Wireless Network Security: Vulnerabilities, Threats and Countermeasures

Min-kyu Choi[1)], Rosslin John Robles[1)], Chang-hwa Hong[2)], Tai-hoon Kim[1)]
School of Multimedia, Hannam University, Daejeon, Korea
puremiroa@naver.com, rosslin_john@yahoo.com, taihoonn@hannam.ac.kr

Abstract

Wireless networking provides many advantages, but it also coupled with new security threats and alters the organization's overall information security risk profile. Although implementation of technological solutions is the usual respond to wireless security threats and vulnerabilities, wireless security is primarily a management issue. Effective management of the threats associated with wireless technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats. We present a framework to help managers understand and assess the various threats associated with the use of wireless technology. We also discuss a number of available solutions for countering those threats.

Keywords : Wireless Network, Wireless Security, Wireless Threats, Signal-Hiding

1. Introduction

Wireless networking presents many advantages Productivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality. Although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. The objective of this paper is to assist managers in making such decisions by providing them with a basic understanding of the nature of the various threats associated with wireless networking and available countermeasures.

The popularity of wireless Networks is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The majority of computers sold to consumers today come pre-equipped with all necessary wireless Networks technology. The benefits of wireless Networks include: Convenience, Mobility, Productivity, Deployment, Expandability and Cost.

Wireless Network technology, while replete with the conveniences and advantages described above has its share of downfalls. For a given networking situation, wireless Networks may not be desirable for a number of reasons. Most of these have to do with the inherent limitations of the technology. The disadvantages of using a wireless network are: Security, Range, Reliability, and Speed.

Wireless Networks present a host of issues for network managers. Unauthorized access points, broadcasted SSIDs, unknown stations, and spoofed MAC addresses are just a few of the problems addressed in WLAN troubleshooting. Most network analysis vendors, such as Network Instruments, Network General, and Fluke, offer WLAN troubleshooting tools or functionalities as part of their product line.

2. Wireless Vulnerabilities, Threats and Countermeasures

The wireless networks consist of four basic components: The transmission of data using radio frequencies; Access points that provide a connection to the organizational network and/or the Client devices (laptops, PDAs, etc.); and Users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability.

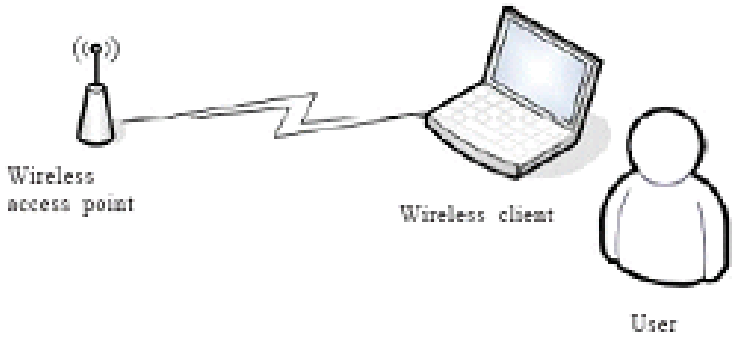

Fig. 1 Wireless networking components

2.1 Wireless Network Attacks

2.1.1 Accidental association

Unauthorized access to company wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighboring company’s overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

2.1.2 Malicious association

"Malicious associations" are when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP). These types of laptops are known as "soft APs" and are created when a cracker runs some software that makes his/her wireless network card look like a legitimate access point. Once the cracker has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans. Since wireless networks operate at the Layer 2 level, Layer 3 protections such as network authentication and virtual private networks (VPNs) offer no barrier. Wireless 802.1x authentications do help with protection but are still vulnerable to cracking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the cracker is just trying to take over the client at the Layer 2 level.

2.1.3 Ad-hoc networks

Ad-hoc networks can pose a 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.

2.1.4 Non-traditional networks

Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These non-traditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.

2.1.5 Identity theft (MAC spoofing)

Identity theft (or 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 IDs 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.

