WI-FI SECURITY AND ENCRYPTION

OVERVIEW

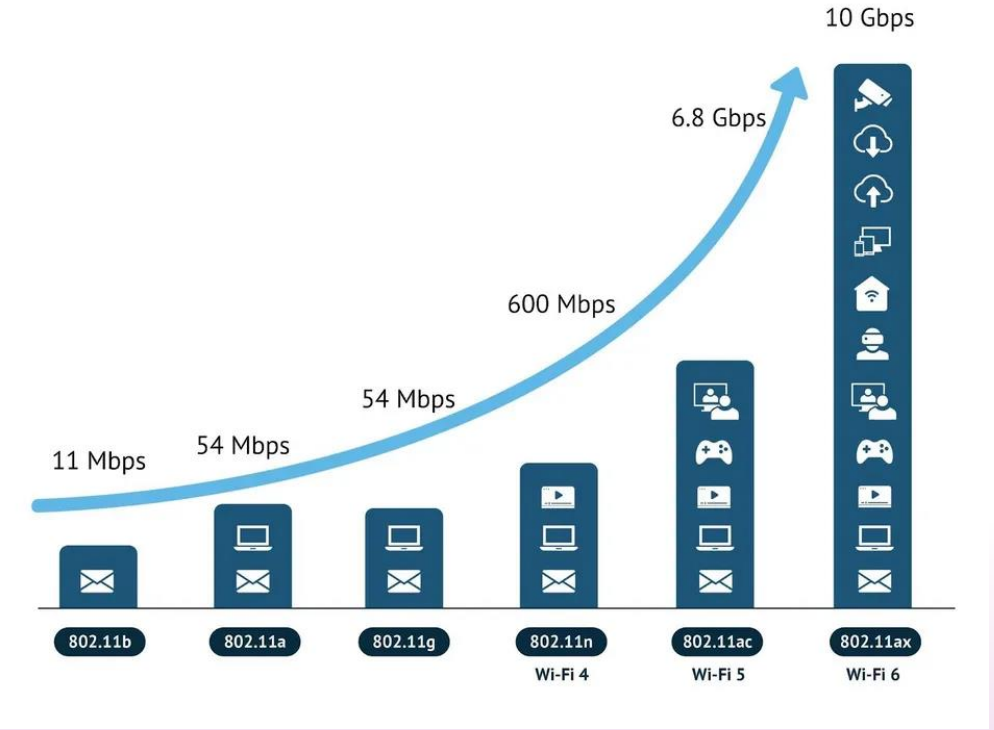
- Evolution of 802.11
- 802.11 Modes
- Authentication
- Encryption Algorithms
- Other Ways to Protect

IEEE 802.11 - WI-FI

- Radio Access Technology that was released in 1997 and operated in the 2.4GHz portion of the electromagnetic spectrum. Later made use of the 5 GHz radio bands.
- Initial standard was not widely adopted due to interoperability issues.
- Subsequent releases/updates have seen continually evolving technology, making more efficient use of the spectrum, adding capabilities and further securing radio communications will boasting ever faster speeds.

802.11 EVOLUTION

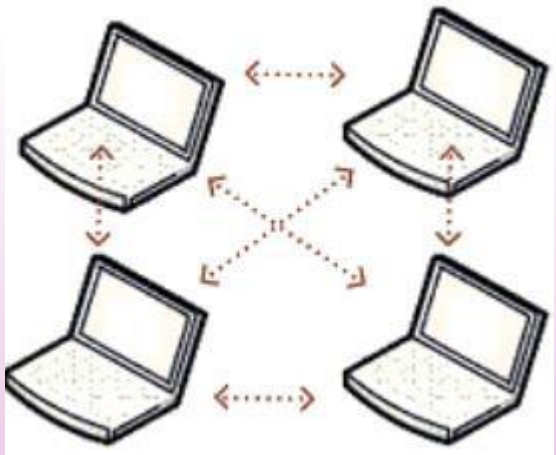
- 802.11a - 1999
- 802.11b - 1999
- 802.11g - 2003
- 802.11n – 2009 – Wi-Fi 4
- 802.11ac – 2013 – Wi-Fi 5
- 802.11ax – 2019 – Wi-Fi 6
- 802.11be – 2024 (expected) – Wi-Fi 7
  - Standard for max throughput will be 46.1 Gbps



