Practical Defence against WEP and WPA-PSK Attack for WLAN

Ying Wang, Zhigang Jin, Ximan Zhao
School of Electronics and Information Engineering
Tianjin University
Tianjin, China

***Abstract*—WLAN is widely used since it provides a both convenient and flexible way of communication. However, it is more vulnerable to unauthorized access. So WEP and WPA are proposed to improve the security of WLAN as two popular standards. But they are not perfect. In this article we analyze their shortcomings and raise two mechanisms named d-WEP and d-WPA-PSK. The d-WEP adopts the frequency of ARP requests to AP as a standard to judge whether AP is attacked and prevents the client suspected to access by dropping the ARP requests from it. Next we theoretically analyze the feasibility and do some corresponding experiments based on the loadable module, netfilter and hostap functions of linux. The experimental results show d-WEP can effectively prevent the active attack against WEP which is consistent with the result of theoretical analysis. On the other hand, the d-WPA-PSK uses such a mechanism that the PSK is regularly replaced to prevent dictionary attacks. This method has been proven to be feasible in theory. So for wireless network security, our research will have great significance.**

***Keywords*-WEP; WPA-PSK; WLAN; Defence; 802.11**

I. INTRODUCTION

Wireless Local Area Network (WLAN) is playing a major role in modern communications, which provides a both convenient and flexible way of communication. The main attractions of WLANs includes of cost effectiveness, ease of installation, and its mobility. However, Media access in wireless networks is fundamentally different from the media access mechanisms in wired networks, where one has to hook up a computing device to a network cable for transmitting and receiving data, and the cables are physically protected by walls, ceilings, doors, and other forms of physical structures. WLAN does not have the same physical structure as LANs do, and therefore are more vulnerable to unauthorized access.

To provide wired equivalent media access, IEEE 802.11 standard defined WEP (Wired Equivalent Privacy), which encrypts traffics between clients and AP. And some stronger security technology, such as TKIP (Temporal Key Integrity Protocol) and 802.1X, are developed. Based on these technologies, WPA (Wi-Fi Protected Access) is raised for improving or replacing the WEP mode, which has two operating modes: Enterprise mode and PSK (pre-shared key) mode. In this article PSK is our primary concern. However, in a WEP protected network, all packets are encrypted using the stream cipher RC4 under a common key, the root key [2], which is shared by all radio stations. A successful recovery of this key gives an attacker full access to the network. Besides, the use of WPA-PSK is similar with the use of static WEP, except the password level and management.

Obviously, security in WLANs is a severe issue. So to improve the security in the WLAN environment, in this article we proposed some practical mechanisms. First, based on the linux system, we modify the network protocol stack to detect the probably attack (active attack). If the action detected is consistent with the principles set out in advance, we will prevent the related client to access the AP for a period of time. Using this mechanism named d-WEP active attack against WEP can be effectively prevented. Next, we propose a d-WPA-PSK mechanism in WAP-PSK and analyze the impact in improving the security of WAP-PSK.

The remainder of the paper is structured as follows. Section 2 briefly issues the related work. In section 3 we mainly introduce the principle and weaknesses of WEP and WPA-PSK. Our design and analysis are presented in section 4. Section 5 gives some related experiment. And finally the conclusion is introduced in section 6.

II. RELATED WORK

Research on wireless network security has been a great deal of work, especially with regard to the existing popular WEP encryption algorithm. Firstly, Fluhrer, Mantin and Shamir in [5] showed a noteworthy cipher text attack on WEP. They proved the secret key can be recovered if a large amount of encrypted frame can be eavesdropped. Next, a passive-only attack which can significantly improve the key recovery process on WEP in [9] and a correlation related to the first three bytes of the secret key and the first byte of the key sequence in [8] are presented. More advanced attacks were published in the last years making it possible to recover the secret key of the network in less than 60 seconds [4]. In response to these attacks, there are but small defense researches. In [6], the authors analyze WEP security holes and propose an improvement over WEP which achieves a security service which is replay detection. Besides an alternative solution to WEP hacking, Interference-Based Prevention Mechanism, is proposed in [10]. This mechanism is proven to be effective in preventing attackers for getting the key by means of packets gathering.

