APNIC

Wi-Fi Security

WEBINAR COURSE

Overview

- Introduction to Wi-Fi
- What is 802.11 protocol?
- Wireless security standards
- Security concerns and exploits
- Wi-Fi security tips and practices

What is Wi-Fi?

- Wi-Fi is a type of wireless communications technology for local area networks

- Provides freedom of mobility
  - Mostly for laptop and mobiles
  - Now also used with IoT devices

Wi-Fi in the enterprise

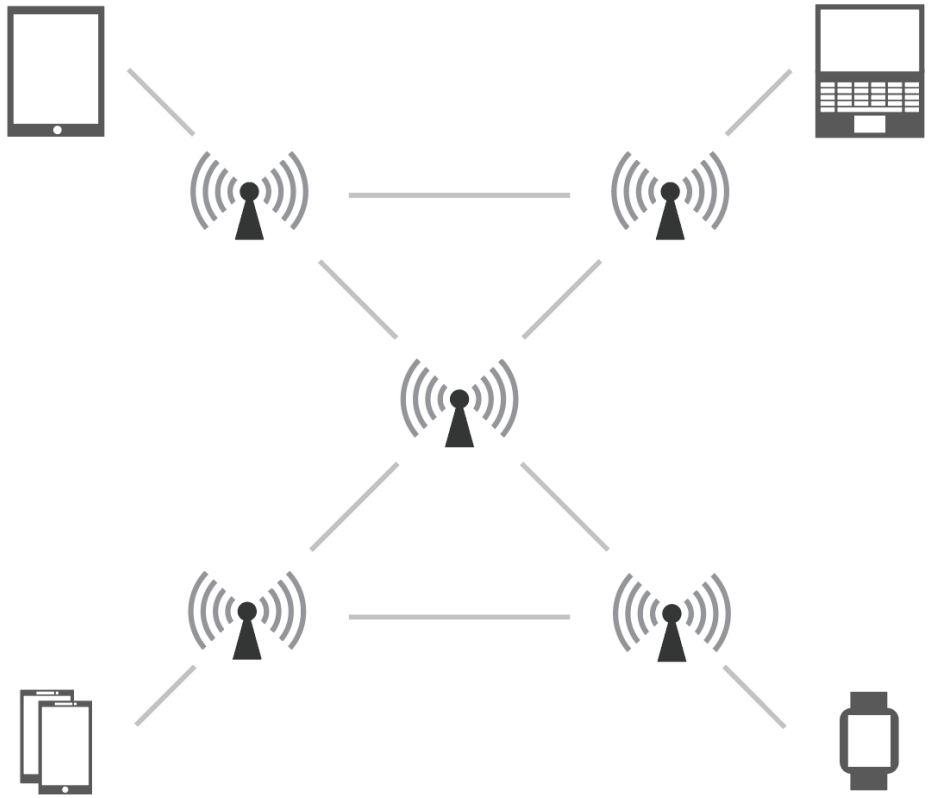
Typical components:

- Wireless access points (WAPs)
- Centralized controller

Topology:

WAPs are generally connected to the LAN via Gigabit ports. A central wireless controller configures and manages all the deployed APs.

To authenticate, users can either use shared password or an authentication server.



Wi-Fi @ home

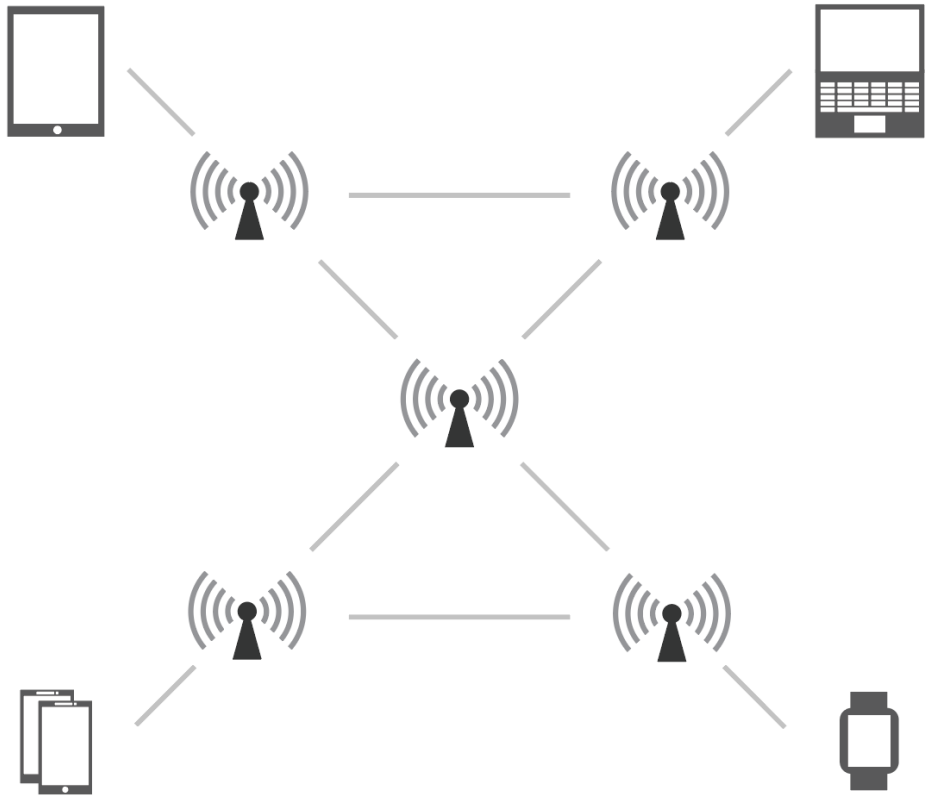
Typical components:

