Wireless Network Security

Survey Paper

Kevin Kuo
Department of Computer & Information Sciences
Towson University
Towson, USA
kkuo1@students.towson.edu

***Abstract*—There has been an increased demand for wireless networks due to the proliferation of laptop computers and mobile devices such as smart phones, tablets, and watches. With the development and release of new wireless devices as well as improvements in wireless technology, wireless security has been increasingly important. This survey paper will explore the improvement made to wireless security and make suggestions where future effort should be directed.**

Keywords—Open System authentication; Access Point; Association Request; Wireshark; Service Set Identifier (SSID); NetStumbler; Kismet; Raw monitoring (RFMON) mode; Wired Equivalent Privacy (WEP); Kali Linux; Offensive Security; Metasploit Framework; Airmon-ng; Airodump-ng; Aircrack-ng suite; Aireplay-ng; Wireless Local Area Network (WLAN);Wi-Fi Protected Access (WPA); Wi-Fi Protected Access II (WPA2); Wi-Fi Protected Access-Enterprise (WPA-Enterprise)

I. Introduction

Wireless network connections are quickly becoming the most common way to connect personal devices to the network for Internet connectivity. Wireless network are a part of daily life. They are prevalent in cafes, bookstores, airports, fitness gyms, work places, restaurants, etc. Wireless is synonymous with mobile devices such as cell phones and tablets. We did not get to today's implementation of wireless networks without having learned some invaluable lessons along the way. The goal of this survey paper is to research existing protocols of wireless security and how the latest standard can be improved.

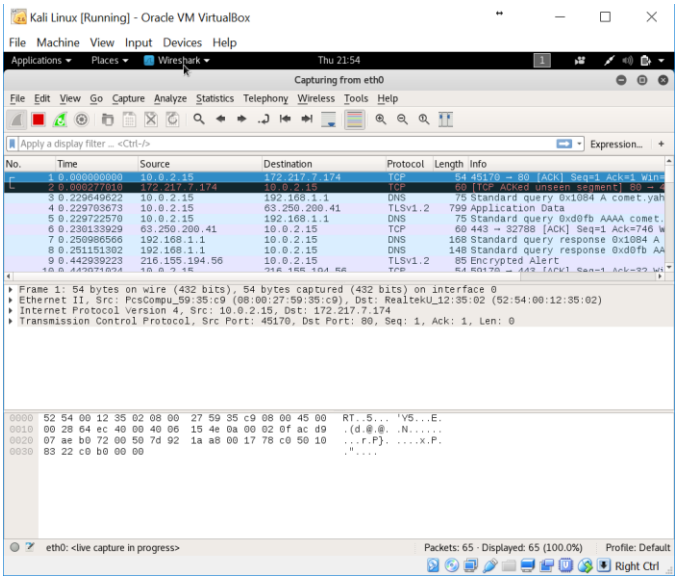
II. Methodology

A. Open System Authentication

Open System authentication is the default authentication protocol for 802.11. It authenticates anyone requesting authentication. A client will send an authentication request to an Access Point and the Access Point responds with an authenticate response. The client then sends an Association Request to which the Access Point replies with an Association Response. The connection between the client and Access Point is then established.

1) Tools – Wireshark: Wireshark is an open source multi-platform graphical user interface network traffic analysis tool that can be used to capture wireless network packets. With an open an unsecured wireless network, an actor can eavesdrop and capture all packets transmitted among clients of wireless network. Any data within those packets that is not ecrypted at the application level will appear as plaintext. For example, if a user were to log into a server using Telnet over an open wireless network connection, the username and password would be exposed and parsed by Wireshark or any other network traffic analysis utility.

