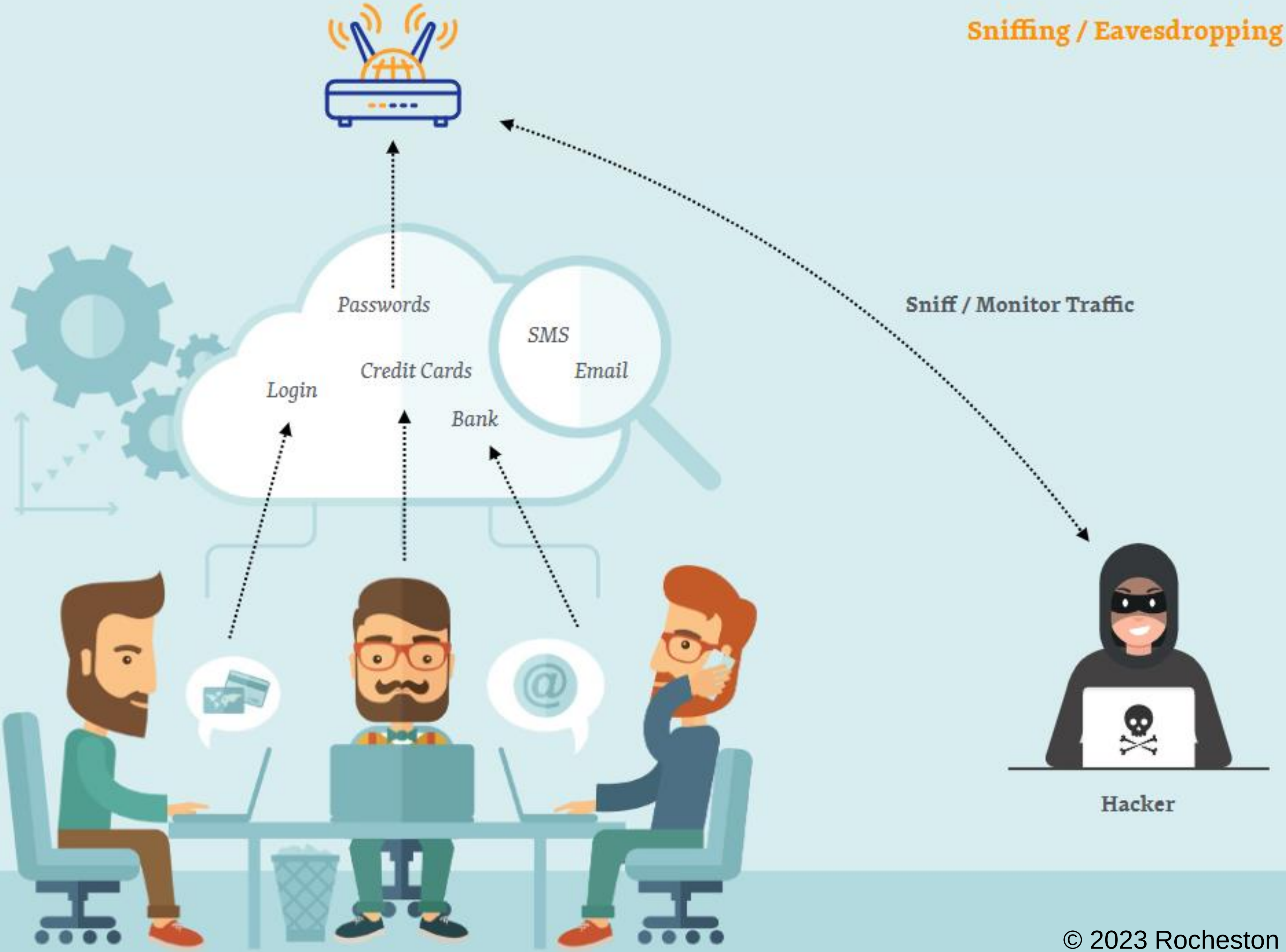
Wireless Threat

- The increased development of Wireless LAN has increased the potential threats to the user.

- A WLAN uses radio frequency that exposes layer 1 and layer 2 to whoever can listen into the radio frequency range.