2.1.6 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. Man-in-the-middle attacks are enhanced by software such as LANjack and AirJack, which automate multiple steps of the process. What once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

2.1.7 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. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

2.1.8 Network injection

In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as "Spanning Tree" (802.1D), OSPF, RIP, and HSRP. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

2.1.9 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.

3. Securing Wireless Transmissions

The nature of wireless communications creates three basic threats: Interception, Alteration and Disruption.

3.1 Protecting the Confidentiality of Wireless Transmissions

Two types of countermeasures exist for reducing the risk of eavesdropping on wireless transmissions. The first involves methods for making it more difficult to locate and intercept the wireless signals. The second involves the use of encryption to preserve confidentiality even if the wireless signal is intercepted.

3.1.1 Signal-Hiding Techniques In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. There are, however, a number of steps that

organizations can take to make it more difficult to locate their wireless access points. The easiest and least costly include the following: Turning offthe service set identifier (SSID) broadcasting by wireless access points, Assign cryptic names to SSIDs, Reducing signal strength to the lowest level that still provides requisite coverage or Locating wireless access points in the interior of the building, away from windows and exterior walls. More effective, but also more costly methods for reducing or hiding signals include: Using directional antennas to constrain signal emanations within desired areas of coverage or Using of signal emanation-shielding techniques, sometimes referred to as TEMPEST, 1 to block emanation of wireless signals.

3.1.2 Encryption The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic. This is especially important for organizations subject to regulations.

3.2 Preventing Alteration of Intercepted Communications

Interception and alteration of wireless transmissions represents a form of "man-in-themiddle" attack. Two types of countermeasures can significantly reduce the risk of such attacks: strong encryption and strong authentication of both devices and users.

3.3 Countermeasures to Reduce the Risk of Denial-of-Service Attacks

Wireless communications are also vulnerable to denial-of-service (DoS) attacks. Organizations can take several steps to reduce the risk of such unintentional DoS attacks. Careful site surveys can identify locations where signals from other devices exist; the results of such surveys should be used when deciding where to locate wireless access points. Regular periodic audits of wireless networking activity and performance can identify problem areas; appropriate remedial actions may include removal of the offending devices or measures to increase signal strength and coverage within the problem area.

4. Securing Wireless Access Points

Insecure, poorly configured wireless access points can compromise confidentiality by allowing unauthorized access to the network.

4.1 Countermeasures to Secure Wireless Access Points

Organizations can reduce the risk of unauthorized access to wireless networks by taking these three steps:

1. Eliminating rogue access points;
2. Properly configuring all authorized access points; and
3. Using 802.1x to authenticate all devices.

4.1.1 Eliminate Rogue Access Points

The best method for dealing with the threat of rogue access points is to use 802.1x on the wired network to authenticate all devices that are plugged into the network. Using 802.1x will prevent any unauthorized devices from connecting to the network.

4.1.2 Secure Configuration of Authorized Access Points

Organizations also need to ensure that all authorized wireless access points are securely configured. It is especially important to change all default settings because they are wellknown and can be exploited by attackers.

4.1.3 Use 802.1x to Authenticate all Devices

Strong authentication of all devices attempting to connect to the network can prevent rogue access points and other unauthorized devices from becoming insecure backdoors. The 802.1x protocol discussed earlier provides a means for strongly authenticating devices prior to assigning them IP addresses.

5. Securing Wireless Client Devices

Two major threats to wireless client devices are (1) loss or theft, and (2) compromise. Loss or theft of laptops and PDAs is a serious problem. laptops and PDAs often store confidential and proprietary information. Consequently, loss or theft of the devices may cause the organization to be in violation of privacy regulations involving the disclosure of personal identifying information it has collected from third parties. Another threat to wireless client devices is that they can be compromised so that an attacker can access sensitive information stored on the device or use it to obtain unauthorized access to other system resources.

6. Securing Wireless Networks

6.1 Use of Encryption

The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn’t have an encryption feature, consider getting one that does. Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on.

