Wi-Fi security protocols Background

Wi-Fi security protocols use encryption technology to secure networks and protect the data of their clients.  The most common Wi-Fi security protocols today are WEP, WPA, WPA2 and WPA3.

They use cryptographic keys to randomize data to make it undecipherable.

**WEP (Wired Equivalent Privacy)?**

WEP is the oldest and most common Wi-Fi security protocol.It was ratified by Wi-Fi Alliance as a security standard in 1999. It has been plagued over the years by many security flaws and vulnerabilities that had been exploited easily and made it to be officially retired in 2004.

**WPA and WPA2 (Wi-Fi Protected Access)?**

It was released in 2003 to address the growing vulnerabilities of its predecessor, WEP. It uses a 256-bit key for encryption , it also uses the *Temporal Key Integrity Protocol* (TKIP), and dynamically generates a new key for each packet, or unit of data. TKIP is much more secure than the fixed-key system used by WEP. Since TKIP as the core component of WPA, was designed to be implemented onto WEP-enabled systems via firmware updates, It is relying on easily [exploitable](https://www.avast.com/c-exploits) elements.

WPA2 (Wi-Fi Protected Access 2) is the second generation of WEP which ensures that only people with your network password have access to it. It introduced the Advanced Encryption System (AES) to replace the more vulnerable TKIP system used in the original WPA protocol.

Unfortunately, like it’s predecessor, WPA2-enabled access points (usually routers) are vulnerable to attacks through WEP. To eliminate this attack vector, disable WEP and make sure your router’s firmware doesn’t rely on WEP. Here is a breakdown of the three most common Wi-Fi security types and their technical specifications:

|  |  |  |  |
| --- | --- | --- | --- |
|  | WEP | WPA | WPA2 |
| Year introduced | 1999 | 2003 | 2004 |
| Encryption protocol | Fixed-key | TKIP | CCMP |
| Session key size | 64-bit/128-bit | 256-bit | 256-bit |
| Cipher type | RC4 stream cipher | TKIP (RC4-based) | AES |
| Data integrity | Cyclic Redundancy Check | Message Integrity Check | CCMP |
| Authentication method | Open system/Shared key | PSK | PSK + PMK |
| Key management | Symmetric key encryption | WPA + WPA-PSK | PMK + PSK |

The Main Protocols’ Weakness

|  |  |
| --- | --- |
| **Protocol** | **Weekness** |
| WEP | * **The Size is short and reused/repetitive RC4 Key** * **RC4 algorithm is outdated** * **Simple forging of authentication message** |
| WPA | * **TKIP protocolhas the weakness** |
| WPA2 | * **AES is time consuming** * **Moderate security as attack allclients connected to particular AP having same group key.** * **ARP Poisoning/Spoofingattack is possible. (Stealth mode) WPA2** |
| WPA3 | * **Ongoing security risks shortly**[**after WPA3 was released**](https://www.pcmag.com/news/flaws-in-wi-fis-new-wpa3-protocol-can-leak-a-networks-password)**, researchers discovered a flaw that exposed network passwords. More coding problems may lurk within the new protocol.** * **Poor support. Even if you buy WPA3 routers, you may not be able to connect unless your devices also support the protocols. Older computers and smartphones may not.** * **Enhanced cost. Companies may balk at the bills associated with new system-wide routers.** |

Cracking Wireless network WEP/WPA keys

It is possible to crack the WEP/WPA keys used to gain access to a wireless network. Doing so requires software and hardware resources, and patience. Kali is a Linux-based security operating system. Kali comes with a number of security tools which can be used to gather information, assess vulnerabilities and perform exploits among other things. Some of the popular tools that Kali has includes for WI-Fi attack are Aircrack-ng, Reaver, Pixiewps, Wifite, Wireshark, oclHashcat ,Fern Wifi Cracker, Wash, Crunch, Macchanger [2]

**References :**

# [1] Wi-Fi Security: WEP vs WPA or WPA2 , Avast.com, <https://www.avast.com/c-wep-vs-wpa-or-wpa2>, Accessed: 2’nd March, 2023

# [2]:H. Josef, Aug. 2016, The Top 10 Wifi Hacking Tools in Kali Linux, Medium.com,< <https://medium.com/@henslejoseph/the-top-10-wifi-hacking-tools-in-kali-linux-fd707537ffe3>>, Accessed: 2’nd March , 2023