AirPTWFrag: A New Wireless Attack

Raghuveer Singh Dhaka, Arvind Dhaka, Priyank Singh Hada

Abstract— one of the issues with corporate wireless networks in general, and WLANs in particular, involves the need for security. Several protocols have been proposed and used for providing security to wireless networks. The Wired Equivalent Privacy (WEP), used to secure 802.11 based networks, suffers from many weaknesses making a way for several types of attacks. In this paper a new attack on wireless security has been proposed. We will give a review of the attack that is capable of decrypting messages in WEP enabled wireless networks without requiring the knowledge of the encryption key.

Keywords- WLAN Security; Denial of Service; MAC Spoofing; TKI; WEP; WPA; PTW; ARP

1. Overview Of Wireless Security

From the evolution of wireless networks IEEE 802.11 has obtained popularity over the Local Area Networks (LANs). Radio frequencies are used as a medium for communication in wireless networks. It is not a difficult task for an attacker to arrogate the messages that are being transmitted between wireless access points and the wireless network clients. Simple text communication is unsafe because an attacker can easily sniff the packets for as banking passwords, credit card numbers, and other personal information.

The first section of this paper will explore several methods of encryption based and other wireless network attacks, specifically the KoreK Attack, PTW Attack, Chop-Chop Attack, Denial of Service Attacks, Spoofing Attacks, ARP poisoning Attack and Man-In-The-Middle Attacks. For each attack, we shall discuss the wireless vulnerabilities that give way to the attacks, the methodology of the attack, and specific examples of implementations. The second section of this paper will discuss proposed method "A new wireless attack AirPTWFrag (Combination of PTW with fragmentation attack)".

2. Wireless Security Attacks And Vulnerabilities

2.1 Encryption-Based Attacks

WEP was introduced to provide security to the wireless networks via implementing data confidentiality. WEP encrypts data, via RC4 stream cipher, with 64 bit key size generated by the combination of 40-bit Secret key and 24-bit initialization vector (IV). However WEP is considered as a weak security measure. One of the security limitations of WEP is its key size.

Another protocol proposed, Wi-Fi Protected Access (WPA), is more secure and advantageous in comparison to WEP. WPA provides the wireless security against WEP attacks. WPA replaces the 40-bit key with Temporal Key Integrity Protocol (TKIP) which provides a 128-bit per packet key that is dynamically generated to prevent collisions. It also included a Message Integrity check which is used to prevent hackers from capturing, altering, and/or resending data packets. WPA2 is more secure and more advantageous in comparison to WPA. In WPA2 the RC4 stream cipher with Counter Mode replaced with Cipher Block Chaining Message Authentication Protocol (CCMP) Advanced Encryption Standard (AES) algorithm is used in it.

1) KoreK Attack: KoreK is a famous attack developed in 2004. It was a cracking suite which consisted of 17 different attacks. In this suite the attacks were implemented in three groups. The first group consisted of an attack similar to the FMS attack. In this attack the key is recovered by the use of the first word of output from the RC4 algorithm. The second group uses the combination of the first and the second word. And the third group, which is known as inverse attacks, is able to omit certain values from being in the key. Instead of guessing what the key values could be it determines what the key values could not be. About 97% probability of success is achieved by KoreK by capturing only 300,000 packets.

2) PTW Attack: In 2007 Pyshkin, Tews, and Weinmann performed an attack on WEP which is known as PTW attack named after its developers. In this attack, it picks a set number of keys and continues the RC4 algorithm based on these keys instead of trying all possible combinations of the key [2]. Around 97% probability of success is achieved by using only 20,000 to 40,000 packets.

2.2 Wpa Attacks

1) Chop-Chop Attack: It is an attack on TKIP. Chop-Chop attack is not a key recovery attack. Originally this attack was implemented against WEP. By sending m*128 packets into the network it allows the attacker to decrypt the last m bytes of plaintext of an encrypted packet. It exploits the weakness of the CRC32 checksum called the ICV which is added to the data of the packet [7]. The attacker attenuates the last byte of the encrypted packet and guess the value and returns the packet to the access point. The packet will be discarded if it is incorrect. Once the attacker have guessed the right value for the last byte attacker can continue backwards through the rest of the bytes until the attacker guess the whole packet. To find out the right value it takes an average of 128 guess per byte [6]. The attacker now captures a packet and find out a low traffic channel where the sequence counter will still be low and tries the attack. The access point will still silently drop the packet when the attacker guess the last byte wrong, but if the guess is correct then a MIC failure report frame is sent to the client. Once an attacker received it he knows that his/her

guess is correct and must wait at least 60 seconds before disconnected he continuously guessing in order to prevent the client from being disconnected. Once the last 12 bytes are decrypted by the attacker then the attacker will have the MIC and the ICV in plaintext [8, 9]. By the use of ICV, the attacker can guess the rest of the packet and perform the CRC32 until the values match and they know they have decrypted the packet. The attacker can reverse the algorithm to recover the MIC key.