- The attacks for WLAN include but are not limited to Eavesdropping, Rogue access points, Man-in-the-middle, and Piggybacking.

Sniffing / Eavesdropping



Eavesdropping

- Enables an attacker to gain access to the network traffic and read the message contents that are being transmitted across the network.

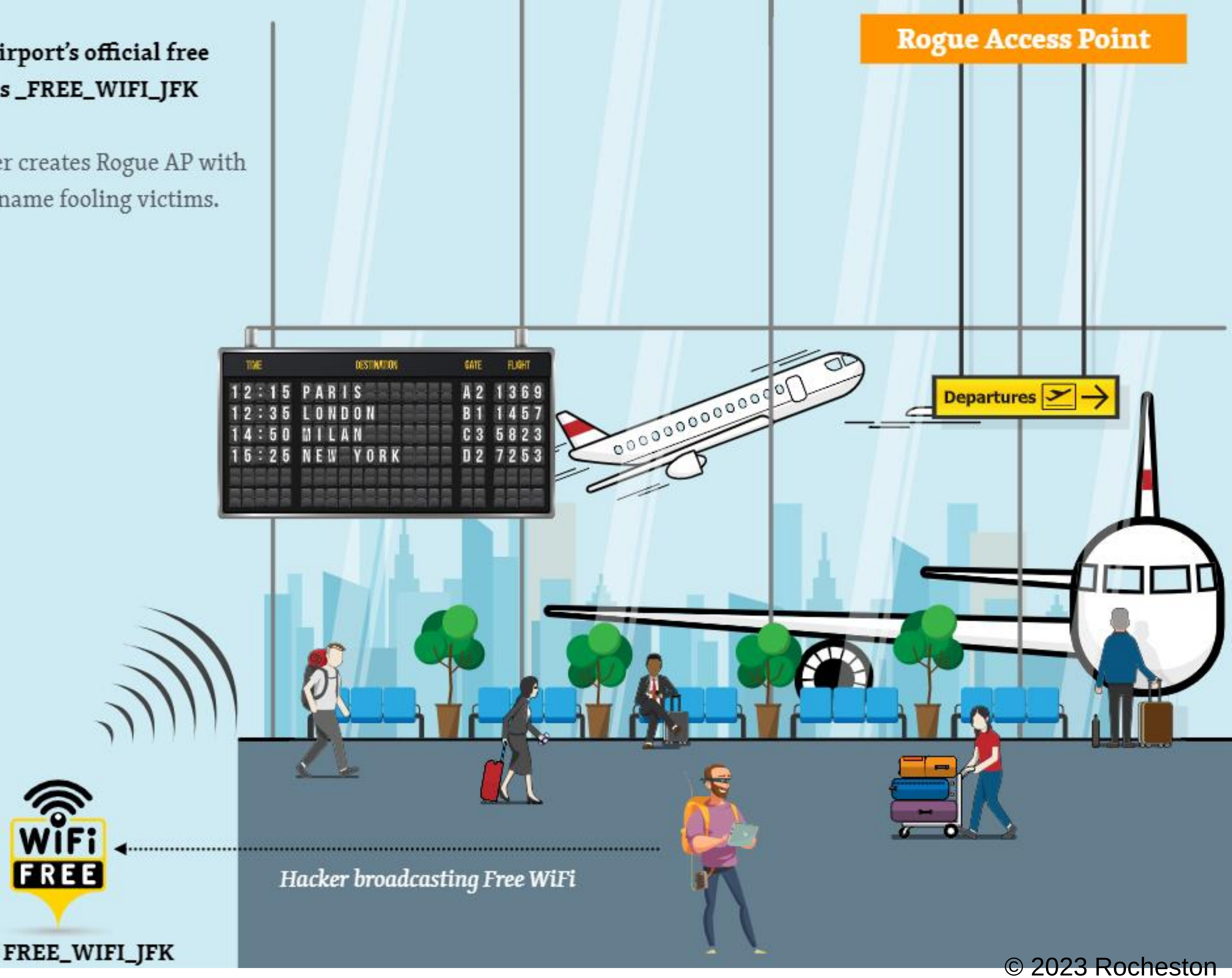
- The attacker passively monitors the wireless session and the payload such as the packets, especially their source, destination, size, number and time of transmission.

