An Innovative Wireless Network Security for Air force Using WEP, WAP and WPA2

A.ANTONY VINOTH KUMAR,
M.E Applied Electronics,
Department of Electronics and Communication,
Einstein College of Engineering,
Anna University.
search.antony@gmail.com.

C.KARTHIKEYAN,
Assistant Professor
Einstein College of Engineering,
Anna University,
karthik.mit2006@gmail.com

Abstract -- The objective of this paper is to prevent the attackers against the WEP in wireless networks. Wirelesses Local Area Networks (WLANs) have become more prevalent and are widely deployed in many popular places like university campuses, cafés, airports, residences, etc. However, WLAN security is a very important but usually neglected issue. Focusing on three major types of typical wireless security standards: WEP, WPA and WPA2, we aim to explore the current state-of-the-art in security protocols and to present an overview of their real-life vulnerabilities by issuing successful attacks against WEP and WPA-protected WLANs

Index Terms: WLAN (Wireless LAN), WEP (Wired Equivalent Privacy), WPA2 (Wi-Fi Protected Access 2), ATTACK WEP, ATTACK WPA2.

I. INTRODUCTION

The IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. Such networks are met frequently in typical home or office facilities. The first IEEE 802.11 standard came with a basic protecting mechanism called Wired Equivalent Privacy (WEP). WEP requires all clients and access points (APs) in the network to share up to four different secret symmetric keys. This makes difficult the implementation of a larger installation, where users change frequently, and that's the reason why most installations use a single secret key named root key. WEP has some major drawbacks and was hacked in 2001 by Fluhrer, Mantin, and Shamir . They showed that an attacker may recover the secret key of a network with an average consumer laptop in an average of 1-2 hours. Nowadays, it is possible to recover the secret key in less than 60 seconds.

II. LITERATURE REVIEW

In that existing system WEP protocol is used to overcome the attackers. The WEP protocol uses the RC4 algorithm for confidentiality and the CRC-32 checksum for integrity. The resulting key is used as an input, the so called 'seed', for a Pseudo-Random Number Generator (PRNG) that yields a key sequence equal to the length of the plaintext plus the Integrity Check Value (ICV). The result of the key sequence and the ICV will go to RC4 algorithm.

Wires Equivalent Privacy (WEP) is used to improve the security of wireless LAN (WLAN). By analyzing the weaknesses of WEP and RC4, we design a simulative platform including software and hardware to crack WEP keys. The results show that the WLAN based on WEP is insecure. At last we give some improvements to enhance the WLAN security

WEP (Wired Equivalent Protocol) is a wireless security protocol ratified by IEEE (The Institute of Electrical and Electronics Engineers) in 1999. Since then, WEP is widely used in telecommunication field. In daily usage, it had been phased-out by IEEE since 2005 to be replaced by WPA/WPA2 (Wi-Fi Protected Access). WEP encryption algorithm can be easily cracked because of its widely documented weaknesses. Nevertheless, WEP is still has been used extensively as a research topic in the academic field. Certain enterprises still using WEP due to lack of security consciousness, economical constraint or because it is difficult to replace the legacy communication devices in which WEP is already bulged. In this paper, we give a review on WEP wireless security protocol in terms of its history, weaknesses, improvements, and current alternative approaches to overcome its weaknesses regarding the protocol in ICT (Information and Communication Technology) field. This research aims to address WEP protocol in its current versions and to give a spirit future direction research to enhance its security mechanism.

III. METHODOLOGY

The WEP protocol had some serious security problems, such as: it does not prevent forgery of packets, it does not prevent replay attacks, it uses RC4 improperly, because the keys used are very weak and can be brute-forced on standard computers in hours to minutes, it allows an attacker to undetectably modify a message without knowing the encryption key, etc.. The WPA came with the purpose of solving the problems in the WEP cryptography method, without the need to change the hardware.

III.1 Creating Protocols

A. The WEP protocol

The WEP protocol uses the RC4 algorithm for confidentiality and the CRC-32 checksum for integrity. At first, the secret key used is 40-bit long with a 24-bit Initialization Vector (IV) that is incorporated to it for acting as the encryption/decryption key resulting in a 64-bit total key size. Then the resulting key is used as an input, the so called 'seed', for a Pseudo-Random Number Generator (PRNG) that yields a key sequence equal to the length of the plain text plus the Integrity Check Value (ICV). The result of the key sequence and the ICV will go to RC4 algorithm. A final encrypted message is made by attaching the IV in front of the cipher text. Also the key may be 128-bit long, the only difference is that the secret key size becomes 104 bits and the IV remains 24 bits. For the WEP decryption, the IV of the incoming message and the Pre-Shared Key is used to generate the key sequence necessary to decrypt the incoming message. Thereafter the cipher text and Secret key go to RC4 algorithm and a plain text comes as a result. Next, the plaintext goes to Integrity Algorithm to make a new ICV (ICV') and finally the new ICV (ICV') compares with the original ICV.