2.3Wpa2 Attacks

WPA2-PSK (Pre-Shared Key) is the most secure in comparison to previously described protocols. Advanced Encryption Standard (AES) is used to encrypt the data in place of the RC4 stream cipher. A four way handshaking is performed to authenticate the client with the access point when a client wants to connects to a WPA2-PSK. When a client performs the handshake it implements Secure Hash Algorithm 1 (SHA-1) on the shared key with the access point's Service Set Identifier (SSID) and sends it to the access point for verification. An attacker can capture this packet by eavesdropping over the network traffic. In case if no client tries to connect in the time, the attacker may perform a forced handshaking by means of a de-authentication attack. In this attack the attacker sends a de-authentication packet to the client after disguising themselves as the access point. If the client accepts this packet and re-authenticate with the access point then the attacker captures the handshake. Thereafter it is as easy to recover the shared key in plaintext by performing either a brute force or a dictionary attack.

3. Attack Tools Based On Encryption

There are several tools in hacking market which are used to perform attack on wireless networks. Backtrack 4 is one free Linux distribution which includes hundreds of these tools including the Aircrack suite. Airsnort (part of the Aircrack suite) was the first tools which could be used to deploy the FMS attack. It has become out of date because the use of the Advanced WEP Encryption standard which tries to reduce the number of weak IVs that are generated. Some other tools included in the suite such as Aircrack which is used to perform an attack on the WEP key and WPA. A lot of packet sniffers and packet capturing tools are also used to perform an attack as well as packet injection tools that can be used to perform replay attacks and de-authentication attacks. There are also many other hashing tools such as Hash cat that is used to recover the plaintext from hashes. John the Ripper can be used to generate permutations on common words or passwords to create a larger dictionary file.

4. Other Attacks

4.1 Denial of Service Attacks

Denial of Service Attacks attempts to prevent the availability of information resources of access points to the legitimate users. As a method to perform this attack, noise can be transmitted on radio channels just to keep the service busy, thus preventing the authenticated user to transmit data. This requires a great deal of transmission power and is easy to trace back from the source of the disruption. The main goals of denial of service attacks are to avoid detection and maintain the disruption for the longest period of time [1].

Another attack, known as the Transmit Duration attack, exploits the transmission duration field of 802.11 frames which allows a node to reserve the channel for up to 1/30th of a second. The attacker takes over the network channel by sending 30 packets per second (i.e. injecting packets in network with a maximum transmit duration) thus making the other nodes wait for their turn to transmit.

The Random Packet Destruction DoS attack is another energy efficient attack which is easy to perform and difficult to be detected. It works even in situations when it is hard to inject packets in the network and there are no other means to intrude on the network. The attacker must have the knowledge of detecting packet transmissions over the air to implement this attack.

4.2 Spoofing Attacks

When an attacker captures and then modifies the packets and transmits in the same network masquerading that he is the legitimate user or an access point, it is known as spoofing attack. Spoofing is commonly used as a part of another attack.

Spoofing is used to perform de-authentication attack on WPA, in which the attacker sends de-authenticate packets to the client and illusion is that they are coming from an access point. This attack can also enable the attacker to recover the SSID [12]. When the client re-associates, the handshake packets will contain the SSID of the access point, allowing the attacker to collect it. De-authentication attacks can be used as a targeted denial of service as well, just keeping a certain client from using the network.

4.3 Man in the Middle Attacks

An attacker can use a de-authentication attack against the client on a network disconnecting him from the network. When the client reconnects to the network the attacker masquerade as the access point and captures the data stream sent by the client. The attacker now can read all unencrypted traffic which is sent by the client, but does not gain access to SSL encrypted connection data. One way to avoid this restriction is to rewrite website redirects and links being sent to the client removing "https://" from them to reduce the change that SSL will be used to encrypt the session. Marlinspike's Sslstrip is a tool that performs such type of attack [10]. Sslstrip provides several attacks against HTTP traffic by keeping users from accessing HTTPS versions of sites and rewriting secure sites to use plain HTTP, allowing the attacker to capture "secure" login information. This type of attack requires that the intruding node is able to connect to the network that is being attacked.

