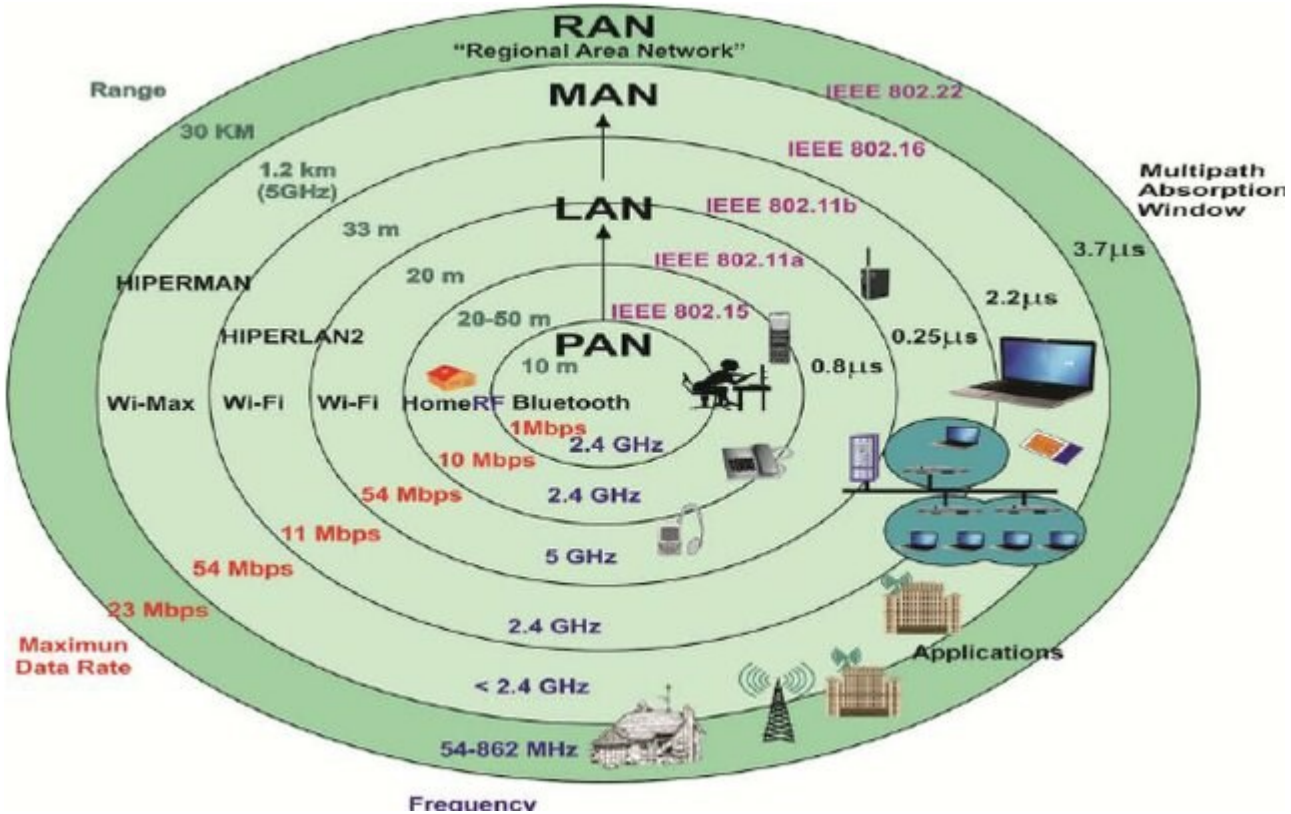
University of Babylon College of information Technology
Department of Information Security