B. The WPA protocol

The standard WPA specifies two operation manners:
1) Personal WPA or WPA-PSK (Pre-Shared Key)which is used for small office home and domestic use, it does not use an authentication server and data cryptography key can go up to 256 bits. Unlike WEP, this can be any alphanumeric string and is used only to negotiate the initial session with the AP. Because both the client and the AP already possess this key, WPA provides mutual authentication, and the key is never transmitted over the air.
2*) Enterprise or Commercial WPA* in which the authentication is made by an authentication server 802.1x, generating excellent control and security in the users' wireless network traffic. This WPA uses 802.1X+EAP for authentication, but also replaces WEP with the more advanced TKIP encryption. No pre shared key is used here, but you will need a RADIUS server. And you get all the other benefits 802.1X+EAP provides, including integration with the Windows login process and support for EAP-TLS and PEAP authentication methods. One of the benefits of WPA is that it allows a more complex data encryption on the Temporal Key Integrity Protocol (TKIP) and it is also assisted by MIC (Message Integrity Check), whose function is to avoid bit-flipping type attacks which can easily be applied to WEP by using a hashing technique.

C.WPA2 Protocol

An 802.1X wireless setup consists of three main components:

1. Supplicant (the wireless client).
2. Authenticator (the AP).
3. Authentication server (usually a RADIUS server).

The supplicant initially connects to the authenticator, as it would to a WEP or WPA protected network. Once this connection is established, the supplicant has in effect a network link to the authenticator (AP). The supplicant can then use this link to authenticate and gain further network access. The supplicant and authenticator first negotiate capabilities. These consist of three items:
· The pair wise cipher suite, used to encrypt uni cast (point-to-point) traffic.
· The group cipher suite, used to encrypt multicast and broadcast (point-to-multiple-points) traffic.
· The use of either a pre-shared key (PSK, or "home user" security, using a shared secret) or 802.1X authentication.
So, the main problem of WPA is solved by dividing the type of security to three categories where just one of them uses pair wise and the two others use group cipher and pre shared key.

IV. RESULTS AND DISCUSSION

Attacking a WEP Network:

WEP cracking can easily be demonstrated using tools such as Air crack

1. Air crack contains three main utilities, used in the three attack phases that take place to recover the key:
• Airo dump: wireless sniffing tool used to discover WEP enabled networks,
• Aire play: injection tool to increase traffic,
• Air crack: WEP key cracker using collected unique IVs.

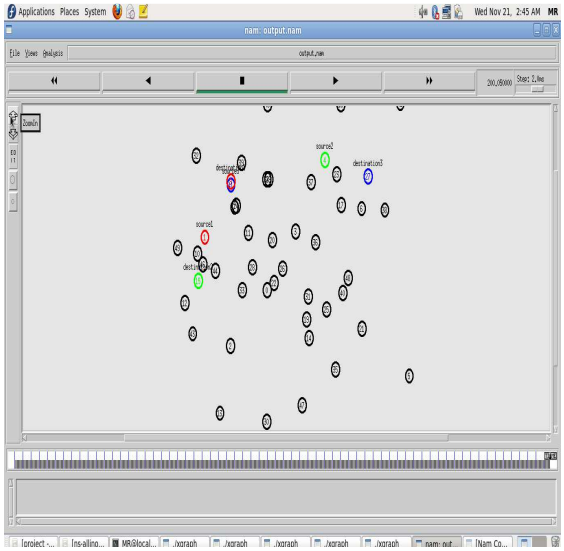

Figure1: Web network

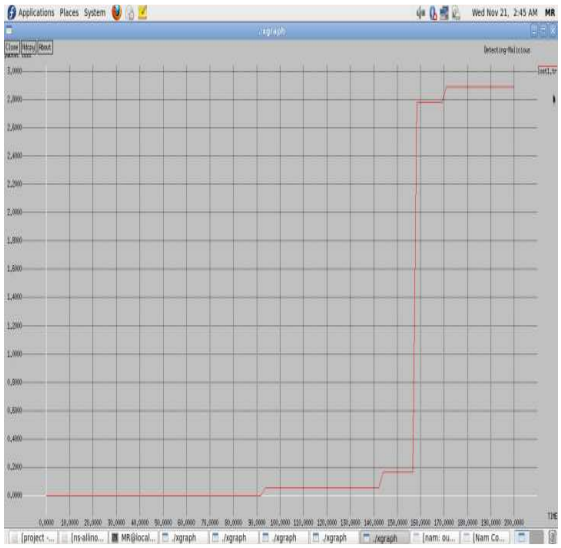

Figure 2: Packet loss

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is distinguished as one of the three main error types encountered in wireless communications; the other two being bit error and spurious packets caused due to noise