4.4 ARP Poisoning Attacks

ARP poisoning is a common network attack that can be used to set up a Man in the Middle attack. ARP stands for the Address Resolution Protocol used to find the MAC address of the host if his IP address is known. It can be accomplished in two ways: spoofing ARP replies or sending spoofed IP packets [11]. If an attacker can get the ARP table entry for the default gateway on the client node to point at itself then all packets, that client tries to send out of the network, will go to the attacker first. A man in the middle attack along the lines of SSl strip can now be carried out. This method also requires access to the network through cracking the network key.

5 Proposed Attack

A new wireless attack AirPTWFrag (Combination of PTW with fragmentation attack)

PTW attack is a Guessed-plaintext/guessed-key stream attack, where some parts of the packet can be guessed by looking at the length of the packet. The fragmentation attack is used to recover full IV+ key stream pairs. The combination of PTW and fragmentation attack is an active attack that cracks a WEP key within a minute.

5.1 Executing the attack

The Execution of PTW attack is a little bit different than the previous attacks. First, we assume that an Oracle WEP (OWEP) is accessed by an attacker and after that collect sessions. In all previous attacks, the attacker tries to determine Rk [0] first, before looking at Rk [1]. Instead of this, all functions f_{ptw1} to f_{ptw13} are evaluated by an attacker for every session. The result of each function is called a vote for σ_m having a specific value. The votes for each σ_m are stored in a separate table. This table is known as frequency table for σ_m. Now, the attacker assumes that each top voted entry in each frequency table is the correct value for σ_m. These values are tested to determine the correctness. If they are correct then the attacker can simply calculate the key from these values.

This attack itself is expected to be weaker than the Klein attack, because every single function, except f_{ptw1}, which is the same as f_{Klein}, has a lower success probability than f_{Klein}. The only advantage of this attack is that an implementation does not need to hold all sessions in the main memory, until the attack is finished. Instead, every session is not needed anymore, after all votes from that session have been added to the frequency tables. The main advantage of the PTW attack is that key ranking is much faster than in the Klein attack.

5.2 New strategies

The choice of static number for every frequency table is just the same as static number of paths to follow because the PTW attack can determine all values for σ_m independently of each other.

Let's assume that the attacker has processed all sessions and now has l_{key} frequency tables t_i. The attacker now assumes that the correct value for σ_m is in the k top voted entries in table t_m. The attacker can now start to test all possible values Rk can take, if the correct value for σ_m is in the k top voted entries in the frequency table t_m. There are at most $k^{l_{key}}$ possible values. Arrangement of all these values usually takes less computational effort in comparison to testing them all. Here, k is allowed to have a larger value than for a pre-PTW attack using the Static number of paths to follow key ranking strategies, because there are no new voting processes during the key ranking necessary. The total size of the data structure can be less than 200 bytes for an efficient implementation.

5.3 Dynamic Key search Method:

We had the idea of creating a better key ranking strategy. In the basic attack, the attacker assumes that for every m, the value σ_m was the most voted value in the respective voting table t_m. If second value for σ_m, which had only a few less votes then the attacker is much unsure about the decision for σ_m, than for another value σ_m, where the top voted entry has much more votes than the second most voted entry.

Let's call the number of possible values at the top of t_m, where possible values for σ_m are taken from, the search border for t_m. In our previous strategy, we assume that for every m, the correct value for σ_m is in the k top voted entries in t_m, and therefore, the search border for every frequency table t_m is k. Now we try a more dynamic approach. At the beginning, the search border for every table is 1, which means that just the top voted entry in the table is a possible candidate for σ_m. Now, we are looking for the table, where the first entry outside the search border has a minimal distance in number of votes to the top voted entry in the table. At this table, the search border is increased by one. Naturally speaking, we try to increase the search borders in tables, where we are unsure if our decision is correct. For tables where the top voted entry has much more votes than the next candidates, we were relatively sure about our decision and the search border is kept small.

The advantage of this strategy is that the number of possible keys can be fine controlled, because every increase of the search border will just increase the number of possible keys by factor 2 at most.

In this Technique every time we perform a fragmentation attack, the AP is helpful to generate a new key stream with a new IV for us. In this way for continuous fragmentation attacks we get a new key stream for every attack, even if we start the attack with the same packet. In this way we get 1985 different key streams to performing 1985 fragmentation attacks.

