Security Analysis of Public Wireless Internet Access Points (November 2004)

S. Chang, B. Huang, V. Lam, and H. Yen

Abstract—**Over the past few years, wireless networks and wireless Internet have become ever increasingly popular, and with it, many security issues have arisen. An important topic is the security of wireless networks. This report investigates two possible solutions, Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). Both of these solutions can protect wireless communications from eavesdropping and modification. Nevertheless, they still have their own vulnerabilities. A brief description of the next-generation 802.11i and WPA2 wireless security will also be included in the report.**

IndexTerms—**Wireless Security, WEP, WPA, 802.11i, and Cryptography.**

1.0 Introduction

Wireless security is becoming increasingly important as wireless applications and systems are being widely adopted. Public places such as libraries, hotels, and Internet cafes are now offering free wireless Internet for travellers to check their e-mail and to access the World Wide Web. While computer users find it easy to use, hackers also find it to be an easy medium through which to snoop around on other people's personal transmissions.

A major difference between wired networks and wireless networks is the manner in which the transmitted data is accessed. The transmitted data of wireless networks can be accessed using equipment that is readily available in the market for a cheap price. But because public wireless access points are meant to serve any individual who comes by and wishes to access it, the service providers do not scramble data with any form of encryption, meaning that all transmitted data is in plain text and is easily readable by third parties.

This wireless security issue is currently being addressed, in part, by various standards such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). This paper will analyze the two standards and provide a brief overview of their operation and their known flaws. Furthermore, we will also take a look at the next generation of wireless security, in the form of IEEE's 802.11i and WPA2 from the Wi-Fi Alliance.

2.0 Wired Equivalent Privacy

WEP is an algorithm that is used to protect wireless communications from eavesdropping and modification. A secondary function of WEP is to prevent unauthorized access to a wireless network. It relies on a secret key that is shared between a wireless station and an access point. The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that the packets are not modified in transit.

2.1 WEP Operation

WEP uses the RC4 encryption algorithm. "RC4 is a stream cipher designed by Rivest for RSA Data Security (now RSA Security). It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation" [1]. WEP works as follows:

i. The sender generates a checksum of the message. The checksum is then concatenated to the end of the message as shown in Fig. 1.
ii. A *keystream* is generated based on a secret key called *k* and an initialization vector *IV* to be transmitted in the clear. *k* is agreed upon by the hosts during the initialization and *IV* is dynamically generated upon encryption.
iii. The result of step i is exclusively-or'ed with the result of step ii. This will create a bit stream called *ciphertext* as shown in Fig. 1.

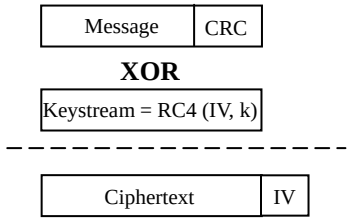

Fig. 1. WEP Encryption (sender)

iv. The *ciphertext* is then concatenated with the public key *IV* that was used to encrypt the message. Follow by transmitting the final result.
v. When the receiver receives the message, it reads the *IV* plain text and uses it with the previously shared secret key *k* to generate the same *keystream* again. At the end it exclusively-ors the generated *keystream* with the *ciphertext* to get the original unencrypted plain text as shown in Fig. 2 [2].

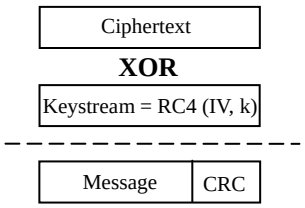

Fig. 2. WEP Decryption (receiver)

2.2 Key Stream Vulnerability

Key stream reuse is one of the big topics in WEP security issues. As mentioned in the previous section, encryption in the RC4 algorithm is done based on two fields: the secret key *k* and the public key *IV*. Since the secret key *k* is constant, if the same public key *IV* is used to encrypt two packets, then these two packets have been encrypted in the exact same way. This is known as key stream reuse [3].

If an eavesdropper intercepts two *ciphertexts* encrypted with the same key stream, it is possible to obtain the exclusive-or of the two plaintexts. Knowledge of this exclusive-or can enable statistical attacks to recover the plaintexts. Once one of the plaintexts becomes known, it is trivial to recover all of the others.

The public key *IV* in WEP is a 24-bit field. This small number of initialization vectors assures the eventual reuse of the same key stream. A busy access point transmitting 1,500 byte packets at 11Mbps will exhaust the *IV* space in about five hours [4]. This means that in a little over five hours, an attacker can collect at least two *ciphertexts* that have been encrypted with the same key stream and perform statistical attacks to recover the plaintext.

