THE VULNERABILITIES OF IEEE 802.11 WIRELESS LANS (WLANS)

HAN ZHONG

ABSTRACT

Wireless LANs have some advantages, it raises productivity, gives people easy life, etc. However, there are also vulnerabilities as the outcomes of these advantages. Some techniques were developed with intent to strengthen security of WLANs. This paper explains SSID, MAC address filtering, WEP/WPA/WPA2 and how they satisfy the security requirements.

I. INTRODUCTION

Nowadays, wireless LANs (WLANs) has been widely used in small areas like home, and even public areas like airport. The main reason for people using wireless LANs is mobility, and it is also fast, reliable and cheap. As we entering the era of wireless LANs, we must consider the security issues according to its special technologies. The widely used WLAN standards are 802.11[1] and Bluetooth. In this paper, only 802.11 standards will be considered. Bluetooth is similar to it and also face some same risks. I will also discuss the techniques used to secure it up.

II. VULNERABILITIES & SECURITY PROBLEMS

The security requirements are same as other networks, and can be summarized to: authentication, confidentiality and integrity. Authentication means that the sender and receiver must authenticate each other; confidentiality means that the communication data must be secured and cannot be understood by others; integrity means that the communication data was not modified by attackers.

[1] Broad heading for IEEE wireless LAN focus groups, currently there are 802.11a, 802.11b and 802.11g who distinguished by the bandwidths, also some others there.

Apart from the traditional networks (wired), the wireless network communications rely on radio channel and the signal is on the air. So this will carry out new vulnerabilities compared with wired networks. In the other words, people lose their security while they enjoying the advantages the wireless technology.

For instance, the very simple and clear vulnerability is that the channel can be **eavesdropped** [LJ08]. This vulnerability will lead to that the communication data can be easily sniffed by attackers by placing another antenna and configure the corresponding channel frequency**.** To prevent this kind of attacks, we can apply encryption protocol like WEP. WEP protocol will be discussed later. The known vulnerabilities of WLANs are predicted in seven categories by Robert [R02]:

- Insertion attacks
- Interception and unauthorized monitoring
- Denial of service (DOS)
- Client-to-client attacks
- Brute force attacks against AP passwords
- Encryption attacks
- Misconfiguration

These attacks and security risk are explained below and some examples are given:

Insertion attacks: is intended to be used by who want to use wireless station/access point's (AP) resource for free. For instance, the attacker plug-in his/her own laptop or PDA to an AP without authorization so he/she can use the internet connection for free.

Interception and unauthorized monitoring: Basically, the attackers sniff and capture the data transferred between clients/users and AP, then analyze it. It is also possible that attacker places another AP which gives out stronger signal and replaces the original one. Then the clients will try to log in the fake AP, and this will lead to loss

on sensitive data. For instance, if clients receive a fail notification of logging in, they may provide their password once more. So attackers will get the password of the users. Furthermore, by placing such intercept AP, attacker is also able to redirect the user to some malicious websites which will carry out further attacks.

Denial of service (DOS): is the same matter with signal jamming in WLANs and it is easily to carry out. Robert [R02] states that "because of their use of the ISM band, these signals can be jammed using cordless phones, baby monitors, a leaky microwave oven, or any other device that transmits at the ISM band frequencies."

Client-to-Client attacks: In some areas like office, there are many wireless clients like laptops, printers, and even servers. Since every client in WLANs can communicate with each other without going through the AP, attackers can perform usual TCP/IP service attacks or hack into clients. Even those clients do not connect to WLANs but installed a WLAN card with users' misconfiguration, attackers is also possible to activate them and so hack to them by the benefit of vulnerabilities of any operation system. Brian [B06] given out an example to explain how a attacker connect to such wireless client, "Wireless Network Interface Cards running in peer mode also send out the probe request frames we discussed in the war driving section. These probe request frames are sent out at regular intervals in an attempt to connect with another device that has the same SSID. Thus, using a wireless sniffer or NetStumbler, we are able to find wireless devices configured in peer mode."

Brute force attacks against AP passwords: Logging into an AP is controlled by password, so attackers can carry out a Brute force[2] cracking of the password.

