Wi-Fi Security with Wi-Fi Protection Plus

Ajin Abraham, Joseph Sebastian
Vimal Jyothi Engineering College.
ajin25@gmail.com
+91-9633325997
josephs_18@live.com
+91-9495587202

Abstract

Current Industrial standards of Wi-Fi security are found to have security loop holes, making it possible for hackers to break it. So we consider the possibility of a new technology for Wi-Fi security. We call it Wi-Fi P+ or Wireless Fidelity Protection Plus

Introduction

Wi-Fi is common nowadays. Every educational institutions and business organizations has got their perimeter covered in Wi-Fi. All the confidential data being transmitted through Wi-Fi, makes it a target for Hackers. To secure it, some Wi-Fi security standards like WEP, WPA, and WPA2 are introduced. Each of them is introduced when the previous security architecture was found to be a failure. But in present situation all of these industrial standard Wi Fi security architectures are found to have vulnerabilities so that a hacker can hack into the Wi Fi network. After conducting a study and analysis of the vulnerabilities of current Wi Fi Security industrial standards, we consider the possibility a new security architecture for Wi Fi which we call Wi Fi P+. Wi-Fi P+ is not a complex security architecture. It act as an additional security layer implemented over WPA/WPA2. It also implements some already available features that are not built in with WPA/WPA2.

Vulnerabilities in Current Wi-Fi Security Standards

The current Wi-Fi Security standards are

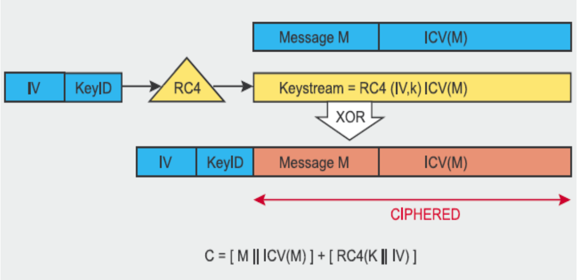
- WEP – Wired Equivalent Privacy
- WPA– Wi-Fi Protected Access
- WPA2 – Wi-Fi Protected Access 2

Vulnerabilities in WEP

WEP (*Wired Equivalent Privacy*) is based on the RC4 encryption algorithm, with a secret key of 40 bits or 104 bits being combined with a 24-bit *Initialization Vector* (IV) to encrypt the plaintext message *M* and its checksum – the ICV (*Integrity Check Value*). The encrypted message *C* was therefore determined using the following formula:

C = [M || ICV(M)] + [RC4(K || IV)]

Where || is a concatenation operator and + is a XOR operator. Clearly, the initialization vector is the key to WEP security, so to maintain a decent level of security and minimize disclosure the IV should be incremented for each packet so that subsequent packets are encrypted with different keys. Unfortunately for WEP security, the IV is transmitted in plain text and the 802.11 standard does not mandate IV incrimination, leaving this security measure at the option of particular wireless access point implementations.


Message M
ICV(M)
IV
KeyID
RC4
Keystream = RC4 (IV,k) ICV(M)
XOR
IV
KeyID
Message M
ICV(M)
CIPHERED
C = [M || ICV(M)] + [RC4(K || IV)]

The WEP protocol was not created by experts in security or cryptography, so it quickly proved vulnerable to RC4 issues described by David Wagner four years earlier. Then a lot of vulnerabilities were discovered during the later years. Some of them are:

Date	Description
September 1995	Potential RC4 vulnerability (Wagner)
October 2000	First publication on WEP weaknesses: *Unsafe at any key size; An analysis of the WEP encapsulation* (Walker)
May 2001	An inductive chosen plaintext attack against WEP/WEP2 (Arbaugh)
July 2001	CRC *bit flipping* attack – *Intercepting Mobile Communications: The Insecurity of 802.11* (Borisov, Goldberg, Wagner)
August 2001	FMS attacks – *Weaknesses in the Key Scheduling Algorithm of RC4* (Fluhrer, Mantin, Shamir)
August 2001	Release of AirSnort
February 2002	Optimized FMS attacks by h1kari
August 2004	KoreK attacks (unique IVs) – release of chopchop and chopper
July/August 2004	Release of Aircrack (Devine) and WepLab (Sanchez) implementing KoreK attacks

The WEP Cracking tool released on 2004, Aircrack was able to crack 128 bit WEP key.