2.3 Finding the WEP Keys

There are many public attack tools available on the Internet. One of the most popular WEP attack tools is AirSnort [5]. AirSnort is a command-line based tool that exploits the vulnerability discussed in the previous section. It first looks for packets that have been encrypted with the same key stream between users and an access point. Those packets are then saved and labelled with “interesting packets.” After it collects a large number of interesting packets, it attempts to crack the WEP key. Once the WEP key is obtained, one can use it with a packet capturing software to see all traffic between users and the access point.

2.4 WEP Vulnerability Solutions

There are several solutions that one can use to prevent the exploitation of their wireless network. The first one is to increase the size of the *IV* field. Although this solution helps, it does not solve the underlying problem. It merely lengthens and delays the encryption breaking process. Another possible solution is proposed by the Wi-Fi Alliance called Wi-Fi Protected Access (WPA). WPA has not only increased the *IV* field from 24 bits to 48 bits, but it has also made the secret key *k* dynamic. Though it may seem that WPA fixed the vulnerability, WPA has its own security vulnerabilities such as the one described in section 3.2.

3.0 Wi-Fi Protected Access

WPA is a standards-based interoperable security specification. The specification is designed so that only software or firmware upgrades are necessary for the existing legacy hardware to meet the requirements. Its purpose is to increase the level of security for existing and future wireless LANs. “To meet these goals, Wi-Fi Protected Access was constructed to provide an improved data encryption, which was weak in WEP, and to provide user authentication, which was largely missing in WEP” [6].

3.1 WPA Operation

As mentioned in the previous section, WPA is a security solution that targets all the known WEP vulnerabilities. Some key features include an 802.1x Extensible Authentication Protocol (EAP) based authentication scheme, a Temporal Key Integrity Protocol (TKIP) on top of the existing RC4 as used in WEP and a Message Integrity Check scheme named *Michael* [7].

WPA adopts the IEEE 802.1x standard and the EAP to address the issue of user authentication in WEP. The authentication process starts when a supplicant (client) initiates connection with an authenticator (server). The authenticator then requests the identity from the supplicant through the EAP methods. The supplicant responds with its identity and then the authenticator passes the identity to an authentication server. Once the server authenticates the identity, an *ACCEPT* message is sent to the authenticator. The supplicant then requests the identity of the authentication server. After the authentication server is identified, the authentication process is completed.

WPA also adopts TKIP to fix the security flaw of key stream reuse in WEP. In order to be compatible with existing hardware, TKIP uses the same RC4 encryption algorithm as WEP. However, a TKIP packet is comprised of three parts: a 128bit temporal shared key, a 48bit secret key *IV* and a MAC Address of a client device as shown in Fig. 3.

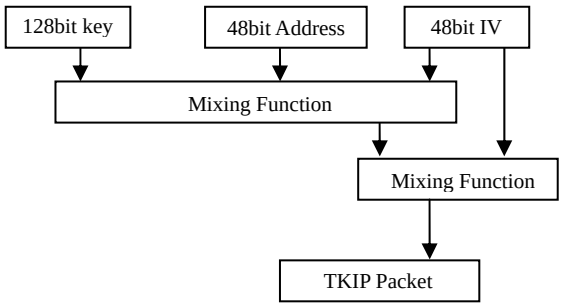

Fig. 3. A TKIP Packet

Compared with WEP, TKIP changes the temporal keys every 10,000 packets. This dynamic distribution of the TKIP key leaves potential hackers little room to crack the TKIP key.

Lastly, WPA adopts a Message Integrity Check algorithm called *Michael* that is used to enforce data integrity. The algorithm generates a 64-bit Message Integrity Code (MIC) message which is inserted into a TKIP packet. Its aim is to detect potential packet content alteration due to either transmission error or deliberate manipulation.

3.2 Pre-Shared Key Vulnerability

WPA provides the support of using Pre-Shared Key (PSK) as an alternative to 802.1x based key establishment. The problems with WPA center on the use of the PSK. A PSK can be either a 256-bit number or a passphrase that is 8 to 63 bytes long. When the PSK is a 256-bit number, the PSK becomes the Pairwise Master Key (PMK) that is used to drive the 4-way handshake and the whole Pairwise Transient Key (PTK) keying hierarchy. However, when the PSK is a passphrase, the PMK is derived from the passphrase according to the PBKDF2 algorithm from PKCS #5 v2.0: Password-based Cryptography Standard [8]. This is where the vulnerability appears as anyone who possesses the passphrase can use it to generate all other information.

According to Robert Moskowitz, a senior technical director at ICSA Labs, the method that WPA devices use to exchange information used to generate data encryption keys for wireless sessions allows attackers who do not know a PSK to guess it using a dictionary attack [8]. Therefore, if a weak passphrase such as a short one is used, an offline dictionary attack can readily guess the PSK. Once the Pre-Shared Key is learned by the attacker, the attacker is now a member of the wireless network, and the whole wireless network is compromised. The attacker can now read and forge any traffic in the Extended Service Set (ESS).