The attack is described as follows:

- By packet sniffing we get at least one data packet.
- This packet is used for a fragmentation attack. We get a full key stream with IV. In case of failure we again perform packet sniffing and retry.
- If the attack succeeds, then we do another fragmentation attack, and get another full key stream.
- Repeat step 3 several times. For every execution we get a new key stream, in this way we get 1987 key streams after performing 1987 attacks. Store the key streams in a single file. We don't need to repeat the entire attack except only

the last part as it will produce different IV/key streams for each iteration.

- When we reach a critical number of key streams collected, run a PTW attack on the key streams, while still doing more fragmentation attacks in the background, in case of insufficient number of key streams are found.
- If the PTW attack remains successful, then store the key and stop running fragmentation-attack on the network. If it fails, then get more key streams until PTW is not successfully crack the key.

6 CONCLUSION

On the basis of the analysis of the existed attacks, especially the attack performed on WEP, we proposed a new type of Wireless Attack in this paper. There are several security flaws in the Wireless protocols. The main advantage of the PTW attack is that key ranking is much faster than in the Klein attack. In the last decade, wireless networks gained a substantial momentum. One of the most beneficial features of wireless networks is that they support user mobility in a convenient way. But the wireless networks are more susceptible to attacks than their wired counterparts which can be easily seen in this paper. It is important to provide appropriate security measures for wireless networks, which ensure the robustness of their operation even in case of malicious attacks. With the help of PTW attack, it is possible to perform an attack on WEP protected networks. The PTW attack is fully automated so the attacker finds all networks and recovers their secret keys.

REFERENCES

[1] Mina Malekzadeh, Abdul Azim Abdul Ghani, Shamala Subramaniam, and Jalil Desa, "Validating Reliability of OMNeT++ Wireless Networks DoS Attacks: Simulations vs. Testbed", International Journal of Network Security, Vol-13, No. 1, pp. 13-21, 2011.

[2] Mina Malekzadeh, Abdul Azim Abdul Ghani, Shamala Subramaniam, and Jalil Desa, "Emprical Analysis of Virtual Carrier Sense Flooding Attacks Over Wireless Local Area Network", Journal of Computer science 5 (3), pp. 214-220, 2009.

[3] Shamala Subramaniam, Mina Malekzadeh, Abdul Azim Abdul Ghani and Jalil Desa "Vulnerability Analysis of extensible Authentication Protocol (EAP) DoS Attack over Wireless Networks", The International Journal on Computer Network and Internet Research, CNIR, Vol 9,Iss. 1, pp. 39-46, July 2009.

[4] E. Tews, R. Weinmann, and A. Pyshkin, \Breaking 104 bit WEP in less than 60 seconds," Cryptology ePrint, 2007, available at http://eprint.iacr.org/2007/120.pdf.

[5] R. Teramura, Y. Asakura, T. Ohigashi, H. Kuwakado, and M. Morii, \Breaking WEP with Any 104-bit Keys {All WEP Keys Can Be Recovered Using IP Packets Only{," Proc. of SCIS2009, CDROM, 1A2-6, Jan. 2009.

[6] M. Beck and E. Tews, \Practical attacks against WEP and WPA," 2008, available at http://dl.aircrack-ng.org/breakingwepandwpa.pdf.

[7] IEEE-SA Standards Board, \Wireless lan medium access control (MAC) and phys- ical layer (PHY) speci_cations," Communications Magazine, IEEE, 2007.

[8] Martin Beck, Erik Tews. Practical attacks against WEP and WPA [C]. Proceedings of the 2nd ACM Conference on Wireless Network Security, WiSec'09, p79-85, 2009.

[9] Masakatu Morii Toshihiro Ohigashi. A Practical Message Falsi_cation Attack on WPA. 15 July 2009.

[10] H. Tang, R. Sun, W. Kong, " wireless intrusion detection for defending against TCP SYN flooding attack and man-in-the-middle attack," Key Laboratory of Intelligent Computing & Information Processing, July 2009.

[11] Hao Hua, Steven Myers, Vittoria Colizza, and Alessandro Vespignani. WiFi Networks and Malware Epidemiology. Proceedings of the National Academy of Sciences, Vol. 106, No. 5. (3 February 2009), pp. 1318-1323.

[12] Erik Tews and Martin Beck. 2009. Practical attacks against WEP and WPA. In Proceedings of the second ACM conference on Wireless network security (WiSec '09). ACM, New York, NY, USA, 79-86.