Ethical Hacking
Lecture 9: Hacking Wireless Networks

Asst.Lect. Rasha Hussein

Wireless Standards

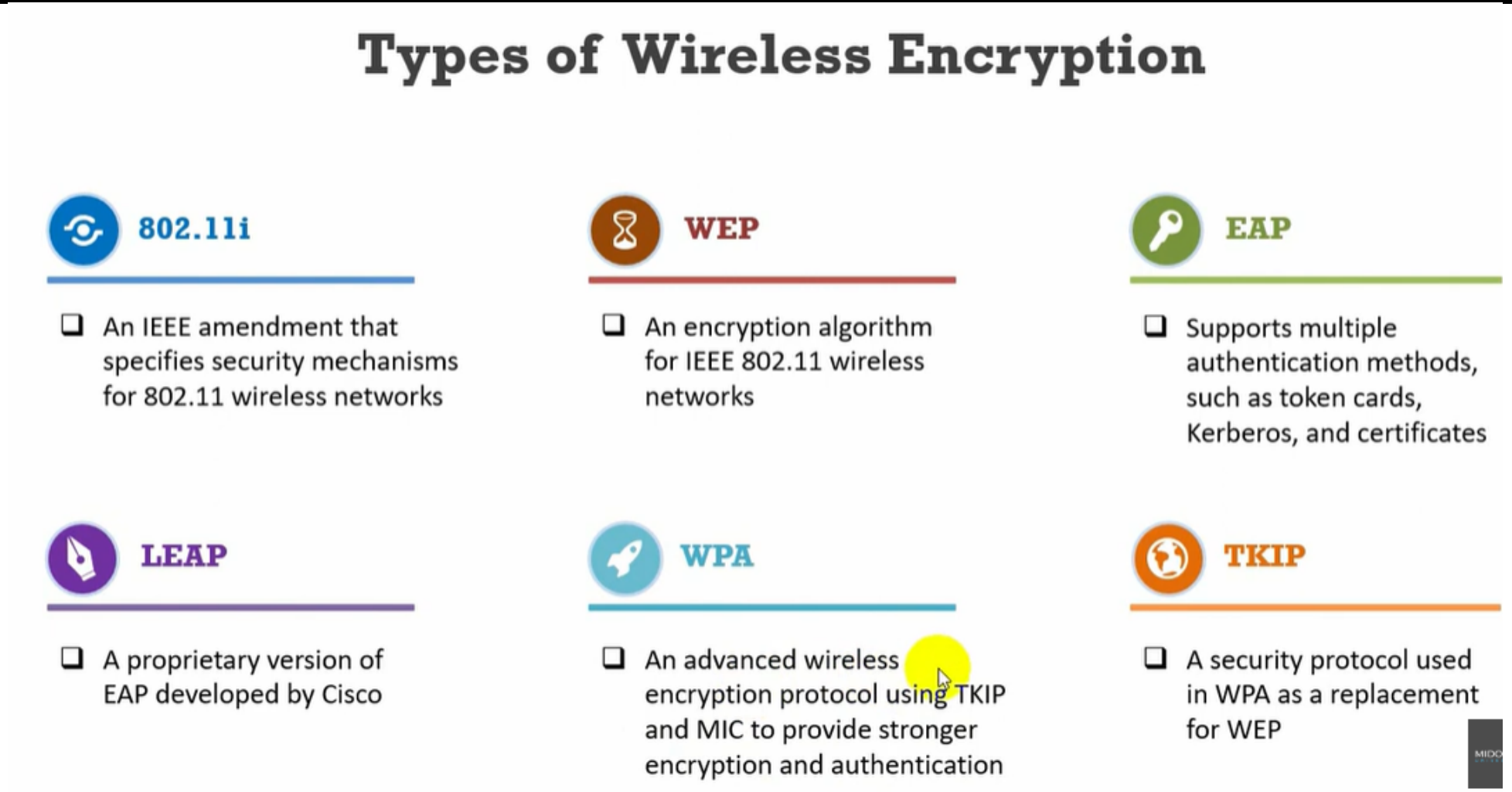
- **802.11 Series** - defines the standards for wireless networks(WLAN)
- **802.15.1** - Bluetooth.
- **802.15.4** - Zigbee - low power, low data rate, close proximity ad-hoc networks·
- **802.16 -** WiMAX - broadband wireless metropolitan area networks



