Gavin Garcia - 3577337, Melissa Cortes - 3217823, Leandro Ricardo - 2892107,
Max Tojeiro - 2932206, Rommel Rodriguez - 2352669, Samuel Soto - 2342980

Wi-Fi Security: Wireless Network Encryption
EEL 4789 - Ethical Hacking

Abstract

We will be analyzing a variety of different network encryptions and discussing how to breach said networks. We aspire to create an accurate and useful analysis of network standards and will suggest ways to improve these networks. Improvements proposed will be made using thorough research into the subject area. Each networking encryption standard will also be thoroughly discussed in the following paper.

Introduction

In this paper we are going to look at a few of the different network related securities that have come along since the Introduction of the Wireless Local Area Network (WLAN) and their various weaknesses.

Mainly we will be discussing topics varying from the open encryption to non-encryption methods which may depend on software encryption (https, etc...) to protect data. As well as the easily broken Wired Equivalent Privacy (WEP) and then the WiFi Protected Access (WPA) followed by the WiFi Protected Access II (WPA2) we are going to explore and discuss proper procedures for maintaining high levels of security in order to keep the user protected.

Wired Equivalent Privacy (WEP)

The first and original security for wireless access points that was created in 1997. In 2001 however it was discovered that WEP had serious flaws, those flaws being that a passive attack could be launched to decrypt traffic based on statistical analysis of the data stream, active attacks could be launched to inject malicious traffic from an unauthorized workstation, or to decrypt traffic based on simply tricking the access point. This was all possible as it used a stream cipher. Stream ciphers operate by expanding a specific key into an extremely long, random, false key. The sender and receiver receive similar keys then they’re converted to plain text. As long as both match, the data is secure. Decrypting said key though is something now of child’s play however.

WEP is generally no longer used anywhere as it has been far depreciated.
One of the reasons that wep is so easy to crack is that it uses a manually entered 40 or 104-bit encryption key. This is actually one of the first things improved upon in the WPA network. A standard WEP key normally concatenates a 24-bit initialization vector to form the RC4 key used

for confidentiality. The main problem with the encryption key is that it is manually entered unlike tkip which puts a temporary key for each packet of data.

One way to start breaching a WEP security network, is to use a packet-sniffing program on linux. It is better to use linux than windows because it can actually sniff WEP packets. One of the most commonly-used programs to accomplish this is backtrack. Through this program and several commands it is possible to find hidden SSID's and the type of encryption each network uses.

Wi-Fi Protected Access (WPA)

WPA is not its own form of new security. It was created to be a wrapper to WEP to safeguard WEP from the flaws that were found with it. It was never meant to be its own defining security standard, just a stop-gap until WPA2 was ready for deployment. WPA works in two secure modes. One being WPA-PSK and the other being WPA-Enterprise. The former is simply a pre-shared key, while the latter requires a RADIUS server and can be combined with an EAP (Extensible Authentication Protocol). WPA also generally uses TKIP, or Temporal Key Integrity Protocol, it is not an encryption protocol but it does make sure every packet of data is sent with a unique key, something that WEP desperately lacked. However, as most consumers simply use WPA-PSK, brute forcing the passcode was a quick and effective way of retrieving the specific user key. WPA is somewhat still used today in older systems that have not been migrated over to WPA2 mostly due to owner complacency.

There are flaws associated with WPA. In order to recognize these flaws it is important to understand the software capabilities. WPA includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or re-sending data packets. WPA uses a message integrity check algorithm called *Michael* to verify the integrity of the packets. However, *Michael* is not as strong as the algorithm used in WPA2. WPA relies on outdated weaknesses in WEP that can be exploited only for the TKIP algorithm and the limitations of *Michael* to retrieve the keystream from short packets to use for re-injection. This very WPA quality is what fuels one of its major security weaknesses. The flaw can only decrypt short packets with mostly known contents, such as ARP messages. The attack requires Quality of Service to be enabled, which allows packet prioritization as defined. "The flaw does not lead to recovery of a key, but only to recovery of a keystream that was used to encrypt a particular packet, and which can be reused as many as seven times to inject arbitrary data of the same packet length to a wireless client."

WPA and 802.11i provide for a Pre-Shared Key (PSK) as an alternative to 802.1X based key establishment. When a PSK is used instead of 802.1X, the PSK is the Pairwise Master Key

(PMK) that is used to drive the 4-way handshake and the whole Pairwise Transient Key (PTK) keying hierarchy. Anyone with knowledge of the PSK can determine any PTK in the ESS through passive sniffing of the wireless network, listening for key exchange data frames. Also, if a weak passphrase is used, for example, a short passphrase, an offline dictionary attack can readily guess the PSK. Since the common usage will be a single PSK for the ESS, once this is learned by the attacker, the attacker is now a member of the ESS, and the whole ESS is compromised. The attacker can now read and forge any traffic in the ESS.

802.11i standard (WPA2)

WPA2 is the proper follow up to WEP. It runs in the same modes as WPA, but instead of using TKIP, it uses CCMP for cryptographic encapsulation. CCMP was designed to have data completely confidential; this is based upon the Counter Mode with CCM (CBC-MAC) of the AES encryption standard. This is used to replace TKIP for message confidentiality and makes WPA lose many of its flaws. WPA2 is what is generally used now by default in most if not all consumer networks. It is the most secure, mainstream, security measure an average consumer can deploy. However its largest weak point would be the use of an easy passkey like “password” or “123456.”