- Wireless router
- Wi-Fi range extenders

Topology:

A wireless router connects to the Internet provider. Wi-Fi range extenders can be used to extend signal throughout the space, usually by creating a wireless mesh network.

To authenticate, users generally use shared password.



What is 802.11 protocol?

IEEE 802.11 is the standard for wireless local area networks (WLAN)

IEEE 802.11 Protocol	Common Name	Frequency (GHz)	Theoretical Speed (Max)	Release Date
802.11b	(Wi-Fi 1)	2.4	11 Mbps	Sep 1999
802.11a	(Wi-Fi 2)	5	54 Mbps	Sep 1999
802.11g	(Wi-Fi 3)	2.4	54 Mbps	Jun 2003
802.11n	Wi-Fi 4	2.4 / 5	150 Mbps	Oct 2009
802.11ac	Wi-Fi 5	5	6.9 Gbps	Dec 2013
802.11ax	Wi-Fi 6	2.4 / 5 / 6	9.6 Gbps	Sep 2019

Most current devices

New standard

Scanning for Wi-Fi

An AP sends out beacon frames, containing its SSID.

Network Name	Vendor	Signal	Channel	Channel Width	Band	Mode	Generation	Max Rate	Security
	Technicolor	-91 dBm	11	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	216.7 Mbps	
	Netgear Inc.	-90 dBm	13	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	173.4 Mbps	WPA2 (PSK)
	Huawei Technologies	-77 dBm	132	80 MHz	5 GHz	a/n/ac	Wi-Fi 5	1300 Mbps	WPA/WPA2 (PSK)
	TP-Link Technologies	-93 dBm	1	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA/WPA2 (PSK)
	TP-Link Technologies	-61 dBm	10	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA2 (PSK)
	TP-Link Technologies	-57 dBm	9	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA2 (PSK)
	Sagemcom Broadband	-88 dBm	1	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA2 (PSK)
	Netgear Inc.	-86 dBm	4	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA2 (PSK)
	TP-Link Technologies	-74 dBm	157	80 MHz	5 GHz	a/n/ac	Wi-Fi 5	1300 Mbps	WPA2 (PSK)
	Netgear Inc.	-89 dBm	8	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA2 (PSK)
	Netgear Inc.	-87 dBm	4	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA2 (PSK)
	Arcadyan Technology Corp.	-87 dBm	11	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	216.7 Mbps	WPA2 (PSK)
	TP-Link Technologies	-89 dBm	9	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA2 (PSK)
	Technicolor	-85 dBm	13	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	216.7 Mbps	
	TP-Link Technologies	-73 dBm	7	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA2 (PSK)
	Huawei Technologies	-61 dBm	2	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA/WPA2 (PSK)
	Sagemcom Broadband	-89 dBm	6	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA2 (PSK)
	TP-Link Technologies	-68 dBm	36	80 MHz	5 GHz	a/n/ac	Wi-Fi 5	1300 Mbps	WPA2 (PSK)
	Google Inc.	-62 dBm	1, 2	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	72.2 Mbps	
	NetComm Wireless	**-53 dBm**	**1, 157**	**20, 80 MHz**	**2.4, 5 GHz**	**a/b/g/n/ac**	**Wi-Fi 4, 5**	**144.4, 1300 M...**	**WPA2 (PSK)**
	NetComm Wireless	-54 dBm	1	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA2 (PSK)
	NetComm Wireless	**-53 dBm**	**157**	**80 MHz**	**5 GHz**	**a/n/ac**	**Wi-Fi 5**	**1300 Mbps**	**WPA2 (PSK)**