BASIC 802.11 ARCHITECTURE

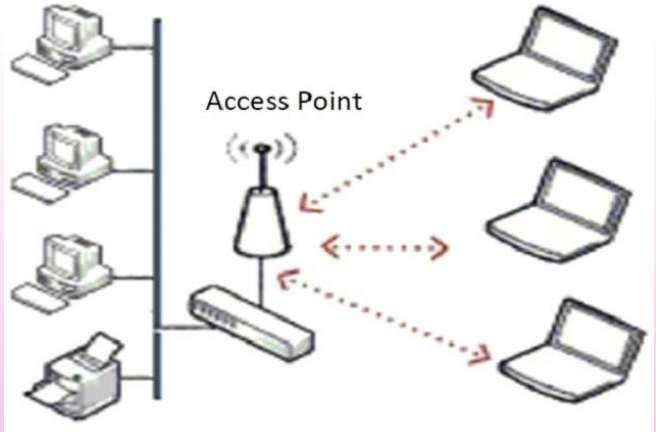
Ad-Hoc Mode

Communication between two end stations (STA) without the use of an access point (AP)



Infrastructure Mode

Stations (STA) communicate across a network through an associated access point

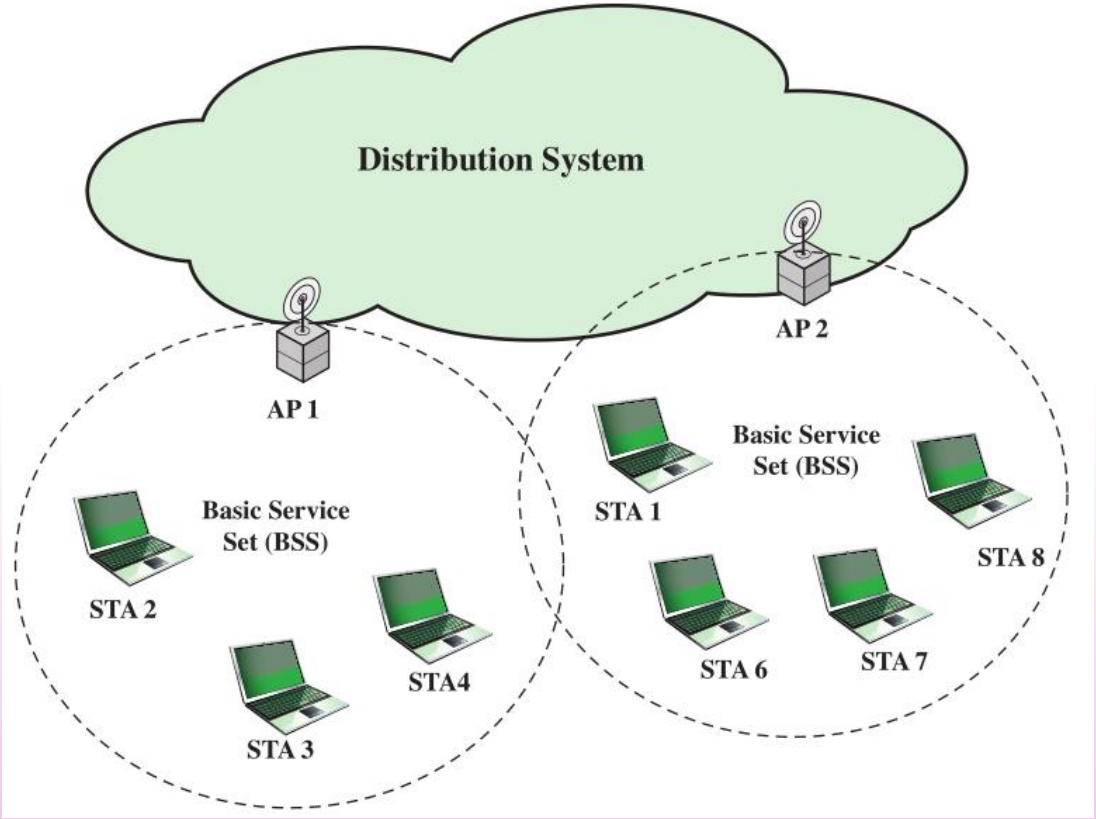


BASIC SERVICE SET (BSS)

- Encompasses all stations and access point that are part of a network. This usually only includes a single access point.
- The access point facilitates all internal/external network communications
- Devices can easily communicate with each other without any problems or extra configuration.
- This is the typical home/office setup for most households.

