“ADVANCES OF WIRELESS NETWORK AND SECURITY”

Mrs. Seema Rani
Asst. Prof. Computer Science Dept.
Govt. College Jind
pdkseema@gmail.com

Abstract-- This paper discusses the network security threats and risks associated with wireless networks, and outlines a number of best practices for deploying wireless networks in corporate and home environments. With advances in technology, wireless accessibility is being deployed increasingly in office and public environments. Wireless networking and security have many importance, many enterprises are embracing wireless networking technologies to improve productivity, provide better customer service, and even offer Internet access to partners and on-site visitors 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, Threats, Wireless technology, Wi-Fi.

I. AN INTRODUCTION TO WIRELESS NETWORKING

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home. We begin by outlining some of the basic technologies of wireless network systems.

A. WIRELESS LOCAL AREA NETWORK

A Wireless Local Area Network (WLAN) is a type of local area network that uses high frequency radio waves rather than wires to communicate between network-enabled devices.

1. *Access Point* (AP) is a hardware device that allows wireless communication devices, such as PDAs and mobile computers, to connect to a wireless network. Usually, an AP connects to a wired network, and provides a bridge for data communication between wireless and wired devices.
2. *SERVICE SET IDENTIFIER* (SSID) is a configurable identification that allows wireless clients to communicate with an appropriate access point.

B. OPEN SYSTEM AUTHENTICATION

Open System Authentication is the default authentication protocol for the 802.11 standard. It consists of a simple authentication request containing the station ID and an authentication response containing success or failure data

C. SHARED KEY AUTHENTICATION

Shared Key Authentication is a standard challenge and response mechanism that makes use of WEP and a shared secret key to provide authentication. Upon encrypting the challenge text with WEP using the shared secret key, the authenticating client will return the encrypted challenge text to the access point for verification. Authentication succeeds if the access point decrypts the same challenge text.

D. WI-FI PROTECTED ACCESS AND WI-FI PROTECTED ACCESS 2

Wi-Fi Protected Access (WPA) is a wireless security protocol designed to address and fix the known security issues in WEP. WPA provides users with a higher level of assurance that their data will remain protected by using Temporal Key Integrity Protocol (TKIP) for data encryption. 802.1x authentication has been introduced in this protocol to improve user authentication.

Wi-Fi Protected Access 2 (WPA2), based on IEEE 802.11i, is a new wireless security protocol in which only authorised users can access a wireless device, with features supporting stronger cryptography (e.g. Advanced Encryption Standard or AES), stronger authentication control .

II. ADVANCES IN WIRELESS SECURITY

1. *Ultra-Wide-Band Radio Communication (UWB)*is a technology developed to transfer large amounts of data wirelessly over short distances over a very wide spectrum of frequencies in a short period of time.

2. *WiMedia* refers to high data-rate, wireless multimedia networking applications operating in a wireless personal area network (WPAN). The WiMedia brand is defined and supported by the WiMedia Alliance. The initial WiMedia radio technology will be based on ultrawideband (UWB) as defined by the MultiBand OFDM Alliance and MAC specifications. The primary goals of the WiMedia Alliance are to enable coexistence

of multi-protocol applications and to enable true multi-vendor interoperability by establishing procedures for ensuring devices from different manufacturers coexist within the common UWB radio platform. UWB Standards802.15.3ais a group working on UWB standards but could not decide between the two approaches – multiband OFDM (MOFDM) from the TI/Intel-led MBOA group, or direct sequence code division multiple access (DS-CDMA) from Motorola.

3. *Wireless Fidelity Systems (WiFi)*Wireless Fidelity (WiFi) is the standard for the high-speed wireless LAN. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wired networks (which use IEEE 802.3 or Ethernet). Wi-Fi networks operate in the unlicensed 2.4 and 5 GHz radio bands, with an 11/54 Mbps (802.11b/g) or 54 Mbps (802.11a) data rate

4. *WiMax*WiMAX is an acronym that stands for **W**orldwide **I**nteroperability for **M**icrowave **Acc**ess. The WiMAX Forum is an industry-led, non-profit corporation formed to promote and certify compatibility and interoperability of broadband wireless products.