Figure 1: Wireshark

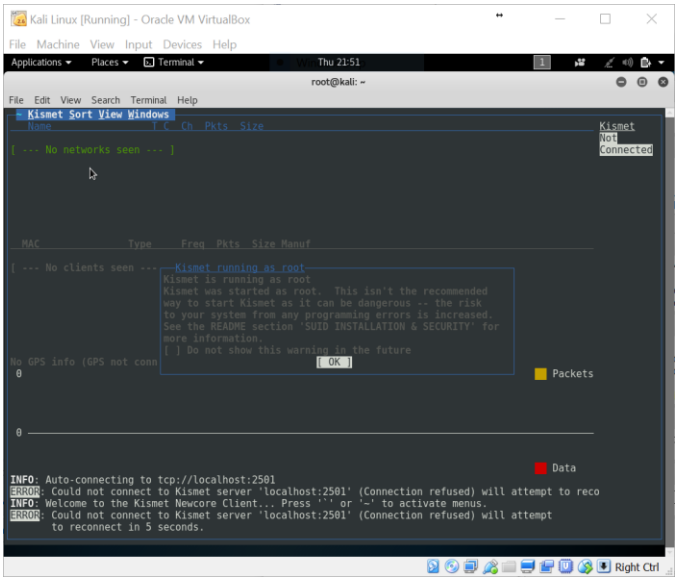


B. *Hidden or Cloaked Wirelss Network*

Lucent defined a proprietary access control mechanism known as a "closed network." Closed networks may be open networks that do not broadcast their Service Set Identifier (SSID). In theory, only those knowing the SSID may attempt to associate with the closed network. However, cloaking networks is ineffective. While cloaking the SSID hides networks from active scanning tools such as NetStumbler, the Access Point name is broadcast whenever an authorized system connects to the network. This is part of the association of the request packet. Intercepting the association request packets is trivial with tools such as kismet.

1) Tools – Kismet: Kismet is a graphical tool that enables passive detection and reconnaissance. Kismet is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system. It works with any wireless network card which supports raw monitoring (RFMON) mode. Kismet listens for broadcast beacons issued by an access point which specify its Service Set Identifier. By using passive detection, it is very difficult for the victim network to detect that passive reconnaissance is taking place. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting closed networks, and inferring the presence of non-beaconing networks via the monitoring of data traffic.

Figure 2: Kismet



C. *Wired Equivalent Privacy*

Wired Equivalent Privacy (WEP) protocol was an initial attempt to secure wireless network traffic. The goal was to restrict access to clients having the private, shared WEP key. The way shared key authentication works is by following this sequence of steps:

- The client sends an authentication request to the Access Point.
- The Access Point responds to the client with a 128-bit challenge text.
- The client returns the challenge text encrypted with a shared key
- The Access Point validates the encrypted response.
- The connection between the client and Access Point is established if the challenge matches.

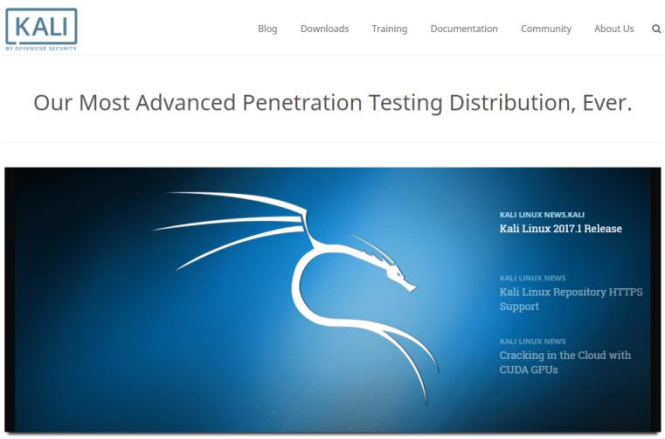
However, WEP has a critical weakness. The Access Point text is sent as plain text. This means that the encryption is XOR'd with the encryption stream and the known initialization vector simplifies cracking.

For attacks against WEP and Wifi Protected Access (WPA) three critical bits of information have to be gathered:

1. MAC address of the target access point
2. MAC address of the one client system
3. Communications channel in use

1) Tools – Kali Linux: Kali Linux is a Debian derived open source project maintained and funded by Offensive Security for digital forensics and penetration testing. Kali Linux comes pre-installed with over 300 penetration testing programs. Kali Linux can run natively from a computer hard drive or as a Live CD or USB. It is a supported platform of the Metasploit Framework.