- This attack can be done away from the premises of any organizations.

Rogue Access Point

JFK Airport's official free Wifi is _FREE_WIFI_JFK

Hacker creates Rogue AP with same name fooling victims.



Hacker broadcasting Free WiFi

SSID: FREE_WIFI_JFK

Rogue Access Points

- The intruder installs an unsecured AP in public areas to intercept traffic from valid wireless clients.

- By doing so, it will create a backdoor into a trusted network by changing its SSID to the SSID of the target organization.

- The attacker uses an unused wireless channel to set up this fake access to stolen credential information of a user.

Step 1: Scan the Wi-Fi network using Wi-Fi scanner

Step 2: Target the Wi-Fi you want to hack

Step 3: Extract the password hash

Step 4: Crack the password

Step 5: Join the WiFi network

You just broken in.

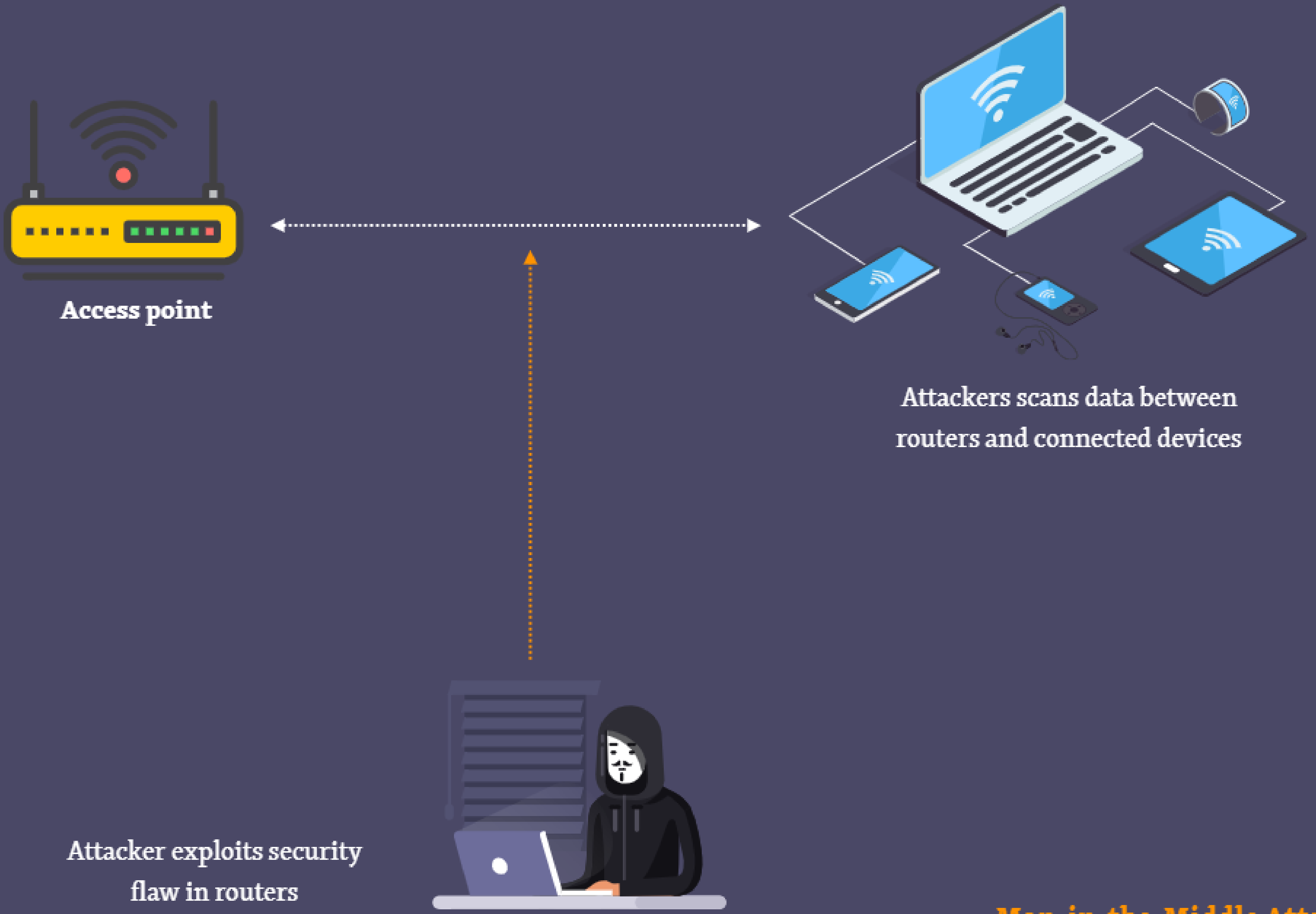
Steps for Hacking Wi-Fi Networks

Piggybacking

- Use other Wi-Fi connections (account) freely without being known by the owner.