Encryption attacks: Most 802.11 WLANs apply WEP protocol. Since the data can be sniffed, attackers can compromise the WEP protocol (WEP will be discussed later).

Misconfiguration: Most of the brand new APs are configured to be unsecured by default. For instance, the administrator's username and password are set to be both "admin" by default. This is not producers' mistake, but it is the responsibility of user to

[2] A Brute Force cracking application proceeds through all possible combinations of legal characters to try out the password. Brute force is considered to be an infallible, although time-consuming, approach.

configure AP. Unfortunately, there are still many users leave their APs with default configurations. Clearly, it is easy to fix.

III. SOLUTIONS

Recently, three basic methods are applied to secure up AP from attacks [R02]. They are service set identifier (SSID), media access control (MAC) address filtering and wired equivalent privacy (WEP).

A WLAN router uses a service set identifier (SSID) to indentify itself. The basic idea to introduce SSID is to distinguish APs in a multiply APs environment. Bradley Mitchell proposes that [B08] "an SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other." Normally, the SSID is broadcasted by WLAN router by default configuration. So when people using WLAN clients, they search and get known about the APs they can access to. It is clearly that attackers will also get benefits of the broadcasting, so many experts recommend user to turn off the broadcast of SSID and treat SSID as a shared password. Only authorized users will know the SSID or it is preconfigured by the network administrator. This method will satisfy

Applying media access control (MAC) address filtering is also a method to prevent attacks. Every network card has its own "unique" MAC address, and it is used to identify itself. Base on this, an AP can maintain a list of MAC addresses, and only those WLAN cards with their MAC addresses is on the list can access to the AP. In this common scenario, the list is called a "white list". Vice versa, the list can also be treated as a "black list" when the AP will block the access from the WLAN cards with their MAC address in on the list. There is no way to build a "white list" or a "black list" automatically, and it is needed to be set up manually by network administrators.

Wired equivalent privacy (WEP) is used to encrypt messages between clients and APs. The key in WEP protocol is symmetric. In the other words, there is only one key for encryption and decryption [M06]. The actually encryption algorithm employed by WEP is RC4. Mark [M06] explains RC4 algorithm in details. RC4 is a stream cipher

which produces a *keystream* by stretches the corresponding key. Then apply XOR operation to the plaintext (message) with the *keystream* to produce the *ciphertext* (encrypted message). When receiver want decrypt the *ciphertext*, receiver will use the same key to produce the same *keystream.* One of the advantages of RC4 is that the length of key can be varied from 0 to 256 bytes, because the key is only used to initialize. The pseudo-code for initialization and keystream production is given by Mark [M06]:

RC4 initialization.

```
for i = 0 to 255
        S[i] = i
        K[i] = key[i mod N]
next i
j = 0
for i = 0 to 255
        j = (j + S[i] + K[i]) mod 256
        swap(S[i], S[j])
next i
i = j = 0
```

RC4 keystream byte.

```
i = (i + 1)  mod 256
j = (j + S[i]) mod 256
swap(S[i], S[j])
t = (S[i] + S[j]) mod 256
keystreamByte = S[t]
```

Where S is keystream, key is the shared symmetric key, N is the length of the key and keystreamByte is a specified byte of the keystream.

For WEP, the length of key is specified relative short compared with the allowed max length of RC4 key which is 40 bit or 104 bit. Moreover, authentication of client to AP can also be carried out by shared key. AP returns a challenge phrase to clients whenever a client sent an authentication request. Then client encrypts the phrase with the predefined shared key and sends the ciphertext (encrypted phrase) back to AP. At last, AP decrypts the ciphertext and compares the result with original one. If they are match, the client is authenticated successfully, vice versa.

Above all, these three methods basically satisfied security requirements in section II. Is that really so simple to prevent attackers? Some more vulnerabilities and the lack in these methods will be discussed in section IV.

IV. DISCUSSION

SSID strengthens security of WLAN in very limited range. Everyone can get known of SSID, since it is broadcasted on the air. People can configure the AP to turn off the broadcasting of SSID; however, this cannot absolutely stop attackers to get these SSID [J05]. But it is really not a big problem need to be concerned. It is the same situation when we solve wired networks security problems, we cannot make clients to be absolutely anonymous. So attackers always know where and what they are attacking. We cannot erase the motivation of attackers, and this paper is not about ethic of networks users.

