**Research on Wi-Fi**

**Technical Overview of the WIFI Network**

WIFI is a short-range wireless transmission technology, hundreds of feet to support access to the Internet in the context of a radio signal. WIFI transfer rate of up to 54Mbps, wide support for data and multimedia services, wireless range up to 100 m, without real geographical restriction, so is ideal for mobile user's needs. WIFI has defined two types of devices. A wireless station usually made up of a PC with a wireless network card. Then there's the wireless access point, its role is to provide a bridge between the wireless and wired networks. A wireless access point typically consists of a wireless outlet and a wired network interface, and bridge software 802.ld bridge agreement. The access point as a wireless base station is a wireless network, to aggregate multiple wireless access points on the cable network.[1]

**WIFI Security**

There are mainly 3 WIFI security algorithms: WEP, WPA, and WPA2. WEP started to be used in 802.11b standard in 1999 and is considered broken nowadays. WPA and WPA2 were introduced in 802.11i for solving the security issues of WEP in 2003 and 2004, respectively.[2]

**Wired Equivalent Privacy (WEP**) is an encryption algorithm aiming to provide secure communication over radio signals between two end-users in a WLAN. It uses a shared key mechanism adopting stream cipher RC4 with two key sides: 40 bits and 104 bits for confidentiality and authentication, and CRC-32 checksum for integrity. This indicates that the security of WEP is mainly dependent on the security of the shared key mechanisms. It is important that whether the key is able to resist a brute-force attack. [2], [3]

**Wi-Fi Protected Access (WPA)** which is an improved solution to WEP security problems and also an intermediate solution between WEP and WPA2. It adopts the Temporal Key Integrity Protocol (TKIP) instead of RC4, which uses a static 40-bit or 104-bit encryption key that has to be manually entered on wireless access points and devices. TKIP is able to prevent the types of attacks that inflict WEP because it employs a per-packet key by generates dynamically a new 128-bit key for each packet.

Moreover, WPA uses a stronger message integrity check algorithm called Message Integrity Code (MIC) for replacing CRC-32 of WEP to verify the integrity of the packets and provides two additional certification programs which are WPA-Enterprise and WPA-PSK for different types of users, the former adopts 802.1x protocol and Extensible Authentication Protocol (EAP) while the latter only uses pre-shared key (PSK). Although WPA is much more secure than WEP, it is better to use WPA2 to replace it if the hardware of a WLAN could support WPA2. [3]

**802.11i (WPA2). Wi-Fi Protection Access, Version 2 (WPA2),** also known as IEEE 802.11i-2004, enhances WPA by introducing Counter Mode CBC-MAC Protocol (CCMP) which is a new AES-based encryption mode with stronger security than TKIP. AES (Advanced Encryption Standard) is a symmetric-key algorithm that uses the same key with a length of 128 bits, 192 bits or 256 bits for both encrypting and decrypting data. Additionally, WPA2 adopts the same methods as WPA for message integrity and user authorization. [3]

**WIFI network security issues**

Attack on the WIFI network can be divided into two classes: one on network access control, data confidentiality and data integrity protection and attack; the other is based on wireless communication network design, deployment, and maintenance of the unique methods of attack. for the first type of attack that can also occur in the cable under the environment of network, wireless network security is on the basis of a traditional wired network that adds new security threats.[1]

**A. The weaknesses of the WEP encryption mechanism**

The mechanism of WEP was intended to provide cryptographic measures to prevent eavesdropping of wireless network communication. However, WEP was found to have many weaknesses in the end. Encryption algorithms are too simple; WEP is easy to crack keys by someone else. Key management is complex, use WEP keys need to accept an external key management system of control, because of the way this process is complex and requires manual operation, so many networks to facilitate the deployment, use the default WEP key, and allowing hackers to crack the key difficulty is significantly reduced.[1]

**B. Search wireless signal attack**

Search for the wireless signals is also a method of attacking wireless networks; there are many identification and attack techniques and software for wireless networks. Nets tumbler software is software that is widely used to find a wireless network. Many wireless networks is not using encryption, even if you use the encryption feature if you did not turn off the AP broadcast message feature, AP Radio and still contains a lot of information can be used to infer the WEP key information in clear text, such as network name, SSID, and other conditions to hackers intrusions. [1]

**C. Wireless network eavesdropping**

Disclosure threats include eavesdropping, interception, and monitoring. Tap refers to eavesdropping through a network of computer communication in electronic form, it is passive and intrusion detection cannot detect the device. Even if the network is not foreign broadcasting network information, if you can find any information in clear text, an attacker can still use some of the network tools, such as AiroPeek and TCPDump to monitor and analyze traffic, so as to identify information that can be overcome. [1]

**References:**

1-@inproceedings{peng2012wifi,

title={WIFI network information security analysis research},

author={Peng, Haishen},

booktitle={2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)},

pages={2243--2245},

year={2012},

organization={IEEE}

}

2- @inproceedings{wen2018wifi,

title={WIFI Security Certification through Device Information},

author={Wen, Yudong and Liu, Tao},

booktitle={2018 International Conference on Sensor Networks and Signal Processing (SNSP)},

pages={302--305},

year={2018},

organization={IEEE}

}

3- @inproceedings{sebbar2016empirical,

title={An empirical study of wifi security and performance in morocco-wardriving in rabat},

author={Sebbar, A and Boulahya, SE and Mezzour, G and Boulmalf, M},

booktitle={2016 International Conference on Electrical and Information Technologies (ICEIT)},

pages={362--367},

year={2016},

organization={IEEE}

}