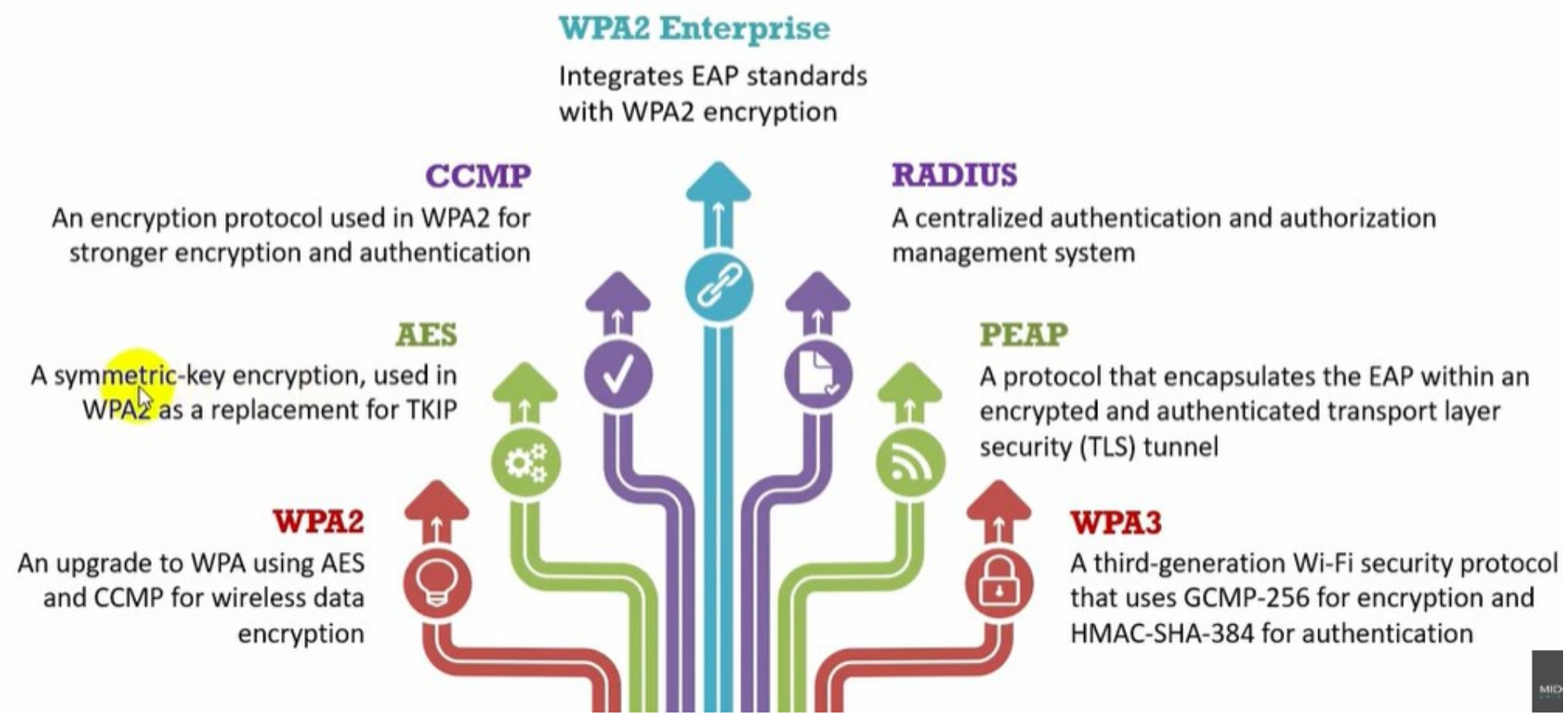
What are Wi-Fi attacks?

- Wi-fi is an important area of cyber security and there is no need for physical cable for the network. Wi-Fi has access to a network signal radius everywhere. The devices and systems can have a network without physical access due to Wi-fi. But everything comes with cons and pros, and if we talk about cybersecurity, it has been established that Wi-fi networks are extremely vulnerable to security breaches and it is very easy to be hacked by hackers. Wi-Fi can be accessed by almost every device in the modern day: it can be smartphones, tablets, computers, and laptops. To know whether someone has been tampering with your personal Wi-Fi there are certain signs that can prove it. The first and most important sign is that your internet speed gets slower, as someone else is using your Wi-Fi surf.