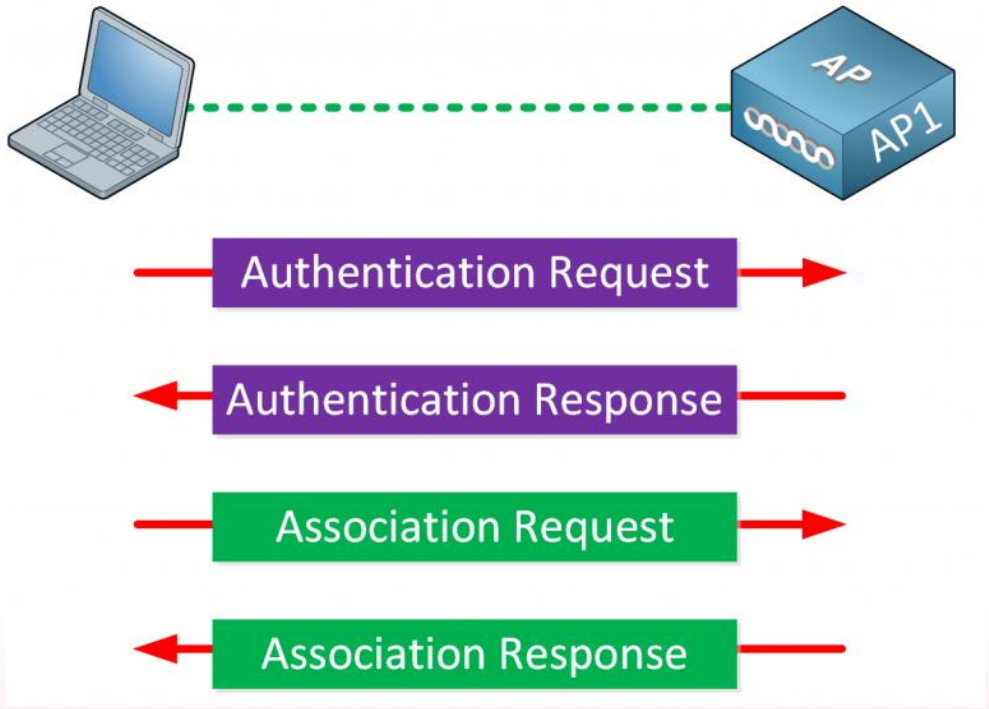
EXTENDED SERVICE SET (ESS)

- ESS: two or more BSSs
- BSSs connected via APs that function as a bridge
- This setup can be found in more advanced home/office setups and are typically seen across larger public/corporate areas such as malls.



AUTHENTICATION

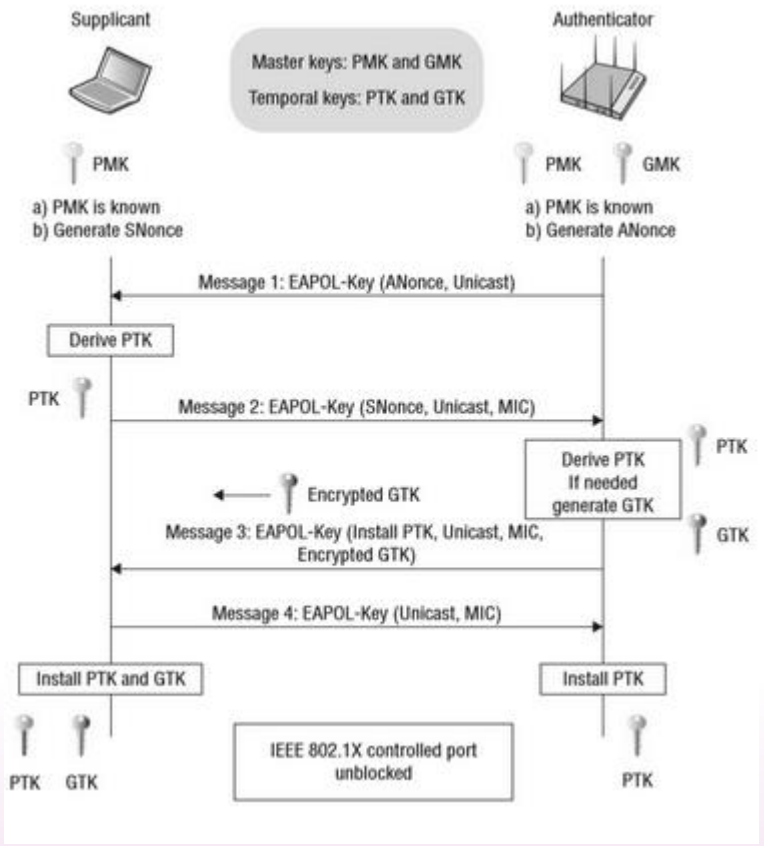
Open authentication is a good way to understand the basics of any of the authentication processes, each of which will involve an Authentication Request and Response and an Association Request and Response. As more security is implemented there is subsequent communication with other devices, but the premise remains the same.