- The aim is to save money or avoid paying.

- The user that uses the Wi-Fi illegally, can use everything that the victim subscribes. The attackers can perform the attack to other locations from the Wi-Fi connection.



Access point

Attackers scans data between routers and connected devices

Attacker exploits security flaw in routers

Man-in-the-Middle Attack

Man-in-the-Middle

- Type of eavesdropping attack that occurs when a malicious actor inserts himself as a relay/proxy into a communication session between people or systems.
- Exploits the real-time processing of transactions, conversations or transfer of other data.
- Allow attackers to intercept, send and receive data never meant to be for them without either outside party knowing until it is too late.

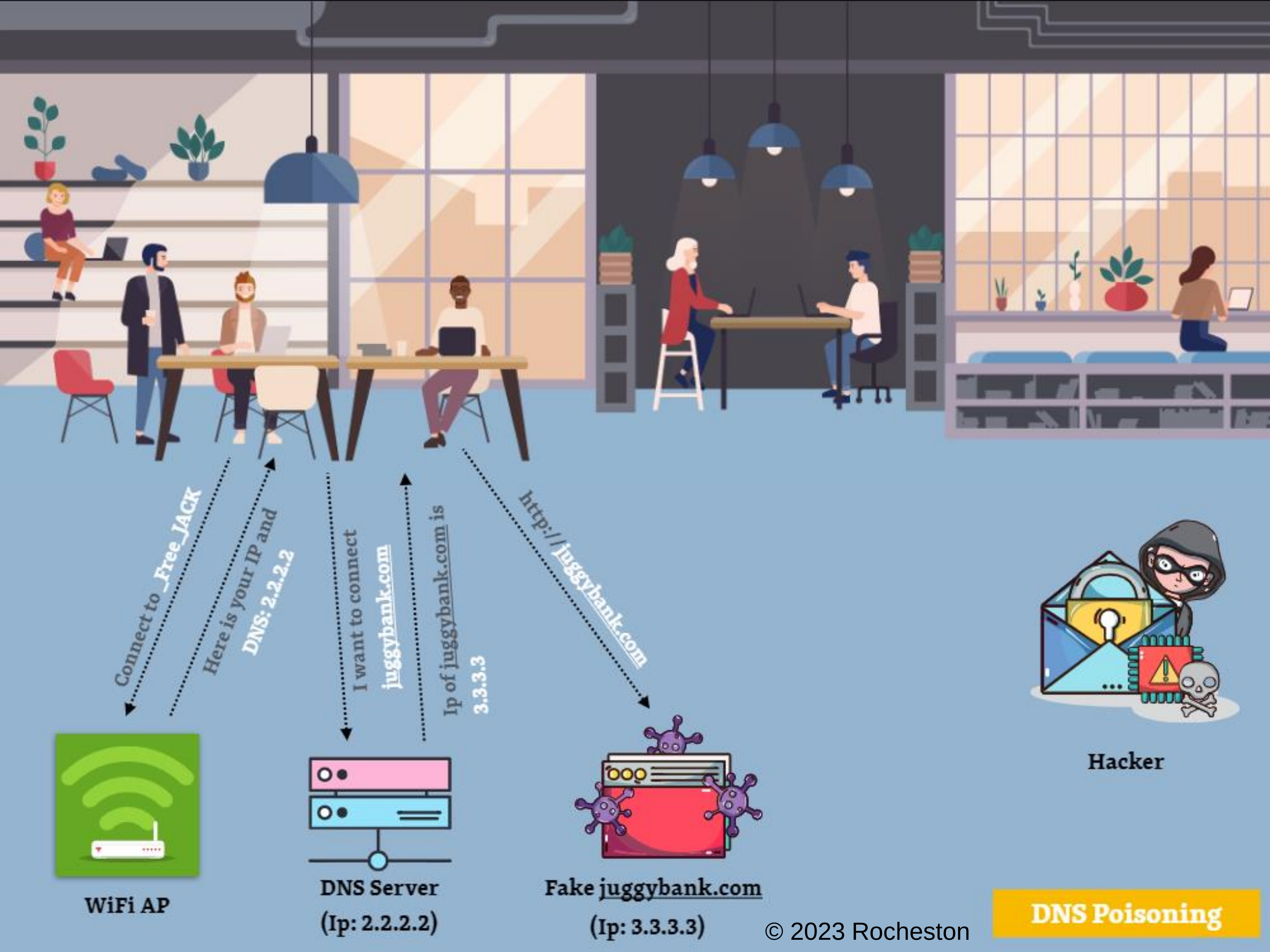
Unsecured WiFi Networks: Hackers can sniff raw traffic traversing the wireless network. Unless you use VPN or SSL traffic then your data is exposed.