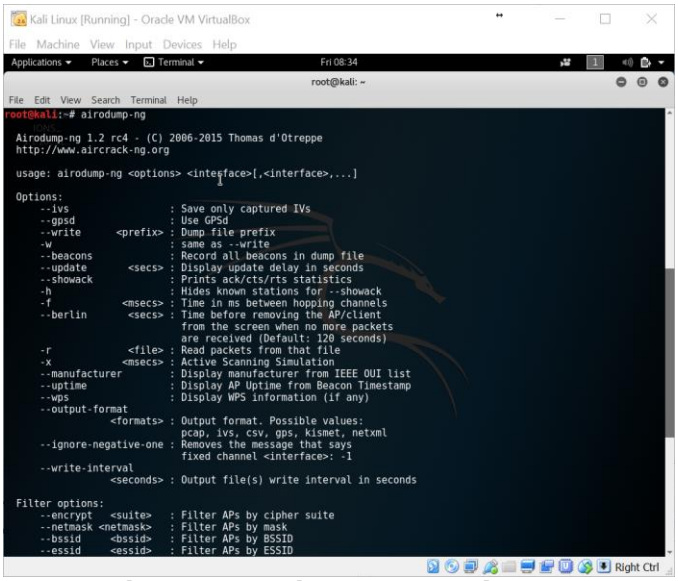
Fig. 3. Kali Linux Open Source Project



2) Tools – Airmon-ng: Airmon-ng is a bash script designed to turn wireless cards into monitor mode. It auto-detects which card you have and runs the right commands. It is necessary to enable monitor mode for wireless network interface cards in order to break WEP encryption.

3) Tools – Airodump-ng: Airodump-ng is part of the aircrack-ng suite. Airodump-ng is a packet capture tool for aircrack-ng. It allows dumping packets directly from WLAN interface and saving them to a pcap or IVs file. Airodump-ng is first used to list all available access points and clients. In monitor mode, once can view details of wireless devices and the associated channel number. Also in monitor mode, airodump-ng can be used to capture wireless traffic on a specific channel or SSID. It is an alternative to Kismet because it does not have a visual component. Airodump-ng is more of a packet dump tool than a reconnaissance tool. It cannot change channels without restarting and it cannot drill down to particular networks.

Figure 4: airodump-ng

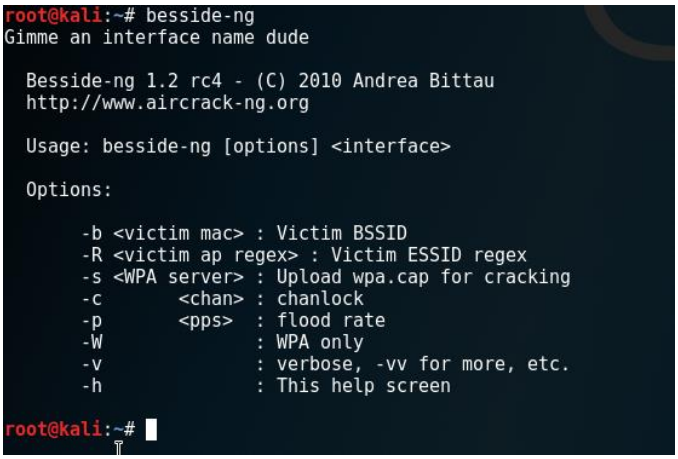


4) Tools – Aireplay-ng: Aireplay-ng injects specially generated ARP-request packets into an existing wireless network in order to generate traffic. By sending these ARP-request packets again and again, the target host will respond with encrypted replies, thus providing new and possibly weak IVs. Aireplay-ng supports single-NIC injection/monitor. Aireplay-ng is also used to deauthenticate a "good" client. This may need to be run a few times in order to "kick" a client off.

5) Tools – Aircrack-ng: Aircrack-ng is a 802.11 WEP key cracking program. Aircrack-ng will recover a WEP key once a sufficient number of encrypted packets have been captured with airodump-ng.

