© 2014 IJIRT | Volume 1 Issue 11 | ISSN: 2349-6002

Wireless Network Security

Amrendra Kumar Upadhyay, Ankit Bhatt, Anil Pilaniya
Dronacharya College Of Engineering, Gurgaon
Sec-5, Haryana-122506

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.**

Index Terms- **Wireless Network, Wireless Security, Wireless Threats, Signal-Hiding**

I. INTRODUCTION

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999, which was outdated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. 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.

II. WIRELESS THREAT AND ATTACKS

Now these days' wireless attacks are rapidly growing. Many organization and institution have not any better plan to prevent these attacks.

2.1 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.

2.2 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.

2.3 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 LAN jack and Air Jack, 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

2.4 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).

2.5 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.

III. SECURING WIRELESS NETWORK

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.6 Don't assume that public "hot spots" are secure:-

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

<u>TIPS ON INTERNET SURFING VIA PUBLIC WIRELESS SERVICES:-</u>

Once you have a wireless device such as a notebook computer or a hand-held device connected to public wireless hotspots, you are exposing yourself to potential attacks from remote attackers. Nonetheless, the following security tips may prevent you from falling into the traps laid by attackers:

1. Don't leave your wireless device unattended;
2. Protect Your Device with Passwords: Enable your device's power-on login, system login authentication, and password-protected screen saver.
3. Disable Wireless Connection When It Is Not In Use: Wi-Fi, infrared, and Bluetooth devices are constantly announcing their presence if they are enabled.

5. Protect your device with anti-virus software using the latest virus definitions. This can minimize the risk of infection by computer viruses or spyware.
6. Encrypt Sensitive / Personal Data on the Device: Even when an unauthorized user gains access to your device, encryption will keep your data away from an opportunistic thief.
7. Turn off Resource Sharing Protocols for Your Wireless Interface Card: When you share files and folders, your shared resources may attract attackers attempting to manipulate them.

IV. 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 nets tumbler and Waveland-tool can be used to do this. Specialized tools such as Air snort 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.

V. 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.

REFERNCES

www.youtube.com
www.wikipedia.org
www.google.co.in