

B03102082

陳孝思

na

1. Wi-Fi Authentication

1. WPA-Personal 不需要額外架設 802.1X 認證伺服器，且所有想要連線的使用者共用同一組密碼（密碼存在 Wi-Fi 路由器裡）

WPA-Enterprise 需要另外架設認證伺服器，且使用者想連入該網路時必須要登入該網路的認證伺服器取得認證才行

Ref: <https://zh.wikipedia.org/wiki/WPA>

<https://www.tp-link.com/us/FAQ-500.html>

2. csie-5g: WPA2 企業級,



csie: WPA2 企業級



2. Wi-Fi Encryption

1. WEP: stream cipher RC4 (40 bit key 加上 24-bit initialization vector)
WPA: stream cipher RC4 (128 bit key 加上 48-bit initialization vector) 加上 TKIP (Temporal Key Integrity Protocol)
WPA2: CCMP (CTR mode with CBC-MAC Protocol) based on Advanced Encryption Standard (AES)

Ref: https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

2. csie-5g: WPA2 企業級



csie: WPA2 企業級



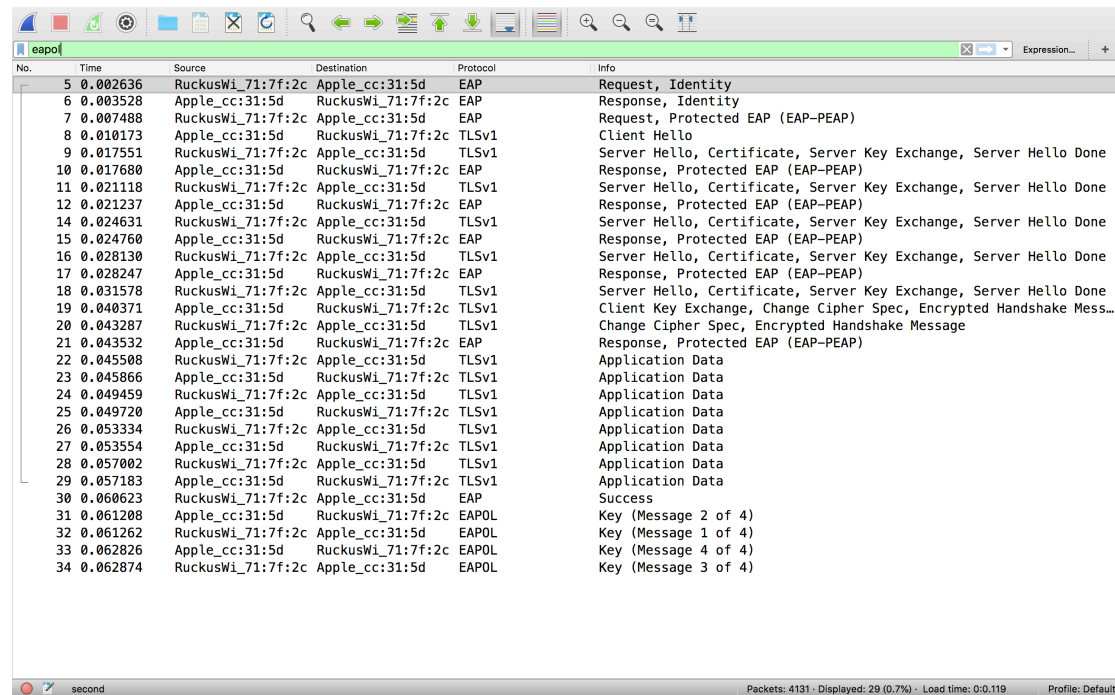
3. WPA3

1. 192-bit 加密
2. 所有 client 與 AP 之間的資料交換都會加密
3. 實作 Simultaneous Authentication of Equals 增加 handshake 安全性

ref: <https://www.welivesecurity.com/2018/02/09/will-wpa3-improve-wifi-security/>
<https://venturebeat.com/2018/05/19/what-is-wpa3-why-does-it-matter-and-when-can-you-expect-it/>

4. Seeing is Believing

3. eapol filtered packages:



