Wired Equivalent Privacy, commonly called WEP is 802.11's first hardware form of security where both the WAP and the user are configured with an encryption key of either 64 bits or 128 bits in HEX. So when the user attempts to authenticate, the AP issues a random challenge. The user then returns the challenge, encrypted with the key. The AP decrypts this challenge and if it matches the original the client is authenticated. The problem with WEP is that the key is static, which means with a little time and the right tool a hacker could use reverse-engineering to derive the encryption key. It is important to note that this process does affect the transmission speed.

WPA builds upon WEP, making it more secure by adding extra security algorithms and mechanisms to fight intrusion.
WiFi Protected Access (WPA) is the new security standard adopted by the WiFi Alliance consortium. WiFi compliance ensures interoperability between different manufacturer’s equipment.WPA delivers a level of security way beyond anything that WEP can offer, bridges the gap between WEP and 802.11i networks, and has the advantage that the firmware in older equipment may be upgradeable.

WPA2 is based upon the Institute for Electrical and Electronics Engineers’ (IEEE) 802.11i amendment to the 802.11 standard, which was ratified on July 29, 2004. The primary difference between WPA and WPA2 is that WPA2 uses a more advanced encryption technique called AES (Advanced Encryption Standard), allowing for compliance with FIPS140-2 government security requirements.