Scanning for Wi-Fi

Network Name	Vendor	BSSID	Device Name	Signal	Channel	Channel Width	Band	Mode	Generation	Max Rate	Secu
	Huawei Technologies			-91 dBm	10	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA
	Huawei Technologies			-91 dBm	9	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA
	Cisco Systems Inc.			**-42 dBm**	**1, 6, 11, 40, 48,...**	**20, 40 MHz**	**2.4, 5 GHz**	**a/g/n/ac/ax**	**Wi-Fi 6**	**573.5, 1147 Mb...**	**WPA**
	Cisco Systems Inc.			-42 dBm	1, 6, 11, 40, 48,...	20, 40 MHz	2.4, 5 GHz	a/g/n/ac/ax	Wi-Fi 6	573.5, 1147 Mbps	WPA
	TP-Link Technologies			-88 dBm	2	40 MHz	2.4 GHz	b/g/n	Wi-Fi 4	300 Mbps	WPA
	Huawei Technologies			-86 dBm	10	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA
	Technicolor		Technicolor DJA0231	-76 dBm	11, 100	20, 80 MHz	2.4, 5 GHz	a/b/g/n/ac	Wi-Fi 4, 5	216.7, 1733.3 M...	WPA
	Cisco Systems Inc.			-42 dBm	1, 6, 11, 40, 48,...	20, 40 MHz	2.4, 5 GHz	a/g/n/ac/ax	Wi-Fi 6	573.5, 1147 Mbps	WPA
	TP-Link Technologies			-87 dBm	4	40 MHz	2.4 GHz	b/g/n	Wi-Fi 4	300 Mbps	
	PePWave			-61 dBm	5, 116	20, 80 MHz	2.4, 5 GHz	a/b/g/n/ac	Wi-Fi 4, 5	144.4, 866.7 Mb...	WPA
	Huawei Technologies			-83 dBm	9	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	144.4 Mbps	WPA
	TP-Link Technologies			-90 dBm	9	40 MHz	2.4 GHz	b/g/n	Wi-Fi 4	300 Mbps	WPA
	TP-Link Technologies		Wireless N Router T...	-89 dBm	6	40 MHz	2.4 GHz	b/g/n	Wi-Fi 4	300 Mbps	WPA
	<Multiple Values>			-39 dBm	1, 11, 40, 52, 64,...	20, 40, 80 MHz	2.4, 5 GHz	a/b/g/n/ac/ax	Wi-Fi 4, 5, 6	72.2, 573.5, 114...	*<Mu*
	TP-Link Technologies		Wireless N Router T...	-78 dBm	1	40 MHz	2.4 GHz	b/g/n	Wi-Fi 4	300 Mbps	WPA
	Cisco Systems Inc.			-42 dBm	1, 6, 11, 40, 48,...	20, 40 MHz	2.4, 5 GHz	a/g/n/ac/ax	Wi-Fi 6	573.5, 1147 Mbps	WPA
	ALFA Inc.			-39 dBm	11	20 MHz	2.4 GHz	b/g/n	Wi-Fi 4	72.2 Mbps	WPA

Wi-Fi 6 Next-Generation

- IEEE 802.11AX protocol

- Features:
  - Increased throughput
  - Enhanced multiplexing for higher efficiency
  - Multi-user MIMO
  - Suitable for dense environments (airports, stadiums, campus)
  - Provides efficiency to support IoT endpoints
  - Introduces WPA3

Wi-Fi Security – Basic Principles

Wi-Fi is a disruptive technology. This also makes it a challenge in terms of security.

The basic security principles still apply:

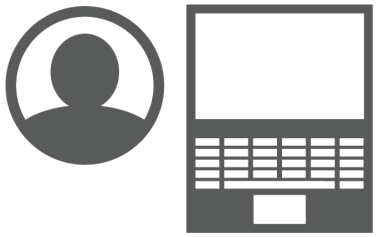
- Confidentiality,
- Integrity,
- Availability

But we need stronger mechanisms to support it.

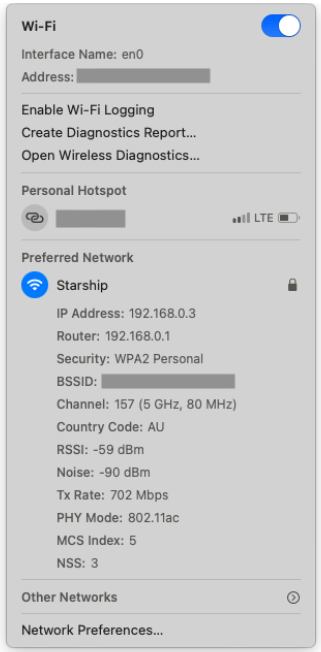
So how do we achieve these in Wi-Fi? Authentication, Encryption, Key Management, Hash functions

How does Wi-Fi work?