MAC address filtering seems to be perfect protection of privacy, since MAC address is fixed in the hardware. Unfortunately, it is not true nowadays. MAC address can be easily changed by current WLAN card drivers. Moreover, maintaining such a list of MAC addresses for large group of users is really painful and even impossible for some public environments. So this method may only suit to home private WLANs and users also need to keep their MAC address in secrete.

The last defense layer is encryption of messages, the WEP protocol. The core of WEP is RC4 algorithm which leads to some weaknesses. Jesse [J00] analyzes security problems of WEP and also talks about some attacks methods. It is clearly shown that WEP becomes vulnerable. There is also a small Perl application called "WEPCrack"[3] developed by Anton Rager, the description of it is "WEPCrack is a tool that cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling." Furthermore, 802.11 standard do is lack of key management. The keys need to be distributed by some other mechanism and even manually. For this reason, it is as harder to maintain the key in secret as growth of the number of users, since most WLANs networks use a single shared key [BGI01]. According to this, WPA was developed. WPA integrates TKIP into RC4; however, it is not a successful protocol. Then WPA2, aka RSN, was developed to satisfy security requirements, and it is claimed [HIM08] to be "the future of over-the-air security for 802.11 as put forward in." The encryption algorithm of WPA2 is Advanced Encryption Standard (AES) and it is based

[3] The application can be found here: http://sourceforge.net/projects/wepcrack

on 820.1X and Extensible Authentication Protocol (EAP) [HIM08]. AES is a block cipher and was developed with intent to replace DES.

There is a table of comparison of WEP, WPA, and WPA2 (RSN) given by Halil, Ihsan and Mesut. In this table, some features are clearly shown, and WPA2 is recommended to be the strongest security protocol. The only problem of WPA2 is performance; some old WLAN card may not work properly. Because AES is implemented, WPA2 more relies on hardware support.

V. CONCLUSION

WLANs have several vulnerabilities; however, the security can be strengthened by configuring AP and WLAN cards correctly. For small groups of users, the combination of SSID hiding, MAC address filtering and WEP protocol normally stratifies the security requirements. In addition, users may also need to generate random WEP keys and change keys often. For large enterprise, however, WPA2 is strongly recommended by security reasons.

BIBLIOGRAPHY

[B06] Brian Rodrigues, “Wireless Attacks ~ Client to Client Hacking”, E-articles.info, *http://e-articles.info/e-terms-and-conditions.htm* (accessed 2 September, 2008)

[B08] Bradley Mitchell. “SSID - Service Set Identifier”, About.com, *http://compnetworking.about.com/cs/wireless/g/bldef_ssid.htm*

[BGI01] Nikita Borisov, Ian Goldberg and David Wagner, *Intercepting mobile communications: the insecurity of 802.11*, New York: ACM, 2001,

DOI = http://doi.acm.org/10.1145/381677.381695

[HIM08] Halil Ibrahim Bulbul, Ihsan Batmaz and Mesut Ozel, *Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols,* Adelaide, Australia: ICST, 2008,

DOI = http://portal.acm.org/citation.cfm?id=1363217.1363229

[J00] Jesse R. Walker, “Unsafe at any key size; An analysis of the WEP encapsulation”, IEEE 802.11-00/362, 2000.

[J05] Joseph Migga Kizza, *Computer Network Security,* New York: Springer Science+Business Media, Inc., 2005, pp. 482-491

[LJ08] Levente Buttyan and Jean-Pierre Hubaux, *Security and Cooperation In Wireless Networks*, New York: Cambridge University Press, 2008, pp. 3-7.

[M06] Mark Stamp, *Information Security Principles and Practice*, Hoboken, New Jersey: John Wiley & Sons, Inc., 2006, pp. 12, 33-37, 45-48.

[R02] Robert J. Boncella, “Wireless Security: An Overview”, Communications of the Association for Information Systems Volume 9, 2002, pp. 269-282.