Unsecured WiFi

WiFi Name: CORP-ACCOUNTING
Encryption: None
Channel 2.4GHZ

Packet Injection

Sniff and 'Inject' packets into the wire



Connect to _Free_JACK

Here is your IP and DNS: 2.2.2.2

I want to connect juggybank.com

Ip of juggybank.com is 3.3.3.3

http://juggybank.com

WiFi AP

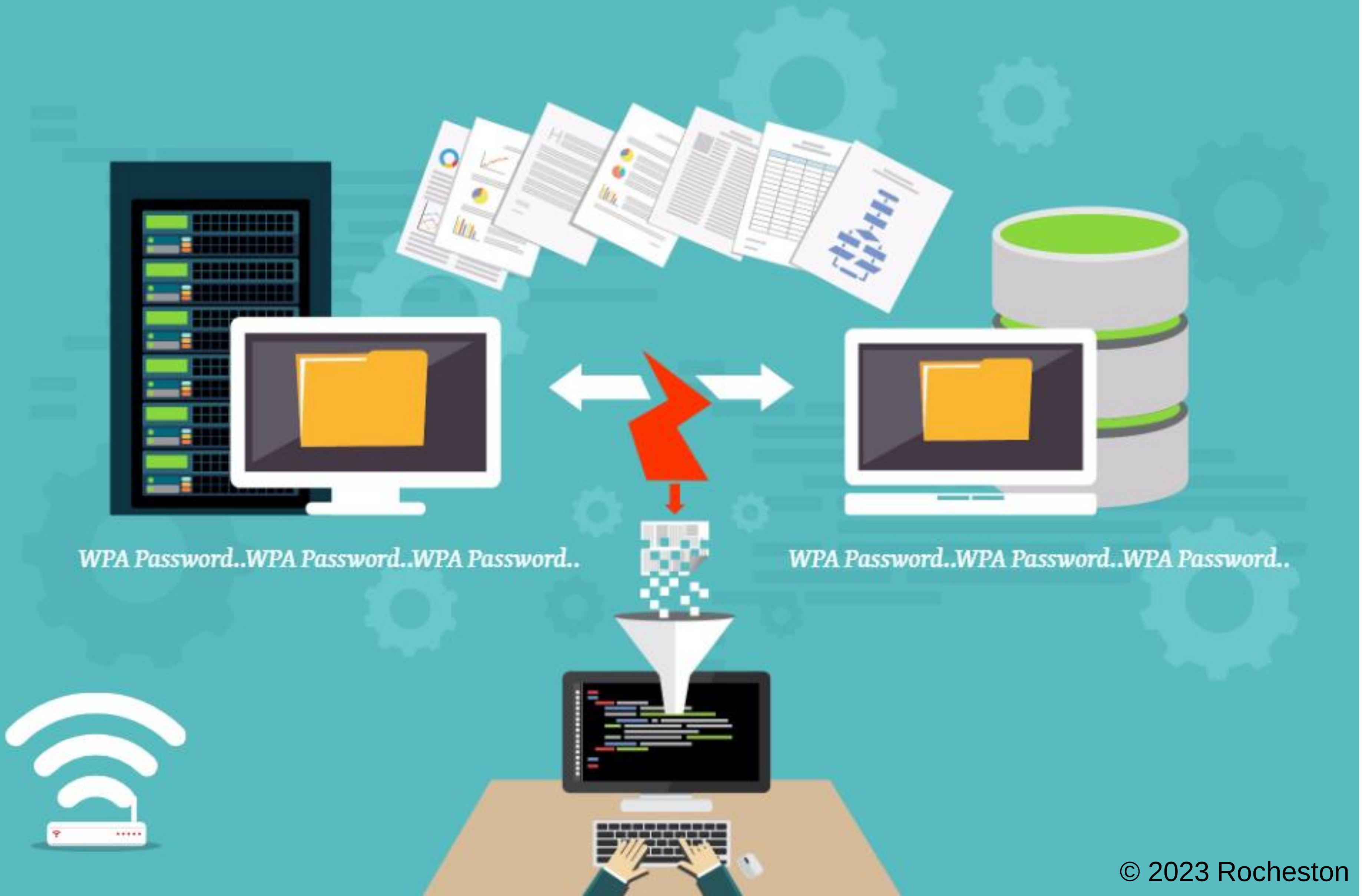
DNS Server (Ip: 2.2.2.2)