No.	Time	Source	Destination	Protocol	Info
5	0.002636	RuckusWi_71:7f:2c	Apple_cc:31:5d	EAP	Request, Identity
6	0.003528	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Identity
7	0.007488	RuckusWi_71:7f:2c	Apple_cc:31:5d	EAP	Request, Protected EAP (EAP-PEAP)
8	0.010173	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Client Hello
9	0.017551	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
10	0.017680	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Protected EAP (EAP-PEAP)
11	0.021118	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
12	0.021237	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Protected EAP (EAP-PEAP)
14	0.024631	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
15	0.024760	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Protected EAP (EAP-PEAP)
16	0.028130	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
17	0.028247	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Protected EAP (EAP-PEAP)
18	0.031578	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
19	0.040371	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess...
20	0.043287	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Change Cipher Spec, Encrypted Handshake Message
21	0.043532	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Protected EAP (EAP-PEAP)
22	0.045508	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Application Data
23	0.045866	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Application Data
24	0.049459	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Application Data
25	0.049720	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Application Data
26	0.053334	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Application Data
27	0.053554	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Application Data
28	0.057002	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Application Data
29	0.057183	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Application Data
30	0.060623	RuckusWi_71:7f:2c	Apple_cc:31:5d	EAP	Success
31	0.061208	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAPOL	Key (Message 2 of 4)
32	0.061262	RuckusWi_71:7f:2c	Apple_cc:31:5d	EAPOL	Key (Message 1 of 4)
33	0.062826	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAPOL	Key (Message 4 of 4)
34	0.062874	RuckusWi_71:7f:2c	Apple_cc:31:5d	EAPOL	Key (Message 3 of 4)

second Packets: 4131 · Displayed: 29 (0.7%) · Load time: 0:0.119 Profile: Default

4. identity info:

► Frame 6: 32 bytes on wire (256 bits), 32 bytes captured (256 bits) on interface 0
► Ethernet II, Src: Apple_cc:31:5d (18:65:90:cc:31:5d), Dst: RuckusWi_71:7f:2c (30:87:d9:71:7f:2c)
► 802.1X Authentication
► Extensible Authentication Protocol

```
0000 30 87 d9 71 7f 2c 18 65 90 cc 31 5d 88 8e 01 00 0..q.,e .l)....  
0010 00 0e 02 00 00 0e 01 62 30 33 31 30 32 30 38 32 .....b 03102082
```

No.: 6 - Time: 0.003528 - Source: Apple_cc:31:5d - Destination: RuckusWi_71:7f:2c - Protocol: EAP - Length: 32 - Info: Response, Identity

Help Close

5.

Wireshark packet capture analysis showing EAPOL (Extensible Authentication Protocol over LAN) frames between RuckusWi_71:7f:2c and Apple_cc:31:5d. The capture shows a sequence of EAPOL frames, including Request, Identity, Response, Identity, Request, Protected EAP (EAP-PEAP), Client Hello, Server Hello, Certificate, Server Key Exchange, Server Hello Done, Response, Protected EAP (EAP-PEAP), and Application Data. The frames are numbered 5 through 34, with timestamps ranging from 0.002636 to 0.062874 seconds. The protocol is EAPOL. The frames are grouped into five categories marked with red brackets and numbers 1 through 5.

No.	Time	Source	Destination	Protocol	Info
5	0.002636	RuckusWi_71:7f:2c	Apple_cc:31:5d	EAP	Request, Identity
6	0.003528	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Identity
7	0.007488	RuckusWi_71:7f:2c	Apple_cc:31:5d	EAP	Request, Protected EAP (EAP-PEAP)
8	0.010173	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Client Hello
9	0.017551	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
10	0.017680	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Protected EAP (EAP-PEAP)
11	0.021118	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
12	0.021237	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Protected EAP (EAP-PEAP)
14	0.024631	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
15	0.024760	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Protected EAP (EAP-PEAP)
16	0.028130	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
17	0.028247	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Protected EAP (EAP-PEAP)
18	0.031578	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
19	0.040371	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess...
20	0.043287	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Change Cipher Spec, Encrypted Handshake Message
21	0.043532	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAP	Response, Protected EAP (EAP-PEAP)
22	0.045508	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Application Data
23	0.045866	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Application Data
24	0.049459	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Application Data
25	0.049720	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Application Data
26	0.053334	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Application Data
27	0.053554	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Application Data
28	0.057002	RuckusWi_71:7f:2c	Apple_cc:31:5d	TLSv1	Application Data
29	0.057183	Apple_cc:31:5d	RuckusWi_71:7f:2c	TLSv1	Application Data
30	0.060623	RuckusWi_71:7f:2c	Apple_cc:31:5d	EAP	Success
31	0.061208	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAPOL	Key (Message 2 of 4)
32	0.061262	RuckusWi_71:7f:2c	Apple_cc:31:5d	EAPOL	Key (Message 1 of 4)
33	0.062826	Apple_cc:31:5d	RuckusWi_71:7f:2c	EAPOL	Key (Message 4 of 4)
34	0.062874	RuckusWi_71:7f:2c	Apple_cc:31:5d	EAPOL	Key (Message 3 of 4)

second Packets: 4131 - Displayed: 29 (0.7%) - Load time: 0:0.119 Profile: Default