Client / STA



User selects the SSID



SSID

Probe Request

Probe Response

AUTHENTICATION & ASSOCIATION

Authentication Request

Authentication Response

Association Request

Association Response

(802.1X AUTHENTICATION)

HANDSHAKE

ENCRYPTED DATA

Access Point

Wireless Authentication

Open System Authentication

- The AP broadcasts its SSID so devices can find and associate with it

Shared Key Authentication

- Using a key or password shared between the client and the AP
- based on the challenge-response protocol

802.1X Authentication

- Forwards the verification process to an authentication server

Wi-Fi security standards

Wi-Fi security standards define the encryption, authentication, integrity protocols used as part of 802.11 standard to protect wifi networks.

STANDARD	WEP	WPA	WPA2	WPA3
YEAR	1997	2003	2006	2019
ENCRYPTION	RC4	TKIP + RC4	AES / CCMP	GCMP-256
AUTHENTICATION	WEP	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
DATA INTEGRITY	CRC-32	MIC	CBC MAC	BIP-GMAC-256
KEY MANAGEMENT	none	4-way handshake	4-way handshake	ECDH key exchange / ECDSA

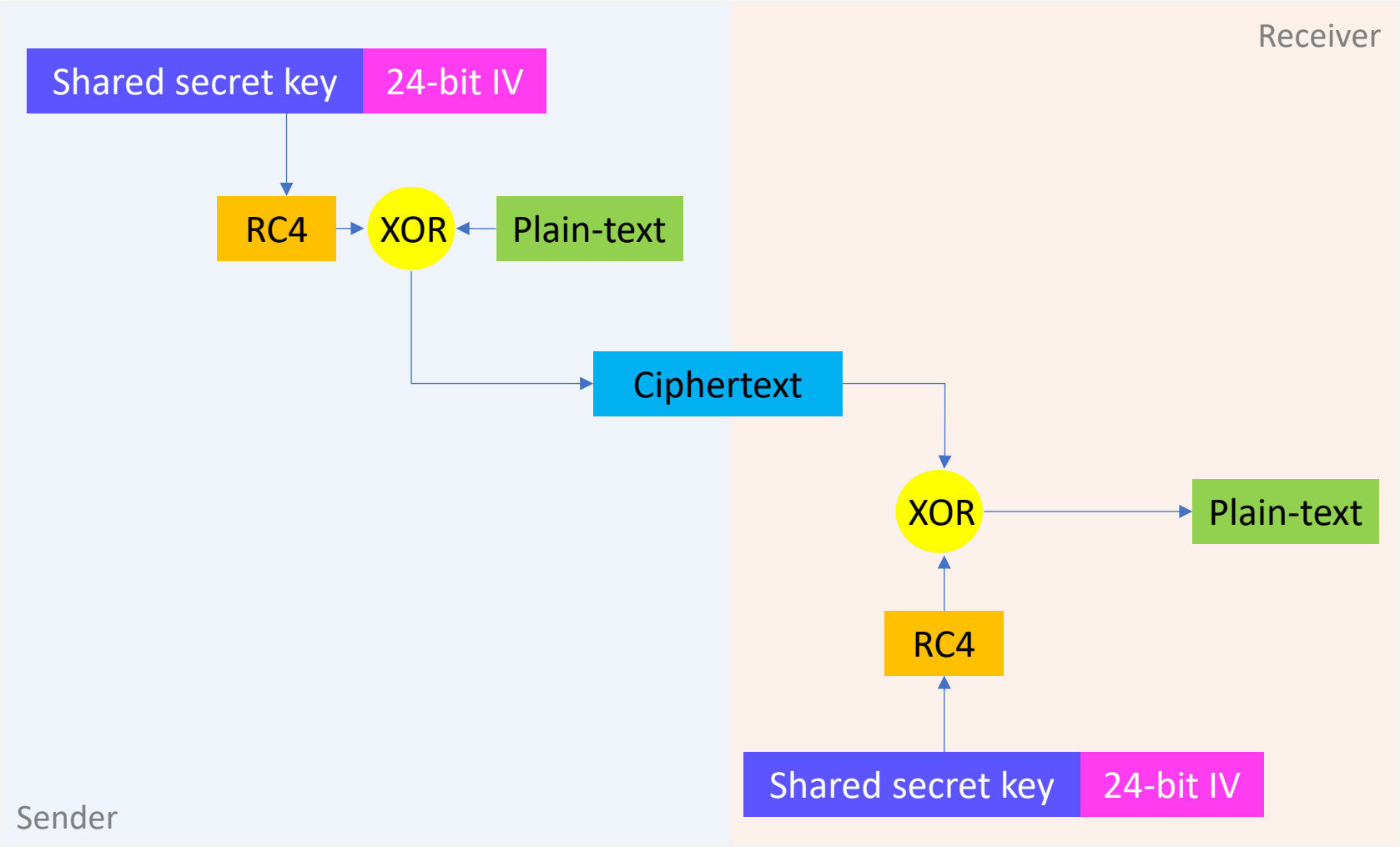
Wi-Fi Security Protocols – WEP

Wired Equivalent Privacy

- The purpose is to provide a level of security equivalent to wired networks
- Used in earlier 802.11 protocols
- Already deprecated

STANDARD	WEP
YEAR	1997
ENCRYPTION	RC4
AUTHENTICATION	WEP
DATA INTEGRITY	CRC-32
KEY MANAGEMENT	none