6) Tools – besside-ng: Besside-ng is a tool that automatically cracks WEP and Wi-Fi Protected Access networks by logging handhakes.

Figure 5: beside-ng



D. Wi-Fi Protected Access/Wi-Fi Protected Acccess 2

Wi-Fi Protected Access and Wi-Fi Protected Access 2's security implementation is secure but the weakness lies in the client/user. The attacks against Wi-Fi Protected Access usually involve breaking predictable or non-complex passwords. When a client authenticates to a wireless network, a temporary key is generated for that session. The Service Set Identifier and password are used in this process. If an individual has the WPA password and is able to capture the authentication, a bad actor can re-generate the key and decrypt traffic. Even the Wireshark tool is able to do this for you. However, you will need to capture the association of each session for each client to decrypt the network traffic. With the Service Set Identifier and the authentication sequence, a bad actor can guess the password. Most attacks are often a dictionary based attack. However, if the user uses a password that is complex and not susceptible to a dictionary attack, the chances of

1) Tools – Genpmk: Genpmk generates a Pairwise Master Key (PMK) for the Wi-Fi Protected Access. Church of WiFi has generated 38 gigabytes of the top 100 SSIDs and a dictionary file containing one million words.

2) Tools – Cowpatty: Cowpatty can be used to take pre-computed hashes and compares the captured WPA handshacke to the generated hashes.

3) Tools – Aireplay-ng: Aireplay-ng is used to de-authenticate the client. The client will then reauthenticate and that's when the handshake with the Access Point is captured. De-authentication and re-

authentication is generally not noticable by the user; they are virtually silent.

III. 802.1X

The spread of 802.11 related wireless security enhancements is currently challenging the hacker community. 802.1X is the next generation of authentication subsequent to WEP. Currently publicly available tools attack EAP-LEAP authentication. LEAP is a Cisco protocol that implements 802.1X on wireless local area networks.

1) Tools – asleap. An example would be "asleap". Asleap is a tool that recovers weak LEAP passwords by capture live data from any wireless inferface in monitor mode. Asleap will actively de-authenticate users on LEAP networks, forcing them to re-authenticate. This makes the capture of LEAP passwords particularly quick. Attacks against other EAP types will emerge and be improved.

IV. Improvements

The ideal combination is to use WPA2 Enterprise and either EAP-TLS or EAP-PEAP-TLS. However, setting this up is not practical for the average home user as this requires enterprise grade equipment, configuration, and support. The improvements in wireless network security need to focus on ways to make strong security practices practical for the average home user and small business.

V. Conclusion

Wireless network security will be at the forefront of network security challenges for quite some time to come. The main challenges in network security is as much of a technology problem as it is a user problem. The public needs to be better educated in how to take advantage of the best practices to secure their wireless networks. The industry needs to focus on improving current technologies and protocols as well as making the best available practices today economical and practical for the average home and small business user.

Acknowledgment

The author would like to acknowledge and sincerely thank those that provided assistance by proofreading and improving the quality and content of this paper. The author would also like to thank his professor for the opportunity to learn more about this important and relevant topic.

References

[1] A.K.M. Nazmus Sakib, S. Ahmed, S. Rahman, I. Mahmud, Md. Habibullah Belali, "WPA 2 (Wi-Fi Protected Access 2) Security Enhancement: Analysis & Improvement," *Global Journal of Computer Science And Technology*, [Online]. Available: https://globaljournals.org/GJCST_Volume12/9-WPA-2-(Wi-Fi-Protected-Access-2).pdf. [Accesed: 06-May-2017].

[2] P. Arana, "Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)," *INFS 612 – Fall 2006*. [Online]. Available: http://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf. [Accessed: 06-May-2017].

[3] "IEEE 802.11i," *Wikipedia, The Free Encyclopedia*, 05-May-2017. [Online]. Available: https://en.wikipedia.org/wiki/IEEE_802.11i-2004. [Accesed: 06-May-2017].

[4] J. Davies, "Wi-Fi Protected Acess 2 Data Encryption and Integrity," *Microsoft TechNet: The Cable Guy*, August 2005. [Online]. Available: https://technet.microsoft.com/library/bb878096. [Accessed: 06-May-2017].