8728	802.11	Management frame	d0:c5:f3:a9:16:c5	Authentication	9c:5d:12:5e:6c:66	Authentication, SN=2002, FN=0, Flags=.....
8730	802.11	Management frame	9c:5d:12:5e:6c:66	Authentication	d0:c5:f3:a9:16:c5	Authentication, SN=1451, FN=0, Flags=.....
8749	802.11	Management frame	d0:c5:f3:a9:16:c5	Association Request	9c:5d:12:5e:6c:66	Association Request, SN=2003, FN=0, Flags=..
8755	802.11	Management frame	9c:5d:12:5e:6c:66	Association Response	d0:c5:f3:a9:16:c5	Association Response, SN=1452, FN=0, Flags=.

4-WAY HANDSHAKE

Exchange of four messages between an access point and client device that generates encryption keys for subsequent communications.



904 EAPOL	Data frame	9c:5d:12:5e:6c:66	QoS Data	d0:c5:f3:a9:16:c5	Key (Message 1 of 4)
906 EAPOL	Data frame	d0:c5:f3:a9:16:c5	QoS Data	9c:5d:12:5e:6c:66	Key (Message 2 of 4)
908 EAPOL	Data frame	9c:5d:12:5e:6c:66	QoS Data	d0:c5:f3:a9:16:c5	Key (Message 3 of 4)
910 EAPOL	Data frame	d0:c5:f3:a9:16:c5	QoS Data	9c:5d:12:5e:6c:66	Key (Message 4 of 4)

WIRED EQUIVALENT PRIVACY - WEP

- First form of security for Wi-Fi with the objective of achieving security levels comparable to that of a wired network.
- While the encryption algorithm that was employed by WEP, a pseudorandom number generation algorithm called RC4 or Ron's Code 4, in and of itself was robust and is still utilized in a number of applications, the implementation of the algorithm led to serious vulnerabilities with the protocol.
- This protocol was retired in 2004, but can still be seen in use throughout the world with outdated infrastructure and devices.