Why is WEP not secure?



WEP is not secure because:

- The Initialization Vector (IV) is limited to 24-bits and repeats after about 5000 packets
- It uses RC4 Stream Cipher, a simple and fast cipher that has multiple weaknesses.
- The 40-bit encryption key is too short and easy
- The master key is used directly, not just to generate temporary keys.

Wi-Fi Security Protocols – WPA

Wi-Fi Protected Access

- Also known as draft 802.11i
- Temporary security enhancement to WEP
- Uses Temporal Key Integrity Protocol
- Firmware upgrade to WEP-enabled devices

STANDARD	WPA
YEAR	2003
ENCRYPTION	TKIP + RC4
AUTHENTICATION	WPA-PSK WPA-Enterprise
DATA INTEGRITY	MIC
KEY MANAGEMENT	4-way handshake

Wi-Fi Protected Setup (WPS)

- Designed to allow easy setup of devices using:
  - Push-button
  - WPS PIN

- This is not secure!

WPS Pixie (2014)

An offline attack against WPS. The aim is to recover the WPS PIN.

Wi-Fi Security Protocols - WPA2

Wi-Fi Protected Access 2

- Standard 802.11i
- Introduced AES as the new encryption protocol

STANDARD	WPA2
YEAR	2006
ENCRYPTION	AES / CCMP
AUTHENTICATION	WPA2-Personal WPA2-Enterprise
DATA INTEGRITY	CBC MAC
KEY MANAGEMENT	4-way handshake

WPA-PSK and WPA-Enterprise

WPA-PSK or WPA2-Personal

- Uses a pre-shared key / password
- This shared key is used to generate the Pre-Master Key (PMK) that will be used for the handshake
  - PMK = Hash (PSK + SSID)