[5] G.Ou, "Understanding the updated WPA and WPA2 standards," *ZDNet for Real World IT*, 02-Jun-2005. [Online]. Available: http://www.zdnet.com/article/understanding-the-updated-wpa-and-wpa2-standards/. [Accessed: 06-May-2017].

[6] G. Lehembre. "Wi-Fi security – WEP, WPA and WPA2," *hankin9*, Jun-2005. [Online]. Available: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf. [Accessed: 06-May-2017]

[7] G. Ou. "Wireless LAN security guide," *lanarchitect*, 03-Jan-2005. [Online]. Available: http://www.lanarchitect.net/Articles/Wireless/SecurityRating/. [Accessed: 06-May-2017].

[8] "Extensible Authentication Protocol" *Wikipedia, The Free Encyclopedia*, 09-May-2017. [Online]. Available: https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol. [Accesed: 10-May-2017].

[9] G. Ashok, T. Buthmann. "The Bell Labs Security Framework: Making the Case for End-to-End Wi-Fi Security," *Alcatel-Lucent: Technology White Paper*, 2007. [Online]. Available: http://www.webtorials.com/main/resource/papers/lucent/paper90/wireless3.pdf. [Accessed: 06-May-2017].

[10] J. Epstein. "802.11w fills wireless security holes," *Network World from IDG*, 03-Apr-2006. [Online]. Available: http://www.networkworld.com/article/2310261/tech-primers/802-11w-fills-wireless-security-holes.html. [Accessed: 06-May-2017].

[11] J. Wright. "802.11w will improve wireless security," *Network World from IDG*, 29-May-2006. [Online]. Available: http://www.networkworld.com/article/2312251/network-security/how-802-11w-will-improve-wireless-security.html. [Accessed: 06-May-2017].

[12] L. Strand. "802.1X Port-Based Authentication HOWTO," *The Linux Documentation Project*, 18-Oct-2004. [Online]. Available: http://tldp.org/HOWTO/html_single/8021X-HOWTO/ [Accessed: 06-May-2017].

[13] J. Bellardo, S.Savage. “802.11 Denialof-Service Attacks: Real Vulnerabilities and Practical Solutions,” *University of California at San Diego*. [Online]. Available: http://cseweb.ucsd.edu/~savage/papers/UsenixSec03.pdf. [Accessed 06-May-2017].

[14] A.K.M. Nazmus Sakib, Dr. M. Ibrahim Khan, M. Md. Saki Kowsar. “IEEE 802.16e Security Vulnerability: Analysis & Solution,” *Global Journal of Computer Science and Technology*, Oct-2010. [Online]. Available: http://computerresearch.org/index.php/computer/article/view/637/637. [Acessed 06-May-2017].

[15] A.K.M. Nazmus Sakib. “Security Enhancement & Solution for Authentication Frame work in IEEE 802.16,” *Academic & Industrial Colleboration Centre [International Journal of Computer Science & Information Technology]*, Dec-2010. [Online]. Available: http://www.academia.edu/419001/Security_Enhancement_and_Solution_for_Authentication_Frame_work_in_IEEE_802.16. [Accessed 06-May-2017].

[16] A.K.M. Nazmus Sakib. “Secure Key Exchange & Authentication Protocol For Multicast & Broad cast Service in IEEE 802.16e,” *AP Journal Special Issue*. [Online]. Available: http://www.academia.edu/493381/Secure_Key_Exchange_and_Authentication_Protocol_For_Multicast_and_Broad_cast_Service_in_IEEE_802.16e. [Accessed: 06-May-2017].

[17] A.K.M. Nazmus Sakib, T. Mahmud, M. Munim, S. Rahman, M. Mushfiqur Rahman. “Secure Authentication & Key Exchange Technique for IEEE 802.16e by using Cryptographic Properties,” *International Journal of Engineering Research and Applications.* [Online]. Available: http://www.ijera.com/papers/vol%201%20issue%203/P013490496.pdf. [Accessed: 06-May-2017].