Abdul Sami Qasim

22i-1725

CY-D

Q1)

WPA2 uses AES encryption with a prestored key and it is vulnerable to offline brute force attacks. WPA3 addresses this by implementing simultaneous authentication of equals, basically replacing PSK with a secure exchange method.

forward secrecy ensures that if a session is compromised, the past communications are safe. WPA3 also limits the number of incorrect login attempts.

Q2)

WEP was an early wifi securing mechanism and it used RC4 for encryption and a short 24-bit initialization vector. These could be reused and it gave attackers enough information to ~~attack~~ crack the WEP key, the fact that WEP's integrity check was weak didnt help either.

WPA improved this by using TKIP (temporal key integrity protocal) which changed the encryption key for each packet, improving overall security.

WPA2 replaced RC4 with AES and it used CCMP for better data integrity checks which helped in securing wifi