Fake juggybank.com (Ip: 3.3.3.3)

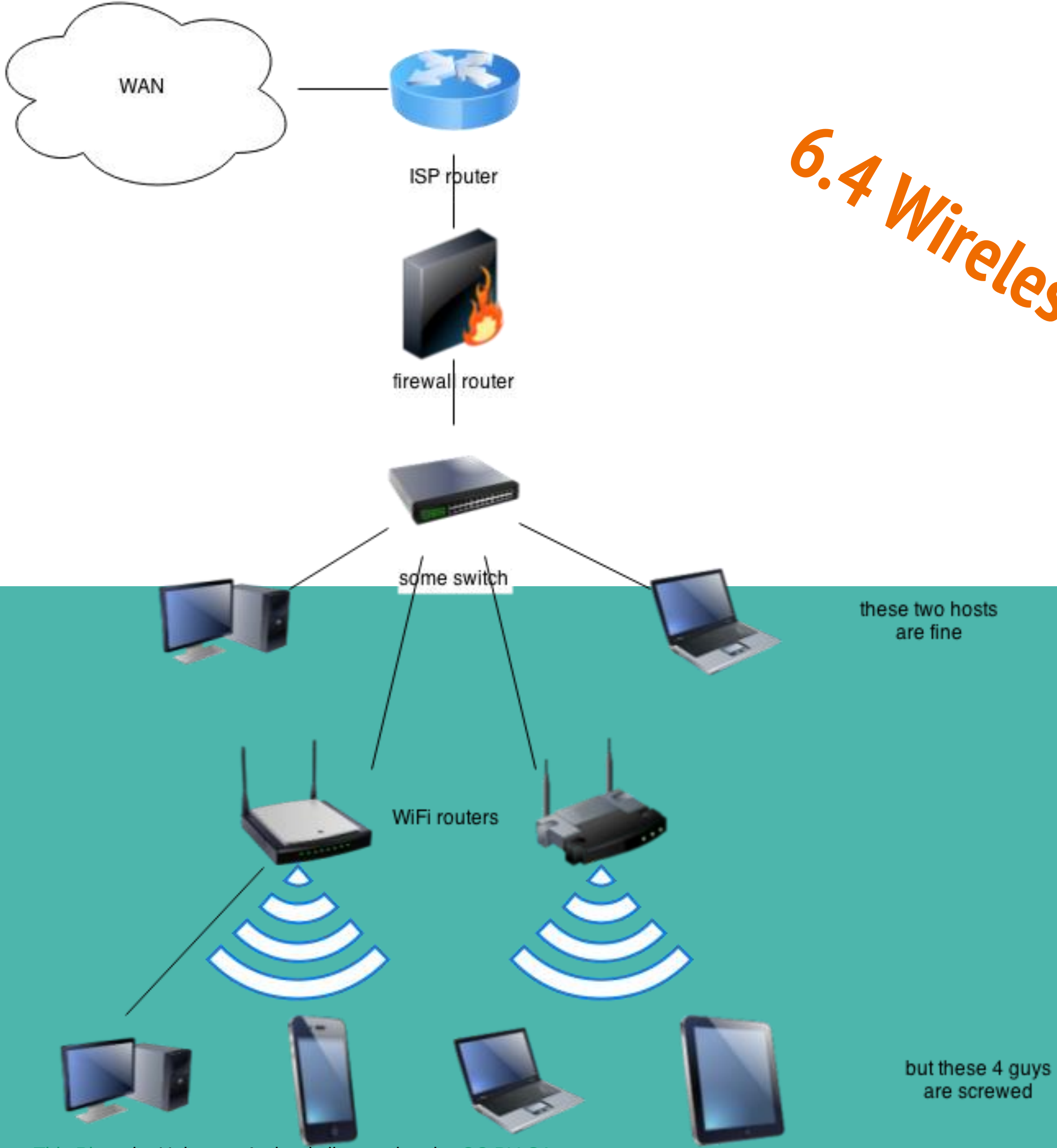
Hacker

DNS Poisoning

WiFi Password Brute-forcing


WPA Password..WPA Password..WPA Password..
WPA Password..WPA Password..WPA Password..