978-1-4244-3709-2/10/$25.00 ©2010 IEEE

In order to fix the weakness discovered, a new standard named Wi-Fi Protected Access (WPA) is released by Wi-Fi Alliance in [1]. Basically, security has been enhanced because of anti-replay protections and a key management scheme to avoid key reuse in WPA. However, some weaknesses are also applicable to WPA despite of the different key between any two encrypted packets in RC4. In [3] Martin describe the first attack on WPA secured wireless networks, which works if TKIP algorithm is used to encrypt the traffic, besides launching a dictionary attack when pre-shared key (PSK) is used. And almost all of WPA versions and problems are explained in [7].

Can be seen from the above, the security research on wireless network mainly concentrated on the attacks, so the research for defence in wireless network has great significance. Our d-WEP is similar with the idea in [6], but besides detection we make some rules to control the client's access according the detection results. And since the research work on WPA-PSK is not much, our d-WPA-PSK mechanism in WPA-PSK has a great significance.

III. VULNERABILITY OF WEP AND WPA-PSK

A. WEP and its Vulnerability

The WEP was designed to give some security by encrypting data transmitted over the WLAN. Figure 1 illustrates WEP encryption process. At first, the secret key used in WEP algorithm and a 24-bit initialization vector (IV) are concatenated as the encryption/decryption key. Secondly, the resulting key acts as the seed to generate the key sequence. Then, plain text message, along with its ICV, is combined with key sequence. After a bitwise XOR process, we get the cipher text. A final encrypted frame is made by attaching the IV in front of the cipher text.

The decrypting process is the reverse process of the encrypting process. Firstly, the receiver generates key sequence by shared key and IV. Then, the initial plaintext can be resumed by XOR operation between the key sequence and the cipher text. Next, data integrity is checked. The plaintext goes to Integrity Algorithm to make a new ICV (ICV') and finally we should compare the ICV' and ICV to determine the data integrity. This process is shown in Figure 2.

Since stream ciphering is used as a pseudo-random number generator in WEP algorithm and in XOR based stream cipher reuse of key stream is forbidden, in WEP an IV filed is added.

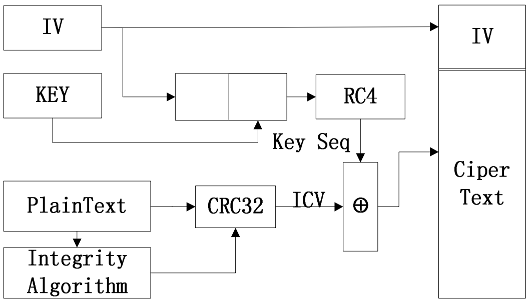


Figure 1 WEP Encryption process

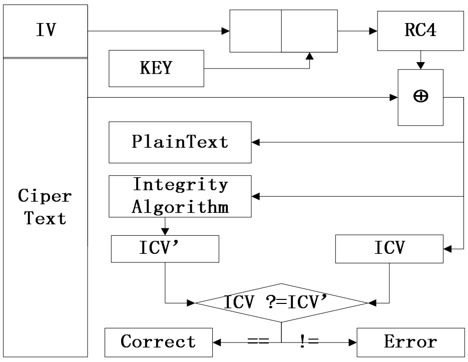


Figure 2 WEP decryption process

However, in practice, reusing an IV is frequent. In addition, WEP key is rarely changed. So to ensure any two different key streams different is impossible. Furthermore, the attacker can simply detect reuse of IV since IV is transmitted as clear text and there are many ways to obtain a clear message. Now with two or more encrypted messages with some same IV and one original message, the attacker can decrypt other encrypted messages using only XOR operations. Next, they can recover the key by gathering the key streams.

B. WPA-PSK and its Vulnerability

WPA is used to strengthen security because of the weaknesses of WEP. One of the most simple way is WPA-PSK. In this case the use of WPA is similar with WEP, although using WPA can obtain higher security including stronger authentication and better encryption.