WPA-Enterprise or WPA2-Enterprise

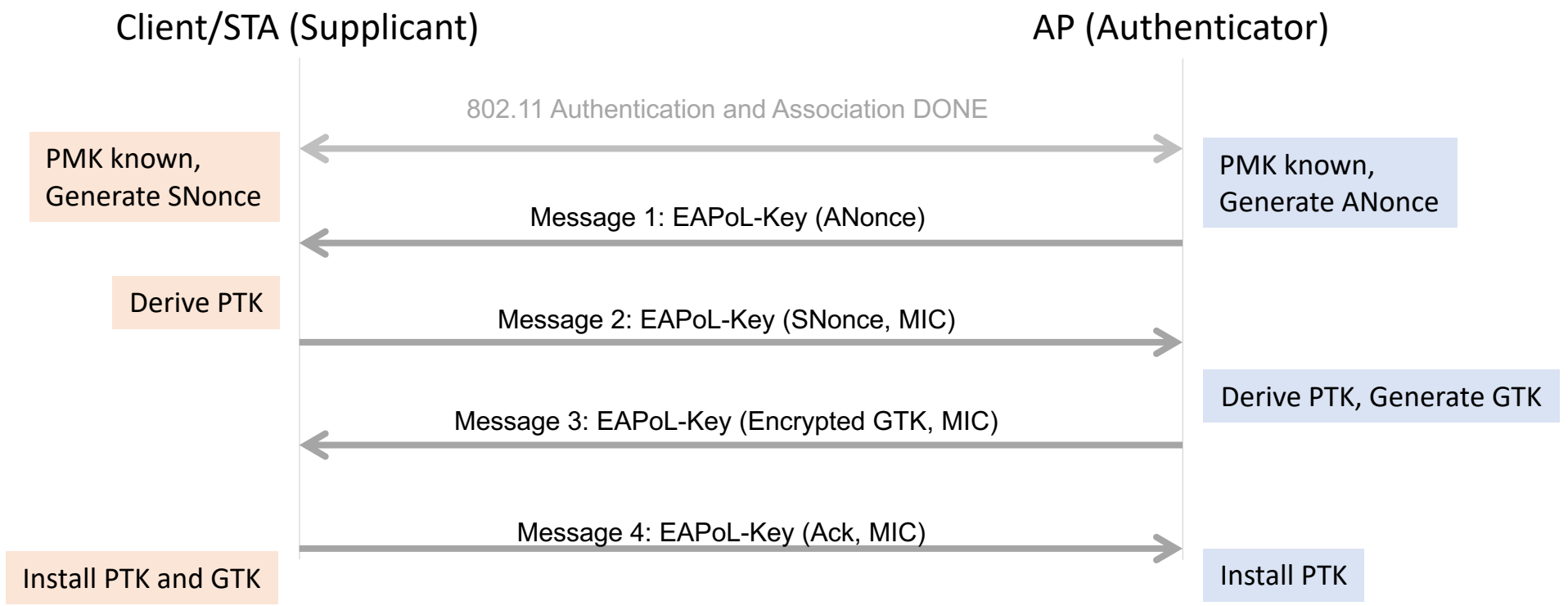
- Uses 802.1X Authentication with a Radius server
- A master session key is generated after this process, which is used to create the PMK => **unique per user**

WPA/WPA2 4-way handshake

Client and AP exchanges 4 EAPoL messages to secure the communication.

Number	Time	Source	Source Port	Destination	Dest Port	Protocol	Info
5	0.011183	Apple_92:51:06		f8:ca:59:0f:8b:c0		EAPOL	Key (Message 2 of 4)
6	0.011230	f8:ca:59:0f:8b:c0		Apple_92:51:06		EAPOL	Key (Message 1 of 4)
7	0.020065	Apple_92:51:06		f8:ca:59:0f:8b:c0		EAPOL	Key (Message 4 of 4)
8	0.020109	f8:ca:59:0f:8b:c0		Apple_92:51:06		EAPOL	Key (Message 3 of 4)

Guide:
Pairwise Master Key (PMK)
Pairwise Transit Key (PTK)
Group Temporal Key (GTK)
Group Master Key (GMK)



WPA/WPA2 4-way handshake

Key		Purpose
Pairwise Master Key	PMK	derived from the master session key (based on PSK or generated from 802.1X/EAP)
Pairwise Transit Key	PTK	derived from PMK, Anonce, Snonce, authenticator address, supplicant address used to encrypt all unicast traffic between the client and AP
Group Master Key	GMK	used in the handshake to generate GTK
Group Temporal Key	GTK	used to encrypt all broadcast and multicast traffic between the client and AP

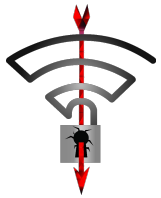
WPA2 Krack Attack

"Key reinstallation attacks"