6.2 Use anti-virus and anti-spyware software, and a firewall

Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

6.3 Turn off identifier broadcasting

Most wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the vicinity announcing its presence. You don't need to broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Disable the identifier broadcasting mechanism if your wireless router allows it.

6.4 Change the identifier on your router from the default

The identifier for your router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Even if your router is not broadcasting its identifier to the world, hackers know the default IDs and can use them to try to access your network. Change your identifier to something only you know, and remember to configure the same unique ID into your wireless router and your computer so they can communicate. Use a password that's at least 10 characters long: The longer your password, the harder it is for hackers to break.

6.5 Change your router's pre-set password for administration

The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router. Hackers know these default passwords, so change it to something only you know. The longer the password, the tougher it is to crack.

6.6 Allow only specific computers to access your wireless network

Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

6.7 Turn off your wireless network when you know you won't use it

Hackers cannot access a wireless router when it is shut down. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

6.8 Don't assume that public "hot spots" are secure

Many cafés, hotels, airports, and other public establishments offer wireless networks for their customers' use.

7. Training and Educating Users

Notice that Figure 1 also includes users as the fourth basic component of wireless networking. As is the case with wired security, users are the key component to wireless networking security. Indeed, the importance of training and educating users about secure wireless behavior cannot be overstated. To be effective, user training and education needs to be repeated periodically.

8. Network Auditing

Wireless network auditing is an important part of WLAN security policy. The network needs to be regularly audited for rouge hardware. In this method the network is scanned and mapped for all access points and WLAN nodes. Then this is compared with previous network map. Commonly available network mapping tools like netstumbler and wavelan-tool can be used to do this. Specialized tools such as Airsnort can be used for WEP cracking and auditing the network for weak keys, key reuse and WEP security settings. These methods include the same tests as those carried out by hackers for breaking into the network.

9. Conclusion

Wireless networking provides numerous opportunities to increase productivity and cut costs. It also alters an organization's overall computer security risk profile. Although it is impossible to totally eliminate all risks associated with wireless networking, it is possible to achieve a reasonable level of overall security by adopting a systematic approach to assessing and managing risk. This paper discussed the threats and vulnerabilities associated with each of the three basic technology components of wireless networks (clients, access points, and the transmission medium) and described various commonly available countermeasures that could be used to mitigate those risks. It also stressed the importance of training and educating users in safe wireless networking procedures.

References

[1] Graham, E., Steinbart, P.J. (2006) Wireless Security

[2] Cisco. (2004). Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, July 19.

[3] CSI. (2004). CSI/FBI Computer Crime and Security Survey.

[4] Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.

[5] Kelley, D. (2003). The X factor: 802.1x may be just what you need to stop intruders from accessing your network. Information Security, 6(8), 60-69.

[6] Kennedy, S. (2004). Best practices for wireless network security. Information Systems Control Journal (3).

[7] McDougall, P. (2004, March 25). Laptop theft puts GMAC customers'data at risk. Information Week Security Pipeline.

[8] Nokia. (2003). Man-in-the-middle attacks in tunneled authentication protocols.

[9] Paladugu, V., Cherukuru, N., & Pandula, S. (2001). Comparison of security protocols for wireless communications.

[10] Slashdot. (2002, August 18). Wardriving from 1500ft Up.

[11] Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). Risk management guide for information technology systems. NIST Special Publication 800-30.

[12] Wailgum, T. (2004, September 15). Living in wireless denial. CIO Magazine.

Acknowledgement

This work was supported by a grant from Security Engineering Research Center of Ministry of Knowledge Economy, Korea

Authors

Min-kyu Choi

He is currently a Multimedia Student at Hannam University, Korea. His research interests are Network Security and Software Security.

Rosslin John Robles

He received his B.S. in Information Technology from Western Visayas College of Science and Technology, Philippines. He is currently a Multimedia integrate Masters-Ph.D. Student at Hannam University, Korea. His research interests are Software Engineering and IT Security.

Tai-hoon Kim

He received B.E., M.E., and Ph.D. degrees from Sungkyunkwan University. Now he is a professor, School of Information & Multimedia, Hannam University, Korea. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments.