Ten Deadly Sins in Wireless Security

The emergence and popularity of wireless devices and wireless networks has provided a platform for real time communication and collaboration. This emergence has created new IT vulnerabilities, which in turn have created the necessity to establish practices that make the wireless environment secure and convenient. in order to reap all of the benefits associated with wireless technology. This paper focuses on the ten deadly sins of Wireless security.

1. Introduction

Wireless technology is yet another offshoot of Information and communication technology revolution. Users now rely extensively on networks for carrying out personal and business activities. Wireless networks provide users with real-time access to information from anywhere at any time without the constraint of wired networks. In essence, wireless networks provide mobility, unavailable with wired networks. It is easier to install wireless network and systems can be configured to communicate in the wireless environment. As more and more people use wireless devices and avail online services, wireless networking is set to gain inroads into the daily routine of users.

1.1 Wireless Security

Laptops, notebooks and other wireless devices facilitate users to access information from remote locations. Users can access online accounts, send and receive e-mails, and conduct transactions by using a wireless network. Radio waves and microwave signals are used to transmit data. Consequently, there remains a threat of intrusion of network, breach of data and privacy of the user. Wireless security is a cause for concern. As with any other technology, wireless technology also makes it easier for perpetrators of crime to achieve their goals.

2. Ten Deadly Sins of Wireless Security

Wireless security has evolved over the years. Substantial progress has been made in encryption protocols from the initial Wired Equivalent Privacy (WEP) protocol to Wireless Protected Access2 (WPA2) protocol. However, risks remain in the horizon. Here are the ten deadly sins of wireless security.

i. Inappropriate Encryption

Encryption is crucial for safe transmission of data in the network. It encodes the data so that only entitled users are able to read it. Users should enable encryption on routers. Lack of proper encryption could expose wireless traffic to other users on the network. Again, older encryption protocols like WEP are vulnerable to attacks from hackers. WPA2 is the latest encryption protocol for wireless networks. Products using WPA could be upgraded to WPA2, while those using WEP cannot upgrade to WPA2. Users may therefore, verify whether routers support the latest wireless encryption standards. In case of WPA2, users are required to enter a security key to connect. On validation, all data transmitted between device and access point is encrypted.

One of the vulnerabilities of the older encryption standard such as WEP was that it used same key for different sessions and clients. WPA2 generates a new encryption key for each session. WPA2 uses Advanced Encryption Standard (AES) for encryption. WPA2 uses Pairwise Transient Key (PTE) for unicast (single user and single receiver) traffic, and Group Temporal Key to protect traffic between multiple users.

ii. Broadcasting SSID

Wireless networks use a mechanism called Service Set Identifier (SSID) or ESSID (Extended Service Set Identifier) – a name assigned to a wireless network. Wireless routers may broadcast signals to announce their presence. These signals know as beacon signal transmit information including SSID, which facilitates other devices to connect to a user's wireless network. It facilitates users to find and connect to other networks.

However, SSIDs are not encrypted and any hacker probing networks could get a crucial piece of information in their efforts to intrude into a wireless network. When a user disables SSID broadcasting, it is no longer sent in beacon signals.

Some of precautions related to SSID and access point include:

a. Disable identifier broadcasting

b. Rename SSID to an unpredictable name. Do not use user name, company name, telephone number, date of birth and other identifiable names for network, as they are easily exploitable by the hacker.

iii. Weak passwords

WPA2 protocol supports use of pre-shared key for authentication for home and small business users. A user has to enter a passphrase[1] in the access point as well as at the client station. The security passphrase must be

[1] Passphrases are similar to passwords, but are longer and used to protect access systems.

between 8-63 characters or 64 hexadecimal values. Passphrases are vulnerable to brute force attacks. A passphrase should be unpredictable and should not include personal information or commonly used terms. It should comprise of random characters and not have sequential characters. To protect against brute force attacks, a passphrase must have at least 20 characters.

Enterprise authentication systems involve two layers of password protection. One is an open authentication system and other is an Extensible Authentication Protocol.

iv. Free Wireless Hotspots

Free Wireless hotspots are Internet access points at public places, which offer connection over wireless networks. They enable users to access Internet, connect with office networks, and check e-mails even when they are away from home or office. Users look for convenience and wireless hotspots provide just that. One can find wireless access points at public places such as Cyber cafés, libraries, offices, airports, railway stations and hotels. However, these wireless hotspots may be insecure.

a. Users may be required to use ISP of access points. Not all ISPs provide secure SMTP for sending e-mail. E-mails send and received by users could be intercepted by others in the network.

b. If user's wireless card is set to ad-hoc mode, other users can connect directly.

c. If the access point does not use encryption technology like WPA or WPA2, other users with a Wi-Fi card could intercept and read username, passwords, and any other information transmitted by the user.