Capture and modify part of the handshake message,

to trick device to install a blank encryption key

Fast BSS transition (or fast roaming) is vulnerable to this attack



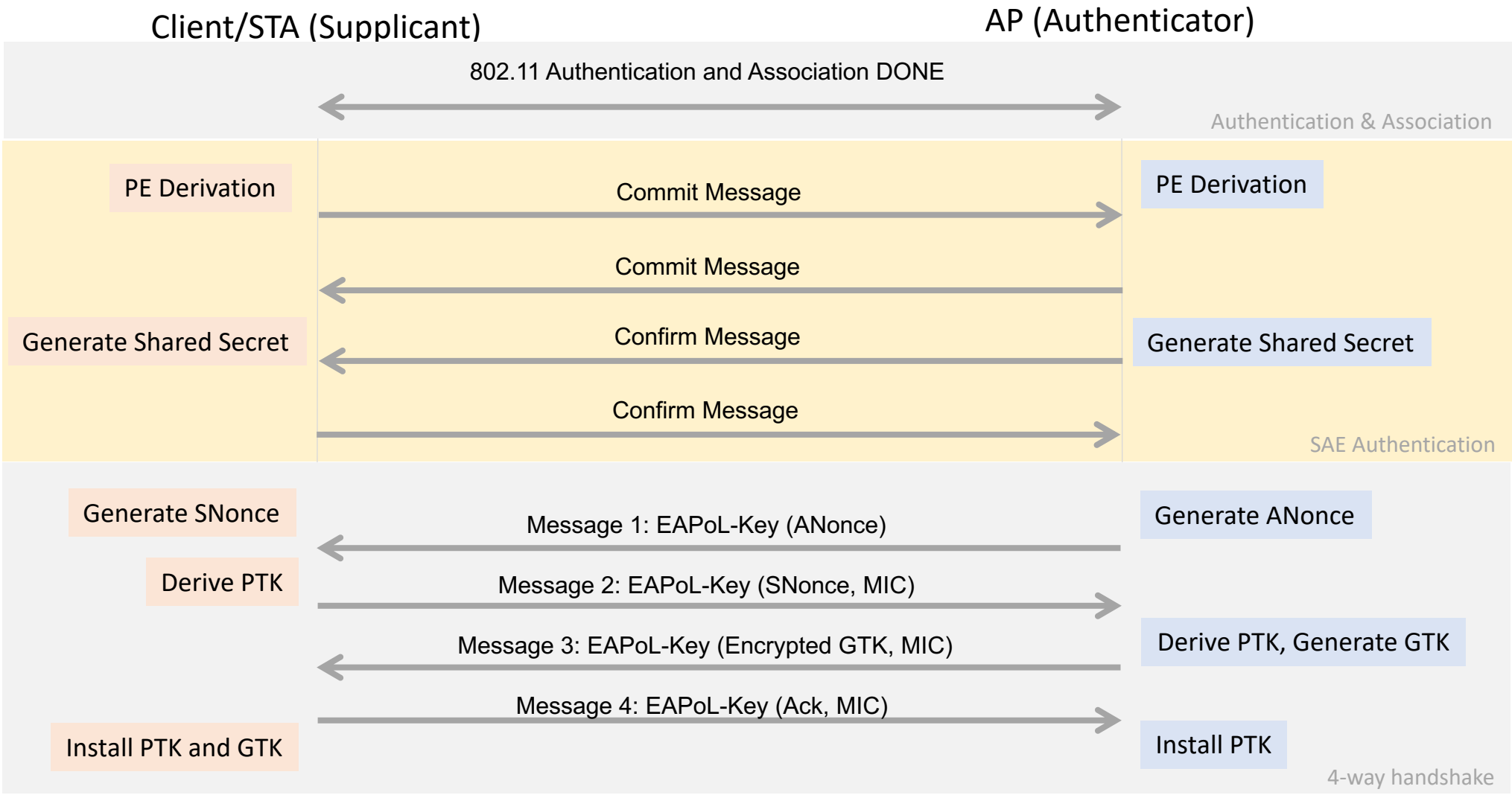
Wi-Fi Security Protocols – WPA3

Wi-Fi Protected Access 3

- Increased protection
  - Brute force protection
  - Public network privacy
  - Stronger encryption (NSA Suite-B 192-bit encryption)
- Management Frame Protection
- Uses the SAE key exchange protocol
  - Provides forward secrecy
  - Resistant to offline decryption attacks
- Also provides Wi-Fi Easy Connect for IoT devices

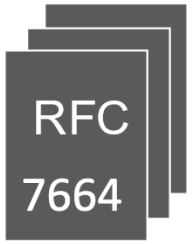
STANDARD	WPA3
YEAR	2018/2019
ENCRYPTION	GCMP-256
AUTHENTICATION	WPA3-Personal WPA3-Enterprise
DATA INTEGRITY	BIP-GMAC-256
KEY MANAGEMENT	ECDH key exchange / ECDSA

WPA3 4-way Handshake



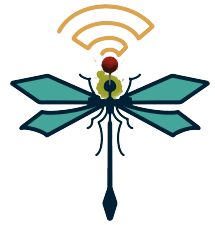
Dragonfly Handshake

- Simultaneous Authentication of Equals (SAE)
- Dragonfly Key Exchange RFC 7664
- Previously used by EPWD protocol



Dragonblood vulnerability

Refer to a couple of vulnerabilities found in WPA3 in 2019.
The first one is a weakness in the use of P-521 elliptic curve which can be downgraded to use a weaker algorithm.
The second bug is related to the EAP-pwd implementation