Moskowitz also pointed out that instead of harvesting large quantities of network traffic as in finding WEP key, WPA PSK attacks only require attackers to capture four specific packets of data. Furthermore, attackers who miss those four packets in transit can easily trick a wireless access point into doing a new handshake and sending the packets to the attackers again. This has made the offline dictionary attack easier than the WEP attack.

3.3 Finding the Pre-Shared Key

As of November 1, 2004, Takehiro Takahashi released a WPA cracker [9]. This tool simply automated Moskowitz's WPA attacking process. It requires the attacker to enter appropriate data retrieved via a packet sniffer such as Ethereal. Once entered, it attempts the dictionary attack. However, just like other dictionary attacks, this is effective only if a weak passphrase is used.

3.4 WPA Vulnerability Solution

The solution to this WPA weakness involves one of three approaches. The first option is to choose a better passphrase, such as picking a passphrase that contains at least 20 characters with random non-sense letters. The second option is to use randomness to choose a passphrase. A random passphrase of at least 96 bits will effectively defeat the cracking method as described by Moskowitz. The third option is to use 802.1x key establishment with WPA. Deploying enterprise-based authentication will allow a strong WPA key to be uniquely assigned to each user.

4.0 Future Wireless Options

Since both WEP and WPA have known vulnerabilities, there exists the need of a new wireless security standard. Therefore, IEEE has proposed a new standard for 802.11-based wireless LAN security named 802.11i while Wi-Fi Alliance has proposed the related WPA2 as the successor of the original WPA.

4.1 IEEE 802.11i and WPA2 Features

The features in IEEE 802.11i and WPA2 are virtually identical. The two most important features beyond WPA that have become standardized in 802.11i and WPA2 are pre-authentication and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) ciphers. Pre-authentication offers secure fast roaming without noticeable signal latency while CCMP offers the use of the AES as the ciphering technique. Different from TKIP, AES ciphers can provide a higher level of data privacy required by large enterprises, government agencies and other organizations. According to Adam Wong, an IBM engineer, the new standards will offer "an unbreakable encryption algorithm" that protects airborne data [10].

Although 802.11i and WPA2 are basically the same, they provide for some differences due to their respective roles in the industry. "The key difference between WPA and 802.11i is the support that the latter will give for fast roaming," according to Moskowitz. "When enterprises begin to look at wireless voice, they are going to need that functionality to prevent signal latency and the dropping of the voice content when roaming. WPA is ready for enterprise use, but lacks certain finishing items, which are in 802.11i. So, 11i provides a more current code set and the ability to do wireless voice" [11].

5.0 Conclusion

The general idea of public wireless access points is to provide easy Internet access to travellers on the go. However, security is still a significant issue that all users should consider about. While new standards are still under evaluation, wireless access point vulnerabilities can be reduced by practicing the suggested methods mentioned previously in this article. Nevertheless, the best way to secure a wireless LAN is to have the security knowledge necessary for proper implementation and continued maintenance. In addition, educating the everyday user to practice safe security habits will further secure a wireless LAN.

REFERENCES

[1] "What is RC4?" RSA Security, [Online] (2004, November 26) Available: http://www.rsasecurity.com/rsalabs/node.asp?id=2250

[2] C. Barnes, T. Bautts, and D. Lloyd, "Hack Proofing Your Wireless Network," USA: Syngress Media, 2002.

[3] J. S. Park and D. Dicoi, "WLAN Security: Current and Future," *IEEE Internet Computing*, Sept.-Oct. 2003, vol. 7, issue 5, pp. 60-65

[4] K. Tyrrel, "An Overview of Wireless Security Issue," USA: SANS (SysAdmin, Audit, Network, Security) Institute 2003, pp. 5-9

[5] AirSnort Homepage, [Online] (2004, November 26) Available: http://airsnort.shmoo.com/

[6] C. B. Grimm, "Wi-Fi Protected Access Overview," Wi-Fi Alliance, [Online] (2002, October 31) Available: http://www.wifialliance.com/OpenSection/protected_access_archive.asp

[7] B. Potter, "Wireless Security's Future," *IEEE Security & Privacy*, July-Aug. 2003, vol. 1 issue 4, pp. 68-72

[8] R. Moskowitz, "Weakness in Passphrase Choice in WPA Interface," ICSA Labs, TruSecure Corp., Nov. 2003.

[9] WPA Cracker, [Online] (2004, November 29) Available: http://www.tinypeap.com/page8.html

[10] E. Christopher and S. Marc, "A new 'i' for Wi-Fi," *U.S. News & World Report*, Aug. 2004, vol. 136, issue 8, pp. 79.

[11] J. Burns, "On the Way: 802.11i and WPA2," *Communications News*, Jun. 2004, vol. 41, issue 6, pp. 33.