In April 2003, the Wi-Fi Alliance introduced WPA based on draft 3 of the IEEE 802.11i amendment which was designed to replace the much weaker WEP encryption without requiring hardware replacements. At the time WPA used strong cryptography support from TKIP based on the RC 4 cipher. By leveraging the RC 4 cipher, the IEEE 802.11i task group was able to improve the security on legacy networks until the IEEE 802.11i amendment was completed. Although there have been no catastrophic security breaches reported on the WPA-TKIP protocol, it was only intended provide enough security for 5 years while organizations transitioned to the full IEEE 802.11i security mechanism.

WPA2 adopted many of the same encryptions methods used for WPA, but in addition implements the mandatory elements of IEEE 802.11i. WPA2 improves the security of Wi-Fi connections by requiring the use of stronger wireless encryption than what WPA requires. Specifically, WPA2 does not allow use of TKIP which has known security holes, but instead introduces CCMP, a new AES-based encryption mode with strong security. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and addresses the vulnerabilities present in WPA.

WPA was designed to work with wireless hardware produced prior to the introduction of

the WPA protocol, but the newer WPA2 is not supported on older hardware products. Beginning in 2004, certification by the Wi-Fi Alliance began and as of March 13, 2006 WPA2 is mandatory for all new devices to bear the Wi-Fi trademark. The current wireless security standard today is WPA2 which uses an encryption device that encrypts the network with a 256-bit key, improving security over WEP and WPA by having a longer key length.

Non-Encryption Methods

Unencrypted networks are usually found in coffee shops, libraries, airports, hotels, universities, and other public places and are convenient, free access points for users within their confines to be granted internet access. This complete lack of security makes it very easy to setup the network on a user's device, but at the same time, if the user is not using an encrypted site, their data can be easily read with something like WireShark which is completely free and works on all operating systems. This can lead to fraud and other financial complications for the user.

Service set identifier or more commonly knows as SSID, SSID is what your network uses to identify itself to local devices. If you prevent your network from broadcasting it's SSID to all local devices, said devices will not be able to see it readily available. Hence this in terms allows local users from being able to access the network without knowing it's SSID first. This however has many shortcomings as one can easily find an SSID without having it be broadcasted by the network.

Another non-encryption method is MAC ID filtering, this form of filtering allows you to specify a set MAC address from your device and allow it on the unsecured network. Since MAC addresses are unique this can be considered a good precaution to have on smaller networks. However due to a criminal possibly sniffing out a valid MAC address and then using MAC address spoofing, criminals can ultimately pretend to be a pre-approved MAC address and gain access to your network.

Static IP addressing allows you to filter out casual users by making a technical barrier a requirement, this barrier being that the user must assign himself a static ip. However this provides little to no protection as would be hackers, know how to do such things as well as they know breathing and sleeping.

Conclusion

There are many ways for data to be compromised and in order to reduce the risk of delicate information falling into the wrong hands. We must follow proper procedures that help

reduce the chances of this occurring. This can be accomplished by using the safest network encryption currently available, In this case said encryption is WPA2. WPA2 contains a crucial flaw though, it's users password. For WPA2 to function correctly users must must take the extra time to set up their network with a strong password. Once this is done it can make it almost impossible for potential hackers to break into said private networks, hence preserving your information from outside access.

Although there isn't a way to ever make data 100% secure, whether it be digital or analogue, you can make it as difficult to obtain by others as possible. This combined with user knowledge goes a long way in the digital security world and in other aspects of our life as well.

References

1. Wi-Fi Security: Cracking WPA With CPUs, GPUs, And The Cloud
http://www.tomshardware.com/reviews/wireless-security-hack,2981-6.html
2. EC Council . *Network Defense: Security Policy and Threats*. Cengage Learning, 2010. eBook.

3. Major Wireless Network Security Breach – Wi-Fi Protected Setup (WPS Bug) PIN Brute Force Vulnerability – Reaver http://www.safegadget.com/72/major-wireless-network-vulnerability-wps-bug/

4. Phifer, Lisa. An Introduction to Wireless Security http://searchsecurity.techtarget.com/feature/An-introduction-to-wireless-security

5. Edney, Jon, and William A. Arbaugh. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Addison-Wesley Professional, 2005. Print.

6. "Simple Wireless Security For Home". Retrieved 2010-03-10.

7. George Ou, "The six dumbest ways to secure a wireless LAN", March 2005, ZDNet

8. Wright, Joshua. "Explaining WPA2." *Network World*. N.p., 11 Sept. 2006. Web. 07 Feb. 2014. <http://www.networkworld.com/columnists/2006/091106-wireless-security.html>.

9. "Wi-Fi Protected Access." *Wikipedia*. Wikimedia Foundation, n.d. Web. 07 Feb. 2014.

<http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA2>.

10. "A Brief History of Wireless Security | Security Uncorked." *Security Uncorked*. N.p., n.d. Web. 7 Feb. 2014. <http://securityuncorked.com/2008/08/history-of-wireless-security/>

11. "Understanding WEP Weaknesses." - *For Dummies*. N.p., n.d. Web. 7 Feb. 2014. <http://www.dummies.com/how-to/content/understanding-wep-weaknesses.html>.