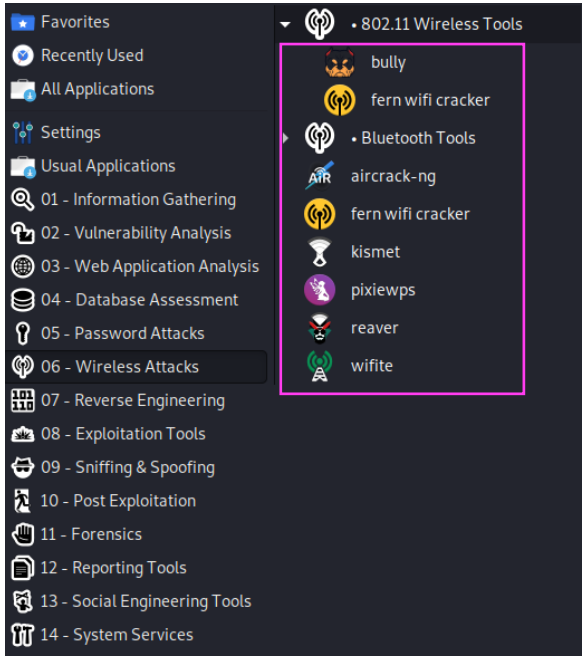


Wi-Fi security concerns and common attacks

- Access to your Wi-Fi is not limited by physical boundaries.
  - Drive-by hacking or Wardriving

- Access to public or untrusted Wi-Fi networks.
  - Could be a fake AP set up by an attacker
    - Rogue access points
  - Could be valid, but you share the network with unknown users (public wifi)
    - Man-in-the-middle attacks (Wireless)
    - Denial of Service (Dos) attacks

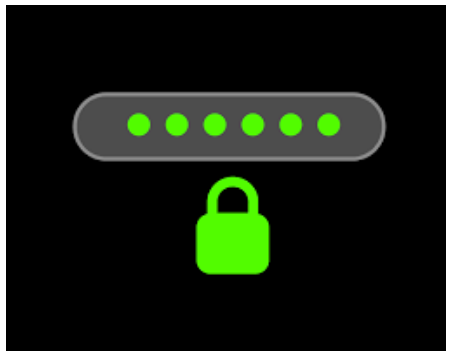
- Open ports and default or insecure settings.



Wi-Fi Security – SSID & Encryption

- Change the default SSID.
  - Hiding SSID may work for some, but not an issue for most bad actors.
  - Using SSID that gives away your info may not be a good idea.
- Choose encryption wisely.
  - Use WPA3 or WPA2/WPA3 (for compatibility).
  - WPA2-PSK is still common.
  - WEP is deprecated, never use it again.
- Disable WPS and UPnP.

Wi-Fi Security – Passwords



- Choose your Wi-Fi password wisely
  - Make it unique.
  - It can be long and “strong” but if it’s in a breached password list, it can still be brute-forced.
- Create an access list
  - MAC address filtering is common feature, but MAC addresses can be spoofed.

Wi-Fi Security – Segmentation

- Isolate networks
  - Separate your data and work machine from IoT devices (sensors, security cameras, DVRs, light bulb, thermostat)
- Create multiple VLANs to allow micro-segmentation of different Wi-Fi network.
- Make use of guest wi-fi, if necessary.
  - Change guest password regularly
  - Disable when not in use

Wi-Fi Security – Management

- Disable remote access.
  - Also check app or cloud-based management.
- Disable open/unused ports to the Internet/WAN link.
  - Check for port forwarding.
- Update firmware, if available.
- Secure the wireless router's web interface.
  - Change admin password (and user if possible).
  - Enable HTTPS, disable HTTP only access

Thank You!

• Any questions?

Please remember to fill out the feedback form
<survey-link>

Slide handouts will be available after completing the survey

• APNIC Helpdesk Chat

APNIC Helpdesk provides assistance to all on matters related to APNIC Services, such as membership and IP address enquiries.

APNIC Helpdesk offers (through prior arrangement) multi-language phone support for the following: Bahasa Indonesia, Bahasa Malaysia, Bengali, Cantonese, English, Filipino (Tagalog), Hindi, Japanese, Malay, Mandarin, Sinhalese, Tamil and Telugu.

You may also find our FAQs helpful with your enquiries.

Contact details

Helpdesk hours 09:00 to 21:00 (UTC +10) Monday - Friday (closed for some public holidays)

Chat APNIC Live Chat Online — Click here to chat

Skype Call — Click here to Skype ID: apnic-helpdesk

Email helpdesk@apnic.net

Phone +61 7 3858 3188

VoIP helpdesk@voip.apnic.net

Fax + 61 7 3858 3199

Service Updates

Service announcement: 10 February 2016

Service disruption: APNIC services were disrupted on Wednesday, 10 February 2016

More announcements

Subscribe to APNIC Service Announcements

Learn more about system maintenance