WPA-PSK cannot be broken by intercepting many packets as WEP, but it is possible as long as 4-way handshake packets are obtained. From figure 3, we can know that SSID, AP_MAC, STATION_MAC, SNonce, ANonce, 802.1x data and MIC are included in 4-way handshake packets. And we also know the MIC is derived from the combination of the other six data and WPA-PSK key by using three hash algorithms (pdkdf2_SHA1, SHA1_PRF, HMAC_MD5). Through these theories, we can use dictionary attack to break WPA-PSK. First, a password dictionary is composited by possible passwords. And then using the password of the dictionary, SSID, AP_MAC, STATION_MAC, SNonce, ANonce and 802.1x data we can compute a new MIC (MIC') through pdkdf2_SHA1, SHA1_PRF and HMAC_MD5. Finally, if we find some MIC' equals with the original MIC, WPA-PSK is broken.

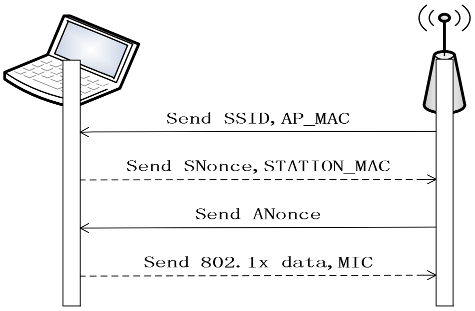


Figure 3 the 4-way handshake of WPA-PSK

IV. Design and Analysis of the Defence

A. *Design and Analysis of the defence against WEP attack (d-WEP)*

The d-WEP is designed to prevent the active attack against WEP in accordance with the ARP packets before connection established. First of all, we intercept the ARP data packets within the scope of the LAN by using the ARP hooks of the netfilter and according to the client IPs of these packets to check whether the AP is attacked. The specific program is as follows: First, there are three lists (IPList_Normal, IPList_Suspect, IPList_Attack) to store IPs and the corresponding frequency of each IP. And they are used to store the legitimate clients' IPs, the suspicious IPs and the IPs which are identified as attack IPs. When a data packet is intercepted, its IP is extracted to determine which list it belongs to. If it belongs to the IPList_Normal and its access frequency is less than the default, the data packets will be processed normally. Or it will be moved the IPList_Suspect list. If the IP is found in IPList_Suspect list and according to the access frequency, it will be determined to be moved to the IPList_Normal list or the IPList_Attack list. Finally, if the IP is searched in IPList_Attack list, this packet will be dropped immediately and after some certain time, the corresponding IP will be shifted to the IPList_Suspect list. And if one IP is entered the IPList_Attack list again in a short time, it will be disable for a longer time. Next we will indicate the feasibility of the design.

Through the results coming for the attacks on WEP using the software such as aircrack-ng, we have found the active attack is a kind of injection attacks. That is, an attacker broadcasts the ARP request eavesdropped from the legitimate client or forged to the local network. And the AP in the local network would response to these ARP requests. In this way, attacker can eavesdrop these responses and intercept the IV inside. The accordance of our design is based on this consideration. When receiving the ARP packets considered invalid, their responses will not be sent. So the attacker cannot eavesdrop the packets as expected. Since the loss of high-speed characteristics of packet interception, the active attack loses the original meaning and is no longer feasible. Thus our design is available in theory. And we will experiment to illustrate this point in the following sections.

B. *Design and Analysis of the defence against WPA-PSK attack (d-WPA-PSK)*

In order to improve the WPA-PSK authentication, we proposed a mechanism named d-WPA-PSK. First, a key generator, which is used to provide different PSKs according to different seeds, is distributed to AP and all legitimate clients. And then AP will broadcast a random seed to around clients after a certain period of time. Next the client receiving the seed will send a feedback to AP to let AP know the client already has this seed. When all clients associated with AP obtain the seed, AP and all clients will generate a new PSK in accordance with the key generator distributed in advance using the seed from AP. Finally, AP and all clients will re-set the network configuration using this new PSK. With PSK regularly updated, to some extent, the security of WPA-PSK will get some improvement, which will be analysed in the following.

When traditional dictionary attack is used to attack WPA-PSK, about 4~23 days are needed to crack a password of length 5 and at least 282110990 days are spent to get a password of length of more than 10. It is clear that it is impossible to break the WPA-PSK. However, with the emergence of 'table', the crack speed has been increased by 200~3000 times. This is because a way of pre-processing approach is proposed to compute the hash of each key in the dictionary. We can know it is possible because of the vulnerability of the WPA-PSK mentioned in the previous section. With all of these data, we can analyze the time needed to crack a WPA-PSK password. Next we can set the update period of PSK based on the time required to attack to achieve such an effect that our PSK will be replaced before being broken. Therefore d-WPA-PSK has a certain degree of significance in preventing the attacks on WPA-PSK.

