

# Encryption of wireless networks

## 1 WEP (Wired Equivalent Privacy)

Encryption algorithm WEP was introduced in 1999 to make wireless networks as secure as wired networks. At the time of creating the standard, the U.S. Government's export restrictions limited strong cryptography, so the first version of WEP (called WEP-40) used 40-bit key and 24-bit initialization vector (IV). Later was created stronger version WEP-104 using 104-bit key and 24-bit IV.

Encryption is done using stream cipher RC4, which input is key concatenated with IV, and the output is XORed with the message.

WEP is no longer secure, there are tools like aircrack-ng, which can crack any WEP network in minutes. Main reason is insufficient size of the IV, which leads in 50 % chance of repeating IV after 5000 packets. Also using RC4 is nowadays insecure.

## 2 WPA (Wi-Fi Protected Access)

Introduced in 2003, WPA was intended to be a temporary replacement for an insecure WEP. Better security is achieved using TKIP (Temporal Key Integrity Protocol), which dynamically generates 128-bit keys for each packet.

## 3 WPA2

WPA2 was released in 2004 as a full replacement for WEP and WPA, since 2006 is compulsory for all Wi-Fi certified devices.

Security is ensured by the protocol CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol), which uses AES in CTR mode (counter mode) for data confidentiality and CBC-MAC for data authenticity and integrity.

## 4 Key distribution schemes

1. WPA-PSK (Pre-shared key) – This scheme is appropriate for home or other small networks. Each user has to use a pre-shared 256-bit key to connect to the network, which is either randomly generated or derived from ASCII string by PBKDF2 function. This removes another flaw in WEP, where ASCII string was directly used as a key, which resulted in keys with very low entropy.
2. WPA-802.1X – An authentication server is used for providing access to the network, designed for enterprise networks.