Types of Wireless Encryption



Types of Wireless Encryption



Comparison of WEP , WPA. WPA2, and WPA3

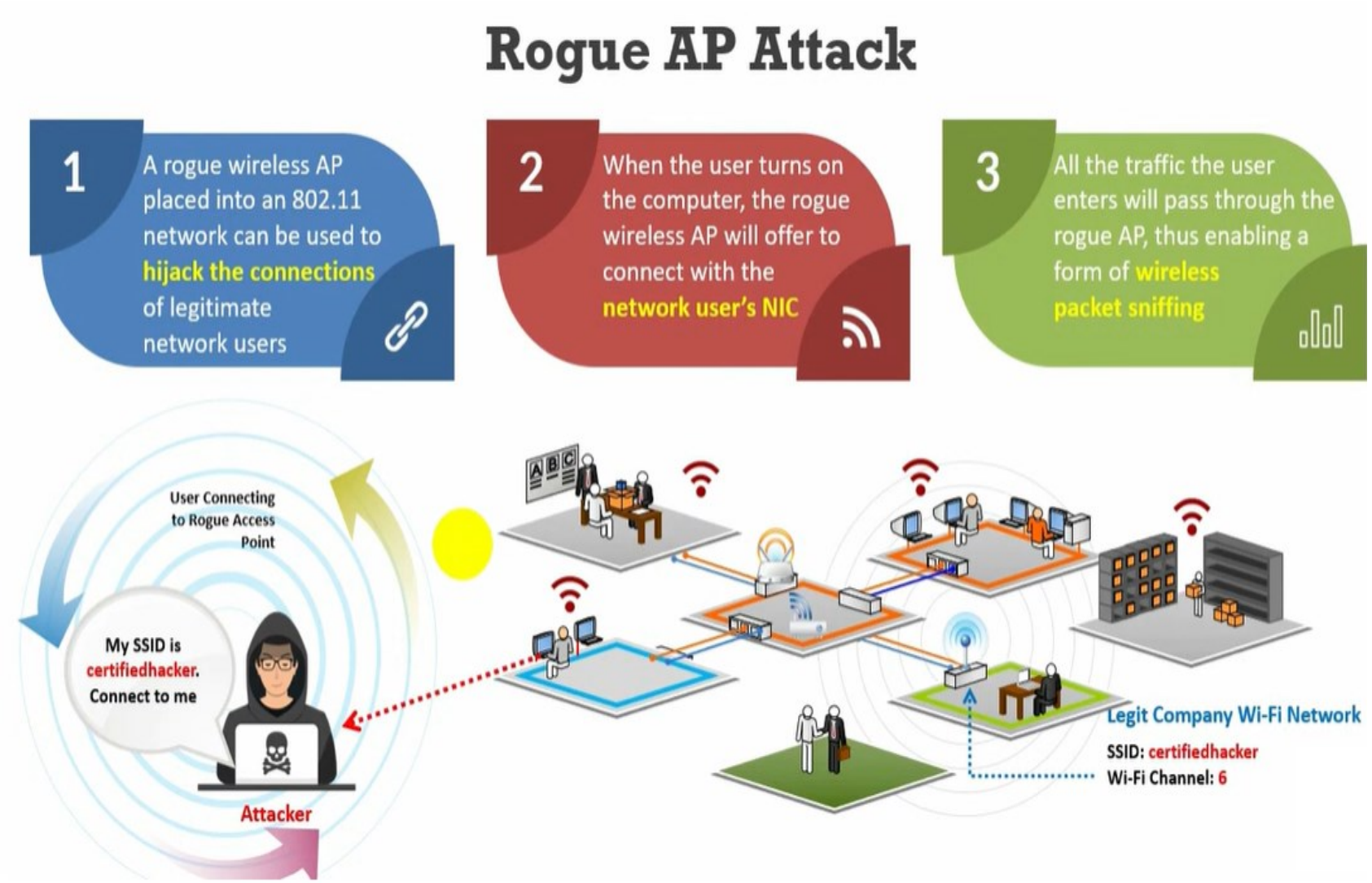
Encryption	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length $1 - 2^{64}$	192-bits	ECDH and ECDSA	BIP-GMAC-256

- **Wireless Attacks Technology**

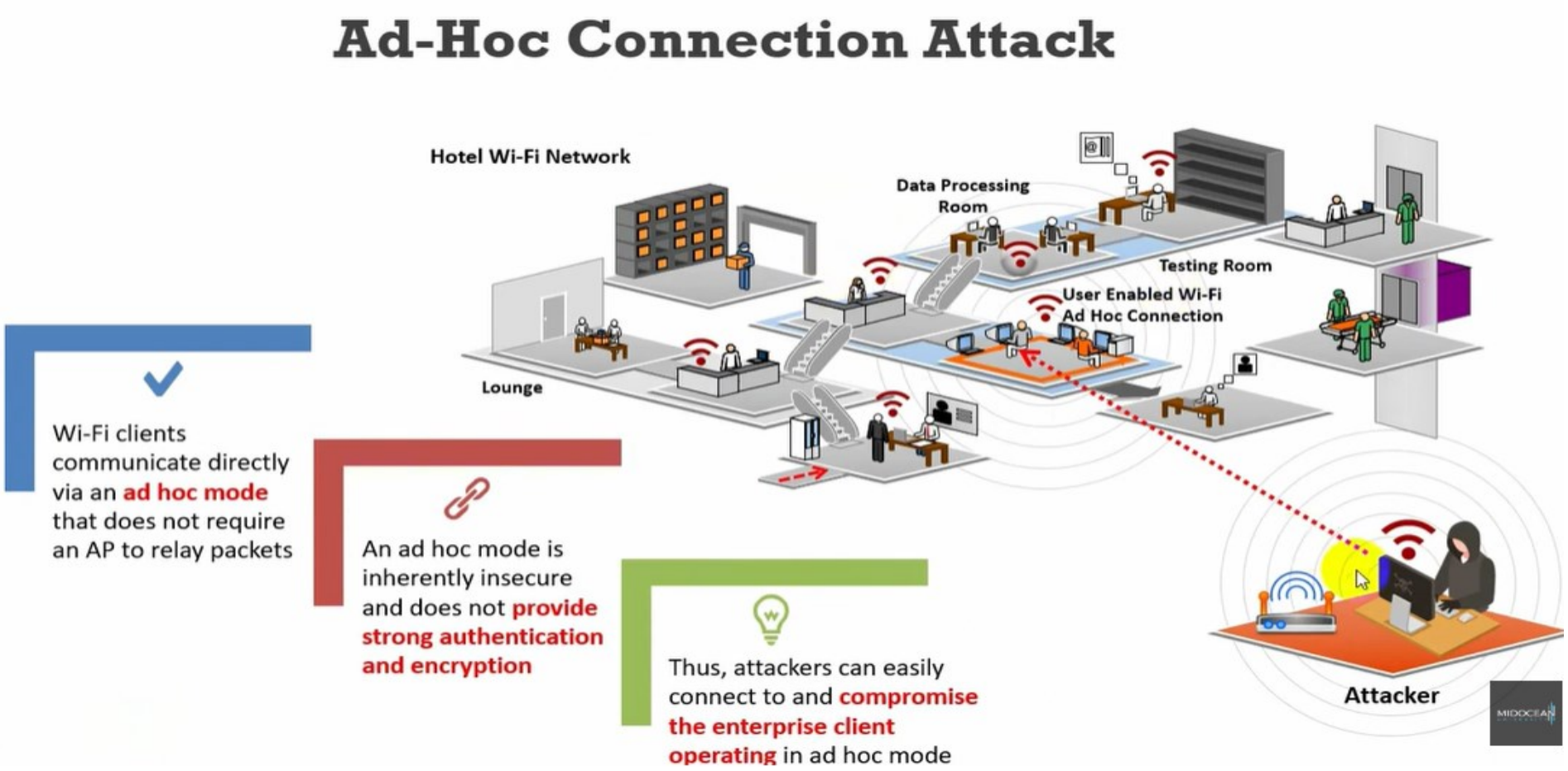
1- Rogue Access Point (Rogue AP) Attack
2- Ad-Hoc Connection Attack
3- Honeypot AP Attack
And others

Wireless Attacks Technology : Rogue AP Attack

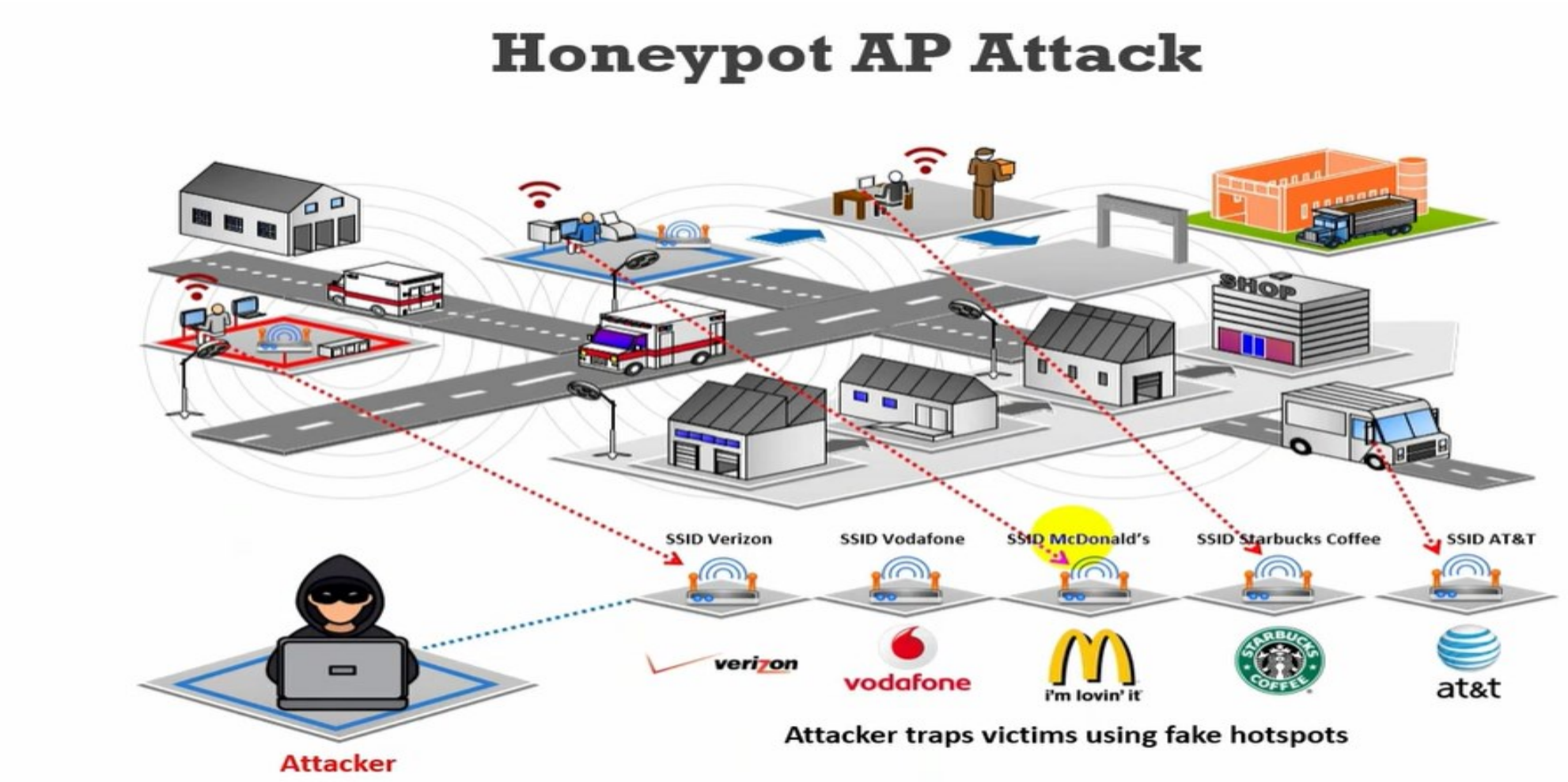
- a rogue access point is an unauthorized access point connected to a secure wireless network. It can be installed by someone within the organization, like an employee, without malicious intent, or by an attacker seeking unauthorized access to the network.



Ad-Hoc Connection Attack



Honeypot AP Attack



Wireless Hacking Methodology

- The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources
- 1-Wi-Fi Discovery
- 2-GPS Mapping
- 3-Wireless Traffic Analysis
- 4-Launch Wireless Attacks
- 5-Crack Wi-Fi Encryption
- 6-Compromise the Wi-Fi Network

Wi-Fi Discovery Tools

Wi-Fi Discovery Tools

Thank You