Vulnerability in WPA and WPA2

The most practical vulnerability is the attack against WPA/WPA2's PSK key. The PSK (*Pre-Shared Key*) same as PMK (*Pairwise Master Key*) is a string of 256 bits or a passphrase of 8 to 63 characters used to generate such a string using a known algorithm: PSK = PMK = PBKDF2(password, SSID, SSID length, 4096, 256), where PBKDF2 is a method used in encryption, 4096 is the number of hashes and 256 is the length of the output. The PTK (*Pairwise Transient Key*) is derived from the PSK using the *4-Way Handshake* and all information used to calculate its value is transmitted in plain text. The strength of PTK therefore relies only on the PSK value, which for PSK effectively means the strength of the passphrase. The second message of the *4-Way Handshake* could be subjected to both dictionary and brute force offline attacks. The cowpatty utility was created to exploit this flaw, and its source code was used and improved by Christophe Devine in Aircrack to allow PSK dictionary and brute force attacks on WPA.

Threats on Wi-Fi

Ad-hoc networks

Ad-hoc network can pose to high security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

MAC Spoofing

MAC spoofing occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to only allow authorized computers with specific MAC addresses to gain access and utilize the network. However, a number of programs exist that have network "sniffing" capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.

Man-in-the-middle attacks

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a "de-authentication attack". This attack forces AP-connected computers to drop their connections and reconnect with the cracker's soft AP.

Denial of service

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash.

Caffe Latte attack

The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.

War driving

War driving is the act of searching for open Wi-Fi networks by a person in a moving vehicle using a portable computer, smartphone or PDA.

Need for a New Security Architecture

Wi-Fi is widely used in different institutions and terabytes of confidential data are being transmitted through it. These data include everything from contacts/clients information, patented data, trade secret, legal and financial information. So it's a target for hackers. Since the PSK vulnerability exists in WPA and WPA2, if the passphrase is not strong enough then it is easy for a hacker to decrypt the key using cowpatty or Aircrack. So the institution is under the threat of confidential data theft. So a new security architecture should be implemented that can safe guard from this attack and data theft.

Solution is Wi-Fi P+

The WPA/WPA2 is vulnerable because all the information required for the generation of Pairwise Transient Key (PTK) formed from Pre-shared Key (PSK) is transmitted in plain text. Hackers can do dictionary attack or brute force attack on the plain text data to get the password key. So here comes the need of Wi-Fi P+. Wireless Fidelity Protection Plus adds up an additional security layer for WPA/WP2 by encrypting the plain text information transferred from PMK. It uses a simple but powerful encryption method given by the equation:

P-PMK = PMK + (256 bit random protection key)

Where P-PMK is the protected PMK and '+' is XOR operator. Here we are doing the XOR operation of plaintext information derived from PMK and a randomly generated number, simply generated using a random() function which makes this encryption method simple, fast and almost solid secure since it is almost impossible to decrypt 256 bit random numbers even by performing a dictionary attack or brute forcing with a super computer. Wi-Fi P+ also imparts additional inbuilt security features like:

- MAC address filtering allows the administrator to restrict the access to a Wi-Fi network based on MAC address. By implementing MAC address filtering, the computers with MAC addresses allowed by the administrator can only connect to the Wi-Fi network.

- MAC Spoofing detection by wireless Intrusion Detection System.

- Logging Wi-Fi users. The IP address, MAC addresses as well as computer name and operating system name is logged.

- Network Encryption using simple random key. This encryption method doesn't make your data transfer slow as it uses simple and fast random key encryption.

- Wi-Fi range limiting can be implemented with Wi-Fi P+.

