NA

Wi-Fi Authentication

1. https://www.speedguide.net/faq/wpa-personal-vs-enterprise-332
   https://www.tp-link.com/us/FAQ-500.html
   https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
   On the WPA-Personal mode, wireless access can't be individually or centrally managed. One password applies to all users. The password is stored on the wireless clients. Therefore, anyone on the computer can connect to the network and also see the password. (ex: temp Wi-Fi in DSA class)
   WPA-Enterprise mode provides the security needed for wireless networks in business environments. It offers individualized and centralized control over access to Wi-Fi network. When users try to connect to the network, they need to login their own passwords. Users never deal with the actual encryption keys. They are securely created and assigned per user session in the background after a user presents their login credentials. This prevents people from getting the network key from computers. (ex: ntu-peap)
2. WPA-Enterprise is used for authentication by csie and csie-5g. Because every student needs to use their own id number as account and login with their workstation password, no one can login with the same password. So it is not WPA-Personal mode, instead, it is the method of WPA-Enterprise method.\
   (my screenshot)

Wi-Fi Encryption

1. https://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2
   https://www.ithome.com.tw/tech/96292

WEP uses the RC4 stream cipher (Rivest Cipher), WPA use RC4 and TKIP (Temporal Key Integrity Protocol), WPA2 uses AES (Advanced Encryption Standards), TKIP and CCMP (Counter Mode with CBC-MAC Protocol).

2. WPA2 (my screenshot)

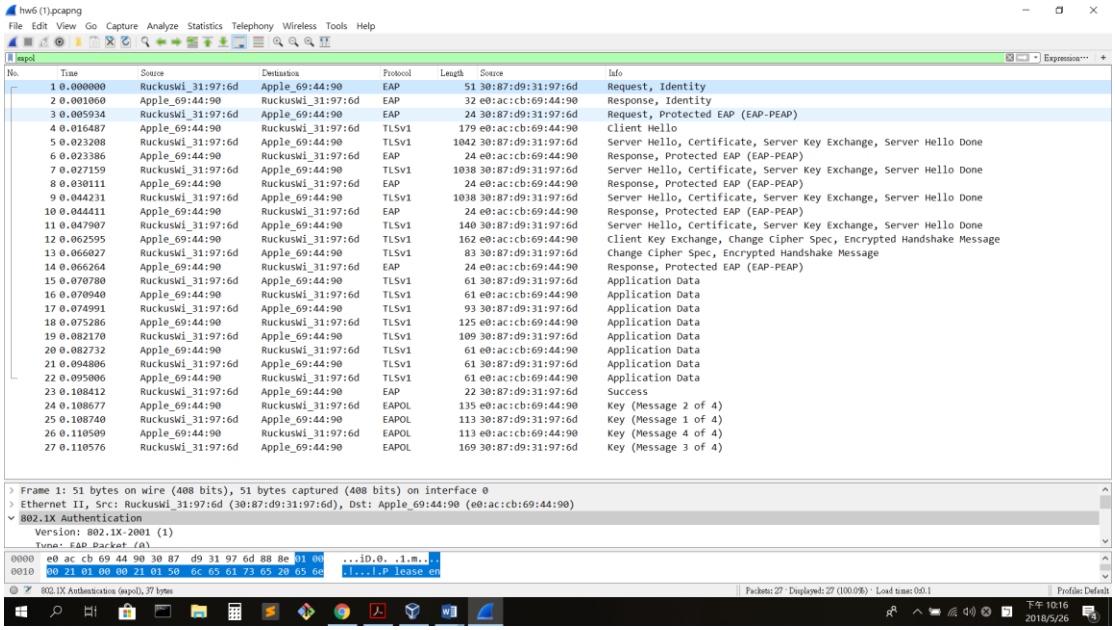
WPA3

http://www.itpro.co.uk/security/30848/what-is-wi-fi-protected-access-3-wpa3
https://venturebeat.com/2018/05/19/what-is-wpa3-why-does-it-matter-and-when-can-you-expect-it/
https://www.digitaltrends.com/computing/what-is-wpa3/

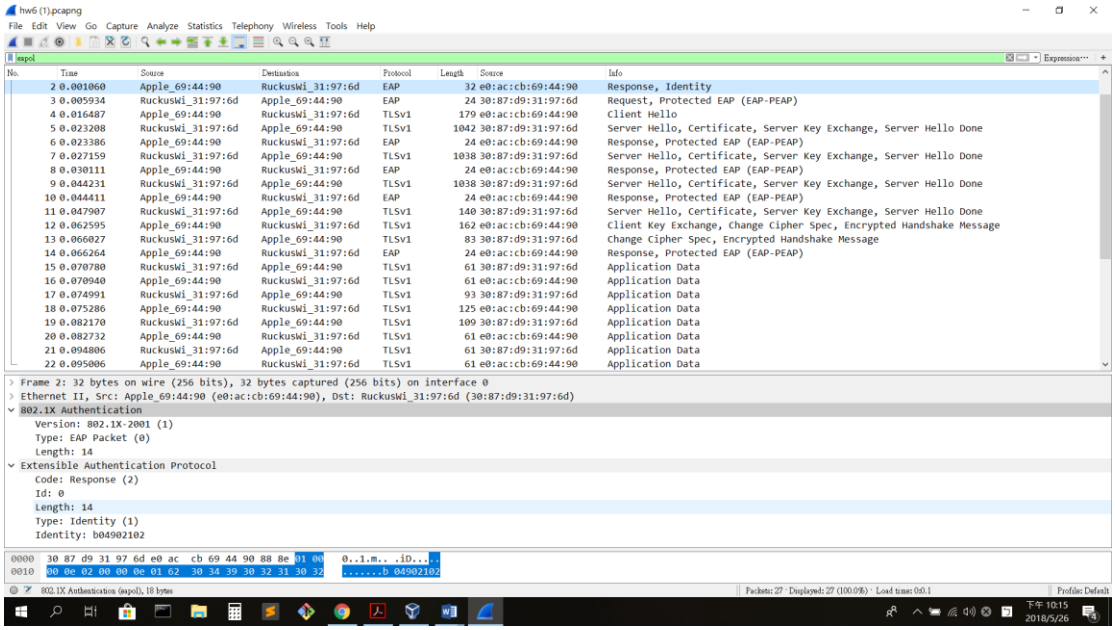
1. WPA3 supports a much stronger encryption algorithm
   With a 192-bit security suite that's aligned with the Commercial National Security Algorithm (CNSA) Suite.
2. It protects against brute force dictionary attack
   WPA3 hardens security at the time when the network key is exchanged between a device and the access point. WPA3 also imposes strict limits on the number of times users can guess a network's password. Even the weak password is less vulnerable to dictionary attack (a brute attack that uses a list of common words, number combinations, and phrases to generate all possible passwords)
3. It secure public Wi-Fi
   WPA3 introduces Opportunistic Wireless Encryption (OWE), individualized data encryption, which encrypts every connection between a device and the router with a unique key. Even if the access point doesn't require a password, your device's data won't be exposed to the wider network.

Seeing is Believing

3.



4.



5.

Stage1: Packet 1~2

Stage2: Packet 3~14

Stage3: Packet 15~22

Stage4: Packet 23

Stage5: Packet 24~27