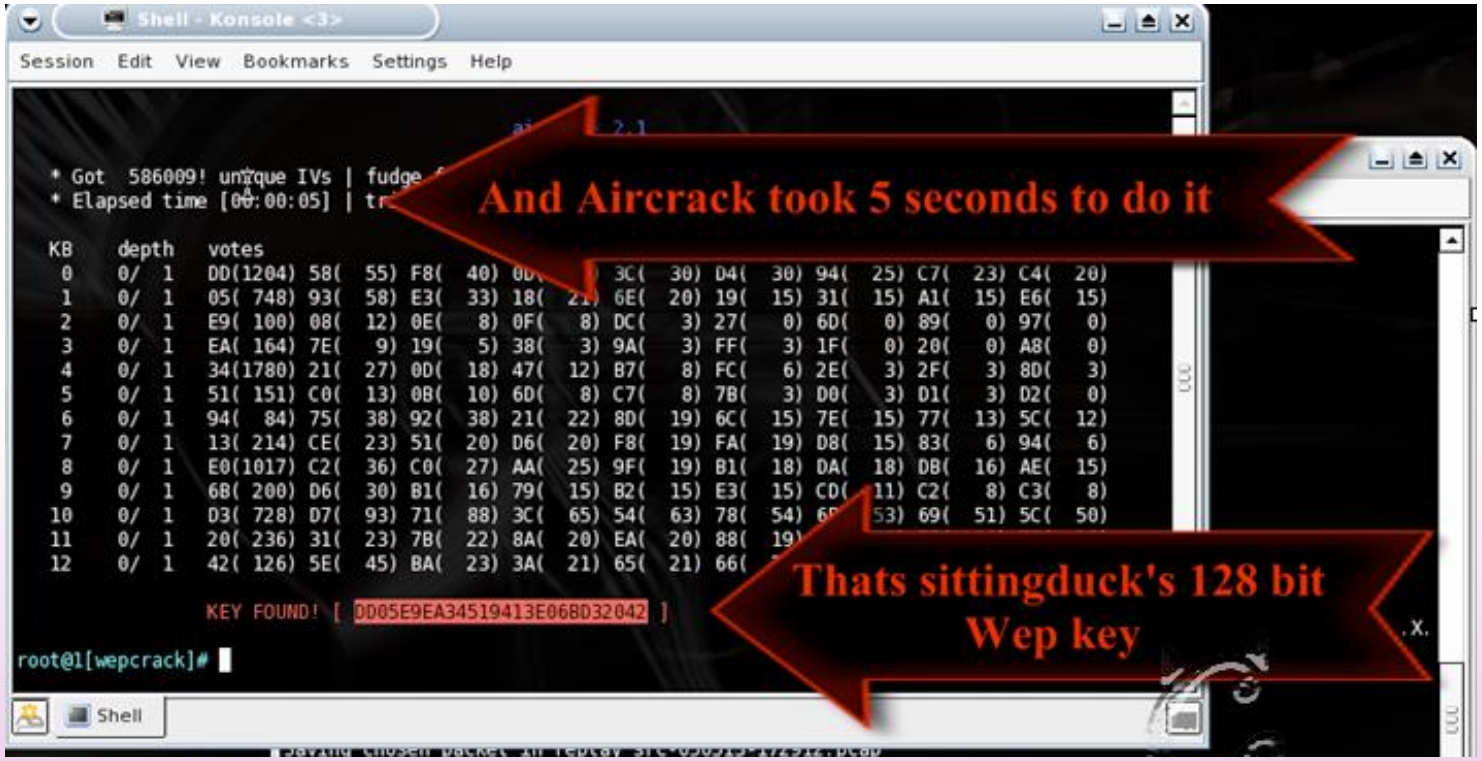
WEP FLAWS AND VULNERABILITIES

- IVs (initialization vectors)
  - A small number of IVs being reused presents a vulnerability.
  - Plaintext appended to the key to avoid repetition.
- Weak keys:
  - It allows an attacker to discover the default key being used by the Access Point and client stations
  - Attacker is able to decrypt all messages being sent over the encrypted channel.

WEP - ATTACKS

- WEP encrypted networks can be cracked in a short amount of time with very little hardware and opensource software.
- Very little hardware and opensource software is required (Linux bootable CD + laptop + wireless card)
- A key can be cracked by collecting enough IVs either passively or actively.
- By injecting packets or deauthing a user from the access point, IVs quicker can be generated quicker.

WEP CRACKING IN LINUX



WPA - WI-FI PROTECTED ACCESS

- Initially released in 2003
- Replacement of security flaws of WEP
  - Use the RC4 algorithm in a proper way and provide fast transfer of the data before someone can decrypt the data.
- Improved data encryption with strong user authentication
- Shared secret key is minimized due to attacks related to static key,

WPA2 - WI-FI PROTECTED ACCESS 2

- Initially released in 2004
- Improved on WPA successes while addressing security concerns.
- Available in both Personal & Enterprise versions
- The primary enhancement over WPA is the use of the AES (Advanced Encryption Standard) algorithm
- The encryption in WPA2 is done by utilizing either AES or TKIP
- Personal mode
  - Uses a PSK (Pre-shared key)
  - Does not require a separate authentication of users
- Enterprise mode
  - Users authenticated by using the EAP protocol

KRACK – KEY REINSTALLATION ATTACK

- Discovered by Mathy Vanhoef of imec-DistriNet, KU Leuven in 2017.
- Works against all modern Wi-Fi networks utilizing WPA/WPA2
- In a key reinstallation attack, the adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial value. Essentially, to guarantee security, a key should only be installed and used once.