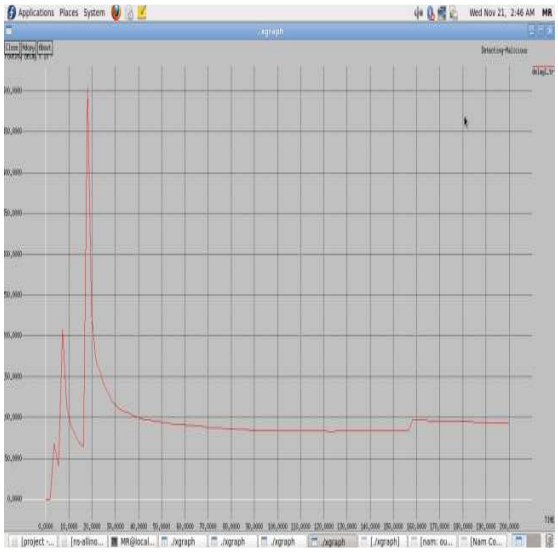

Figure 3:Routing delay

IV.2 Attack Against aWPA2 Network:

A. Four-Way handshake capture

The first step is to start the wireless interface in monitor mode on channel 6, the one the AP uses. Then we start airodump-ng to collect the four-way authentication handshake.

One client, identified by the MAC address is associated and authenticated on this wireless network (meaning that the Four-Way Handshake has already been done for this client). This client will subsequently be disassociated, forcing him this way to initiate a new association and allowing us to capture Four-Way Handshake messages.

The "aireplay" command will be used for this attack and this will disassociate the selected client with the specified BSSID by sending a fake disassociation request. If there was no wireless client currently associated with the AP, then we had to be patient and wait for one to connect to the AP so that a handshake can be captured.

B. Dictionary Attack

The dictionary attack is using a wordlist. Based on our observations, the factory set, default password of Net Faster routers has the following format: "[MAC address]-[a four-digit random number]", so we can generate the suitable wordlist using a program called Crunch. Knowing the router's MAC address, which allows us to use a wordlist containing only 10.000 words, i.e. equal to the amount of all different four-digit number combinations

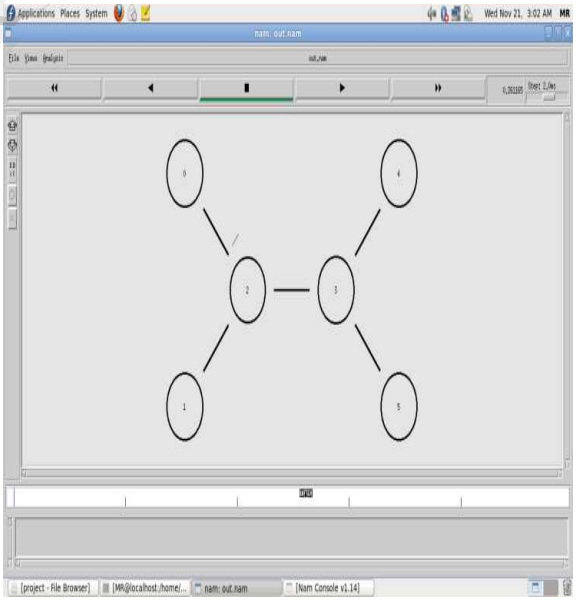

Figure 4: WPA2 Network

V. CONCLUSION

It presented in detail an analytical procedure towards WEP and WPA2 cracking, derived from real-life situations. Our motivation was the need for increased wireless security and the common feel that nowadays WPA/WPA2 security protocols are difficult for a stranger to hack.

REFERNCES

[1] IEEE-SA Standards Board, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Communications Magazine, 2007
[2] S. R. Fluhrer, I. Mantin, A. Shamir, Weaknesses in the key scheduling algorithm of RC4, in S. Vaudenay, A. M. Youssef (eds.),Selected Areas in Cryptography 2001, LNCS Vol. 2259
[3] A. Stubbleeld, J. Ioannidis, A. D. Rubin, A key recovery attack on the802.11b wired equivalent privacy protocol (WEP), ACMTransactions on Information and System Security, May 2004
[4] E. P. Weinmann, A. Pyshkin. In S. Kim, M. Yung, H.-W. Lee (eds.), WISA, LNCS Vol. 4867, Springer, 2007.
[5] A. H. Lashkari, F. Towhidi, R. S. Hoseini, "Wired Equivalent Privacy (WEP)", ICFCC Kuala Lumpur Conference, 2009
[6] D. C. Plummer, RFC 826: Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware, November 1982
[7] IEEE Standards Board. 802 part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY). Specification. IEEE Standard 802.11, 1999 Edition
[8] WANG S M, TAO R, WANG Y. WLAN and Its Security Problems[R]. Proceeding of the Fourth International Conference on Parallel and Distributed Computing, 2003:241-244
[9] Christian Barnes, Tony Bautts. Hack Spoofing Your Wireless Network [M]. Syngress Press, 2002
[10] Scott Fluhre , Itsik Mantin, and Aid Shamir. Weakness in the Key Scheduling Algorithm of RC4. Eight Annual Workshops on Selected Areas in Cryptography, August2001
[11] Adam Stubblefield, John Ioannidis, Aviel D, Rubin, "Using the Fluhrer, Mantin, and, hamir Attack to Break WEP", 2001, AT&T Labs Technical Report TD-4ZCPZZ