V. Implementation and Performance Evaluation of d-WEP

First of all, the main data structure used is shown including the netfilter and the sk_buff. Next, the realization of the d-WEP is mainly introduced. Finally, we do the performance evaluation of d-WEP.

A. *Netfilter*

Netfilter including packet filtering, packet processing and NAT is a function framework, which has several characteristics as follows: For each network protocol netfilter defines a set of monitoring points and hook functions. The hook functions are called when data packets flow through the monitoring points of the packet stack. What's more, multiple hook functions registered in the same detection point are allowed, and the netfilter uses the priority mechanism to control the order of the implementation of the hook functions. In this way the expansion of the netfilter is guaranteed. In our experiment two check points on ARP is used, they are shown in figure 4.

Specific definition is as follows:

NF_ARP_IN: ARP packets prior to ARP process go through this point.

NF_ARP_OUT: This checkpoint can intercept ARP packets sent to network.

B. *Sk_buff*

In network coding sk_buff is the most important data structure that contains many members available for the various subsystems, which is used to indicate the header information of

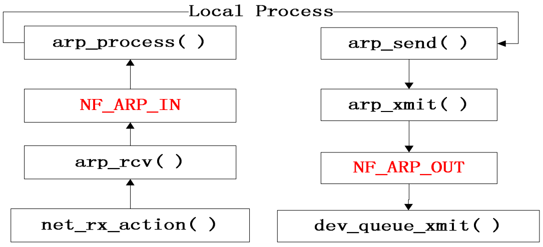


Figure 4 the Structure of the Hook Functions on IPV4 the packets received and the packets to be sent. It is a two-way linked list shown in figure 5. For easy call, an auxiliary node is inserted before the first node of sk_buff.

C. *Implementation of d-WEP*

There are three lists in d-WEP, which are introduced in the design of d-WEP. The process of implementation of d-WEP is shown in Figure 6.

D. *Performance Evaluation of d-WEP*

Based on the soft AP using the hostap driver of linux with the d-WEP module is loaded, we do the attack using the tool of aircrack-ng. From the result in Figure 7, the dropped packets from the attack show that we achieve the defence against the active attack on WEP successfully.

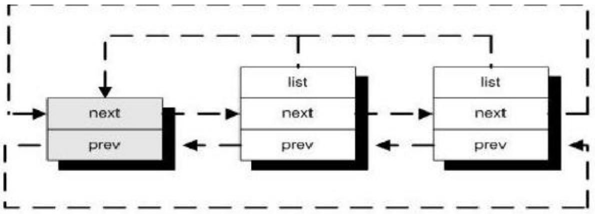


Figure 5 Organizational Structure of sk buff

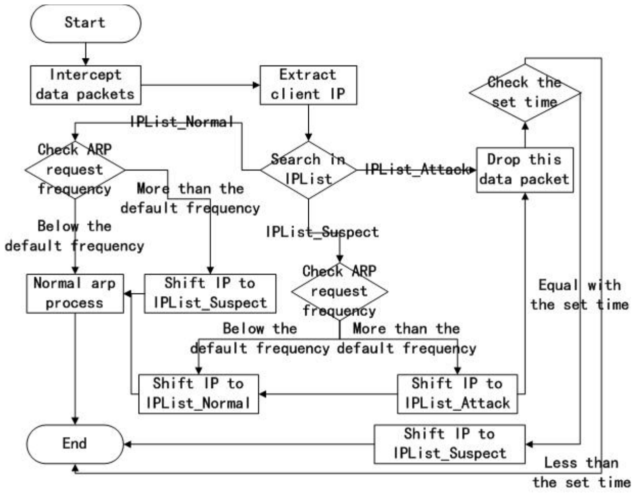
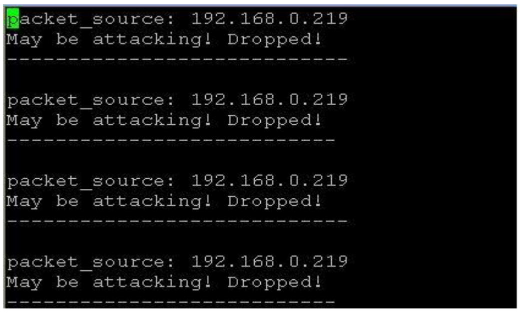

Start
Intercept data packets
Extract client IP
Check the set time
IPList_Normal
Check ARP request frequency
Search in IPList
IPList_Attack
Drop this data packet
More than the default frequency
Below the default frequency
IPList_Suspect
Normal arp process
Shift IP to IPList_Suspect
Check ARP request frequency
Equal with the set time
Below the default frequency
More than the default frequency
Shift IP to IPList_Normal
Shift IP to IPList_Attack
End
Shift IP to IPList_Suspect
Less than the set time

Figure 6 the implementation of d-WEP



```
packet_source: 192.168.0.219
May be attacking! Dropped!
---------------------------

packet_source: 192.168.0.219
May be attacking! Dropped!
--------------------------

packet_source: 192.168.0.219
May be attacking! Dropped!
---------------------------

packet_source: 192.168.0.219
May be attacking! Dropped!
--------------------------
```

Figure 7 the running result of d-WEP

VI. CONCLUSION

On the basis of the analysis of the existed attacks, especially the attack on WEP, and as well as the dictionary attack on WPA-PSK, we proposed the experimental program of d-WEP and d-WPA-PSK. The d-WEP employs such a technical that the frequency of ARP requests on AP is restricted in a certain range. In this way we determine whether there are attacks by detecting this frequency. In addition, the frequency is easily computed. This primary advantage can effectively prevent the active attack on WEP. And according to the experimental result, we indeed do this in the experimental scene. According to theoretical analysis, the WPS-PSK can prevent the dictionary attacks by regular replacement of PSK which is generated by a key generator distributed to all clients in advance. But there also are some problems to be made better. First, in d-WEP, with the frequency bound to IPs, some valid clients may be prohibited. What's more, the passive attack cannot be dealt with. So we will improve d-WEP and implement the d-WPA-PSK in our future work.

REFERENCES

[1] ANSI/IEEE standard 802.11i., "Amendment 6 Wireless LAN Medium Access Control (MAC) and Physical Layer (phy) Specifications", Draft 3. (2003).

[2] Bittau, A., Handley, M., Lackey, J., "The final nail in WEP's coffin", IEEE Symposium on Security and Privacy, pp. 386–400, (2006).

[3] [3] Erik T., Martin B. T., "Practial attacks against WEP and WPA", ACM WiSec 2009, pp. 79-85, (2009).

[4] [4] Erik T., Ralf-Philipp W., Andrei P., "Breaking 104 Bit WEP in Less Than 60 Seconds", Lecture Notes in Computer Science, vol. 4867/2008, pp. 188-202, (2008).

[5] [5] Fluhrer, S., Mantin, I., Shamir, A., "Weaknesses in the key scheduling algorithm of RC4", LNCS, vol. 2259, pp. 1–24, (2001).

[6] [6] Hassan, H. R., Challal, Y., "Enhanced WEP: An efficient solution to WEP threats", WOCN, pp. 594-599, (2005).

[7] [7] Lashkari, A. Mansoor, M. Danesh, A., "Wired Equinalent Privacy versus Wi-Fi Protected Access(WPA)", International Conference on Signal Processing Systems. pp. 445-449. (2009).

[8] [8] Paul, G., Rathi, S., Maitra, S., "On non-negligible bias of the first output bytes of RC4 towards the first three bytes of the secret key", International Workshop on Coding and Cryptography, pp. 285–294, (2007).

[9] [9] Serge V., Martin V., "Passive-Only Key Recovery Attacks on RC4", Lecture Notes in Computer Science, vol. 4876/2007, pp. 344-359, (2007).

[10] [10] Wen-Chuan H., Yi-Hsien C. Chi-Chun L., "An Interference-Based Prevention Mechaniam Against WEP Attack for 802.11b Network", IFIP International Federation for Information Processing, vol. 165/2005, pp. 127-138, (2005).