WPA3 – WI-FI PROTECTED ACCESS 3

- Released in 2018
- Updates
  - Simultaneous Authentication of Equals protocol
  - Individualized data encryption
  - Stronger brute force attack protection
  - Bigger session keys (Up to 192-bit)
- Not automatically supported. Devices and Infrastructure must support be able to be updated to support.

DRAGONBLOOD VULNERABILITIES

- Quickly discovered after the release of WPA3 in 2019. A few initial vectors discovered with more that continued to follow.
- The Dragonblood vulnerabilities include a few different attack vectors such as a DoS vulnerability, two side-channel information leaks, and two downgrade vulnerabilities
- The DoS vulnerability crashes WPA3 consistent access points.
- The other four take advantage of the flaws in the Dragonfly key exchange, which is used to authenticate users to access points and routers utilizing WPA3

ENCRYPTION TAKEAWAYS

- Everything is safe until it no longer isn’t.
- Just because a new standard with new security is released, doesn’t mean that there aren’t security issues. Each of the security protocols has been breached in very short order.
- Bad actors will continue to probe until they find a way.

SSID – SERVICE SET IDENTIFICATION

- Identifies a particular wireless network
- A client must set the same SSID as the one in that particular AP Point to join the network
- Without SSID, the client won't be able to select and join a wireless network
- Hiding SSID is not a security measure because the wireless network in this case is not invisible
- It can be defeated by intruders by sniffing it from any probe signal containing it.

SECURING WIRELESS NETWORKS

- Encryption
  - Latest security protocols
  - Keep devices updated
- Signal hiding
  - Turn off SSID name broadcasting,
  - Reduce signal strengths (place away from windows and external walls
  - Directional antennas
- Change defaults
  - Change default identifier on router
  - Change router’s preset password

SECURING WIRELESS NETWORKS

- Apply MAC-filtering
  - Disallow unauthorized access to the AP
- Use and enable anti-virus, anti-spyware, firewall
- Require authentication for any access including for devices wishing to attach themselves to the AP

REFERENCES

- *4-way handshake*. WiFi. (2022, February 5). Retrieved March 25, 2023, from https://www.wifi-professionals.com/2019/01/4-way-handshake
- *802.11b security mechanisms*. Wireless Computing. (n.d.). Retrieved March 25, 2023, from https://cs.stanford.edu/people/eroberts/courses/soco/projects/2003-04/wireless-computing/sec_80211.shtml
- *Basic security measures for IEEE 802.11 wireless networks - scielo*. (n.d.). Retrieved March 25, 2023, from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-56092008000200012
- *The evolution of Wi-Fi Networks: From IEEE 802.11 to Wi-Fi 6e*. Wevolver. (n.d.). Retrieved March 25, 2023, from https://www.wevolver.com/article/the-evolution-of-wi-fi-networks-from-ieee-80211-to-wi-fi-6e
- *Key reinstallation attacks*. KRACK Attacks: Breaking WPA2. (n.d.). Retrieved March 25, 2023, from https://www.krackattacks.com/
- *Protecting Wireless Networks*. Kaspersky. (2021, January 13). Retrieved March 25, 2023, from https://usa.kaspersky.com/resource-center/preemptive-safety/protecting-wireless-networks
- *Securing Wireless Networks: CISA*. Cybersecurity and Infrastructure Security Agency CISA. (2023, March 24). Retrieved March 25, 2023, from https://www.cisa.gov/news-events/news/securing-wireless-networks
- *WPA3 WIFI standard affected by Dragonblood vulnerabilities*. Binary Defense. (2019, April 11). Retrieved March 25, 2023, from https://www.binarydefense.com/threat_watch/wpa3-wifi-standard-affected-by-dragonblood-vulnerabilities/
- *WPA3™ specification - wi-fi alliance*. (n.d.). Retrieved March 25, 2023, from https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v1.0.pdf