6.4 Wireless Installation



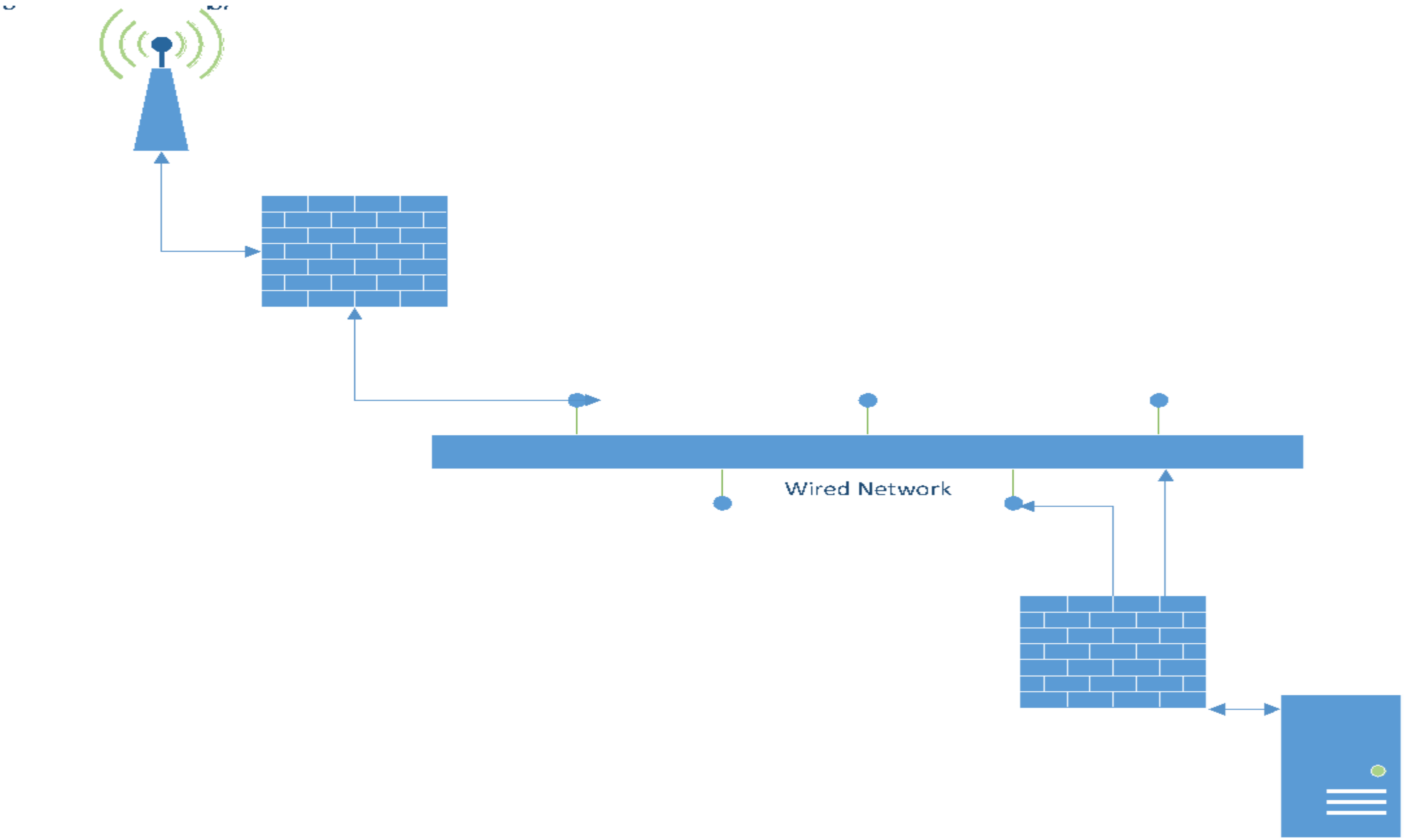
Wireless Installation

- The design should cover:
  - Topology (connection to wired network)
  - Protocol used (b, g, n, ac, ax, or need to be compatible with older device etc.)
  - Security Technology used (WEP?, WPA2, WPA3 or latest secure protocol, RADIUS – Remote Authentication Dial-In User Service)
  - User (how many users to cater for a single Wi-Fi AP?)
  - Placement and coverage (indoor, outdoor, small and secluded areas in a building)
  - Implementation cost of the wireless infrastructure.

Wireless Installation

- Before deciding to install a wireless network:
  - system/application being used
  - the user of the wireless network (who are they and what are their main portfolios for accessing the wireless system)
  - capacity (number of users)
  - the way it is attached to a wired network

Topology



Wireless LAN Security Technology

- There are a lot of technologies that can be used to ensure a wireless LAN is secure such as:
  - Wireless Authentication (RADIUS?)
  - Firewall (inside and outside of an AP)
  - Wireless IPS (some APs are dedicated and configured in WIPS mode; preconfigured for a particular channel and listen to the frequency spectrum all the time to look for anomalies that these APs do not broadcast any WLAN network or allow a user to associate with it
  - Antivirus

Common Defence Strategies

- Change router default username and password.
- Change the internal IP subnet if possible.
- Change the default name and hide broadcasting of the SSID (Service Set Identifier).
- None of the attack methods are faster or more effective when a larger passphrase is used.
- Restrict access to your wireless network by filtering access based on the MAC (Media Access Control) addresses.
- Use encryption.
- Use centralized authentication like the RADIUS server.

Summary

- Wireless networking provides numerous opportunities to increase productivity and lower implementation costs. It also alters an organization’s overall computer security risk profile.

- Although it is impossible to eliminate all risks associated with wireless networking, it is possible and reasonable to level the security by adopting a systematic approach to assessing and managing risk.

- This chapter discussed wireless technologies, components and their concepts, wireless threats and vulnerabilities of wireless networks and described commonly available countermeasures or security approaches that could be used to mitigate those risks.

Source: https://www.ijstr.org/final-print/july2017/An-Analysis-Of-Wireless-Security.pdf

We do not have WiFi, talk to each other. Pretend it is 1995.

References

Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (2003). Securing Your Network.

Luciana Obregon. (2016), Infrastructure Security Architecture for Effective Security Monitoring.

William Stallings. (2017). Network Security Essential.

Man-in-the-Middle Attack.

https://www.veracode.com/security/man-middle-attack

https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/