Further, there is a risk of individuals with malicious intent setting up free wireless hotspots at public places, which may used to sniff data traffic, decipher authentication information and steal data.

While using public access points it is safe to use

a. Secure websites protected by Secure Sockets Layer.

b. Infrastructure mode rather than ad-hoc mode. Infrastructure mode uses access controls to connect to network.

c. Virtual Private Network (VPN) to connect with company network. VPN facilitates access to private network over public connections.

d. Disable file and printer sharing

e. Ensure that firewall is activated, and

f. Make the folders on your personal computer private

v. Lack of Media Access Control (MAC) Address Filtering

The MAC address is a 12-digit hexadecimal number, which uniquely identifies a wireless network adapter. MAC address is also known as physical address. One can find MAC address from the configuration utility. Users can enable MAC address filtering and enter MAC addresses of select devices, which they want to connect. When a device wants to connect to a wireless network, it sends a request to the access point for authentication. Once authenticated the device attempts to connect to the access point. MAC filtering works at this stage. Wireless routers can filter access to the wireless network by matching with MAC addresses listed on access controls. While hackers may probe addresses allowed by the access point and spoof MAC address, MAC address filtering does provide additional layer of protection.

vi. Default security setting

Default settings on programs and devices are usually simple and common, which may be easy to guess for hackers. Manufacturers may use same settings on all devices produced at their factory. For instance, user name may be name of the manufacturer and password may simply be 'password'. In case of wireless networks, routers or access points are key to connection between networks. Therefore, it is crucial to change the default settings. Users can login to the administrative console of a router by using the given user name and password. They can navigate to the change password section and enter a new password and save settings.

Dynamic Host Configuration Protocol (DHCP) automatically allots IP addresses to other devices attempting to connect to the network. However, there is a risk of hackers acquiring an IP address from the router. Further, wireless access points may by default be configured to assign IP addresses in the range of 192.168.0.x. This feature may create possibility of IP address conflict with other wireless access points in the network with same DHCP scope. It is safe to turn off the DHCP on the router and configure with static IP addresses by using private IP address range.

vii. Lack of regular update to latest firmware

Regular update of firmware to various wireless equipment is crucial to ensure proper connectivity. Firmware upgrades are released by manufacturers regularly. These upgrades could be downloaded from manufacturer's website. Some of the upgrades may improve performance of the device. For instance, routers are key to functioning of wireless networks. Regular updates could be downloaded from the website of the router manufacturer. Improper update could lead to malfunctioning of router. Therefore, users may restore router settings before update. After update is completed, user may restore router settings.

viii. Relying solely on Network access control (NAC)

NAC provides regulates entry-level access to network. It also regulates post admission access depending upon the user actions. It also provides protection from rogue Access points through host-based checks. However, a disgruntled employee or user with knowledge of 802.1X credentials can connect a rogue access point to another access point in silent mode. The user may spoof MAC address and modify the MAC address of the rogue access point preventing it from detection by NAC.

The attacker may place rogue access point behind a firewall to prevent flow of MAC address from the local wireless network and address resolution protocol (ARP) tables of the router.

This risk could be checked by using sniffers and probes. Sniffers scan radio frequency channels to detect connections with all access points within their range. Probes monitor all wireless local area network traffic within their range.

ix. Insecure access to company network

Wireless networks facilitate user mobility and allow employees to connect to office networks from distant locations. Many enterprises allow employees to work home. Public networks may however, not be completely secure and provide scope for data interception by other users in the network. In such cases, it is desirable to connect to company network through a Virtual Private Network (VPN). VPN enables a user to secure access with company network over a public connection. Data is encrypted to ensure safe transmission to the official network. VPN monitors the traffic to ensure integrity of data packets during their flow over public networks.

x. Lack of enforced wireless policy

While wireless networks enable enterprises convenient network access, mobility, and reduce dependence on wired networks, it is not devoid of risks. It is easier in wireless environment for employees to access and download restricted business data. A wireless policy is crucial to ensure reliable and safe wireless network. Employer must create mechanisms to enforce its wireless policy. The policy must include provisions for deployment, administration and usage of wireless networks.

Enterprises may frame guidelines and restrictions on use of external network cards and insecure wireless connections in the office premises. It is important to ensure that installations of access points are restricted to authorized personnel. User devices may be configured with smart card readers, and must be configured with proper authentication mechanisms. Employer must also

hold regular training sessions on threat profile and precautions to be followed by employees. Adequate mechanisms must be in place to ensure adherence to regulations and guidelines prescribed for secure use of wireless network in office premises.

3. Conclusion

Wireless networks and devices are vulnerable to intrusions from hackers. Wireless security is crucial to ensure confidentiality, integrity and authenticity of the data transmitted between various wireless networks. It is important to create awareness about the risks involved in wireless environment among users.