- Controlling of Wi-Fi sharing by the users who are under a Wi-Fi network. Administrator can restrict peer to peer Wi-Fi sharing by genuine users under the Wi-Fi network.

- DOS attack discovery and blacklisting the attacker.

- Using Static IP instead of Dynamic IP. Disabling at least the IP Address assignment function of the network's DHCP server, with the IP addresses of the various network devices then set by hand will also make it more difficult for a casual or unsophisticated intruder to log onto the network.

- Built-in Honey Pot for intrusion and attack detection. Honey Pots are traps, waiting for hackers, which seems to be vulnerable, but actually traps the attacker and reveals his identity.

- VPN (Virtual Private Network) for data security and privacy. It is a credible and a popular way for securing data in wireless transmissions.

Implementation of Wi-Fi P+

Implementation of Wi-Fi P+ on an existing WPA/WPA2 is simple. It can act as an add-on for the router firmware. It can be installed along with the router firmware.

Conclusion

Current dominant standards of wireless security are found to be vulnerable even with their complex security architecture and here comes the importance of Wi-Fi P+ with its flaw less secure layer along with other additional protective features, ease of use and implementation makes it a good option for organizations, where secure data transmission is a concern.

References & Bibliography

- Wi-Fi security – WEP, WPA and WPA2 -Guillaume Lehembre
- Avaya. Configuration and deployment of IPSec VPN security for 802.11 wireless
- The evolution of wireless security in 802.11
- networks: WEP, WPA and 802.11 standards-SANS institute
- Wireless Network Security
- 802.11, Bluetooth and Handheld Devices-Tom Karygiannis,
- Les Owens
- LANs. April 2002. URL: http://www.avaya.co.uk/Resource_Library/downloads/msn1710.pdf
- CERT. Configure firewall packet filtering. July 1999. URL: http://www.cert.org/security-improvement/practices/p058.html
- Cisco. Wireless LAN security white paper – Cisco Aironet 1200 series.
- URL: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml
- Geier Jim. OptimumPath secure access wireless router. August 28, 2003.
- URL: http://www.wifiplanet.com/reviews/AP/article.php/3070111
- Kelley Diana, Phifer Lisa. 802.11 Planet - WLAN security tutorial. June 2003.
- Marshall Trevor. Antennas Enhance WLAN Security.
- URL:
- http://www.winncom.com/html/wireless-trevormarshall.shtml
- Roberts Paul. Expert releases Cisco wireless hacking tool. April 8, 2004.
- URL: http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,92049,00.html
- Schafer Marlon. How to Pick the Right Antenna. 2001.
- URL: http://www.odessaoffice.com/wireless/antenna/how_to_pick_the_right_antenna.htm
- Symbol. Why ‘Not Broadcasting the SSID' is not a Form of Security. March 25,2003.

- URL: http://www.symbol.com/products/wireless/broadcasting_ssid_.html
- Wi-Fi Alliance. Wi-Fi protected access overview. October 31, 2002.
- URL: http://www.weca.net/OpenSection/pdf/WiFi_Protected_Access_Overview.pdf
- Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise- Wi-Fi Alliance
- The State of Wi-Fi® Security Wi-Fi CERTIFIED™ WPA2® Delivers Advanced Security to Homes, Enterprises and Mobile Devices- Wi-Fi Alliance
- URL: http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm
- URL: http://www.labnol.org/internet/secure-your-wireless-wifi-network/10549/
- URL: http://en.wikipedia.org/wiki/Pre-shared_key
- URL: http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm
- URL: http://compnetworking.about.com/cs/wirelessfaqs/f/adhocwireless.htm
- URL: http://compnetworking.about.com/cs/wirelessproducts/qt/macaddress.htm
- URL: http://en.wikipedia.org/wiki/Wireless security
- URL: http://compnetworking.about.com/od/workingwithipaddresses/qt/staticipaddress.htm
- URL: http://en.wikipedia.org/wiki/Wardriving