III. ELEMENTS OF WIRELESS SECURITY

1. *Using of Authentication*

When you want to make sure that the individuals who use a wirelessnetwork are authorized to do so, use authentication (sometimes called accesscontrol). Unique logins and passwords are the basis of authentication.

2. *Checking For Rogue Access Points*

A well-meaning employee who enjoys a wireless network at home mightwant to enjoy the same freedom at work. He or she might purchase a cheapaccess point and plug it into a network without asking permission.Checking for rogue access points isn't difficult. There are tools that canhelp, and checking can be done with a wireless laptop and software.

3. *Using Encryption*

To make sure that data can't be read, and to protect data from being altered as it's transmitted between an access point and a wireless device, use encryption.

IV. SOLUTION FOR WIRELESS SECURITY

Three solutions are available for secure wireless LAN encryption andauthentication:
• Wi-Fi Protected Access (WPA)
• Wi-Fi Protected Access 2 (WPA2)
• Virtual private networking (VPN)
The solution you select is specific to the type of wireless LAN you'reaccessing and the level of data encryption required.

1. *Wireless Network Security Encryption*

All of Bluetooth is divided at the core, according to Israelisecurity specialists who have recently reportedly found a serious corevulnerability in the basic Bluetooth specification. According toNewScientist.com, researchers havediscovered a cryptographic, worst kind of flaw in the Bluetoothstandard that renders all Bluetooth implementations vulnerable to a fairlysimple attack, making those implementations completely insecure.Bluetooth is a short-range (about a 300-foot maximum) radio standardused by networks to feed data to printers, portable phones, laptops, and otherelectronic devices. The newly discovered decryption technique makes allBluetooth communications insecure.Instead, the new threat lets attackers penetrate aBluetooth network at any time and take over the connection, perhapsestablishing a connection allowing unlimited long distance calls. Basically,the researchers have found a way to force Bluetooth devices into the initialpairing mode and thus decrypt the 128-bit key in well under a second, evenusing older PCs.In addition, one basic design flaw in Advanced Encryption Standard(AES) allows a timing attack to recover AES keys from a remote server.

2. *WEP Woes*

Enterprises need to be more aware of the critical rolethat security plays in wireless networks.Despite advances in wireless technology, thesecurity of a wireless network will never equal that of a wired network.Unfortunately, most enterprises that have already deployed wirelessaccess chose usability over security, just like most software enterprises. Inaddition, many enterprises don't consider the fact that wireless access doesn'treally offer any advantages over wired access in many cases.In fact, it can actually introduce new problems. Numerous 802.11bwireless network problems have been caused entirely by the use of 2.4-GHzwireless phones, often from wireless PBX systems.Wireless networks are now increasing in the enterprise environment, and enterprisedeployments . However, it is strongly recommended thatenterprises use this strategy when deciding whether to go wireless: Usewireless networking only in cases where wired access is impossible, not justas a simple or trendy alternative, remember that no matter what security technologies orstandards used, there will always be someone out there trying to breakit—and that includes WPA. In any event, you can deploy Gigabit Ethernetaccess at a lower cost, so it can provide both superior security and bandwidthirrespective of data encryption.If wireless access is your only alternative, explore the use of PPTP/L2TPand IPSec on your existing infrastructure before deciding to replace orupgrade existing 802.11a and 802.11b equipment. While it's not pretty froma technological point of view, it's quite functional, and it just might prove tobe more secure than 802.11.

V. ISSUES IN WIRELESS NETWORK

Wireless networks require the same security measures as conventionalnetworks, and then some. The issues that concern you with wireless networks and devices: Keep theencryption strong, keep the certificates in place, and keep focused onsecurity. Wireless security isn't a matter of different security, it's a matter ofmore security. Here are the most common security oversights and how youcan avoid them.

- Don't breach your own
- Don't spurn MAC
- Don't spurn WEP or WPA
- Don't allow unauthorized access points
- Don't permit ad-hoc laptop communications

VI. END POINT SECURITY CONTROL

The widespread use of SSL VPNs for remote access enables more usersto gain access to your network from far more places than they would if theywere using a traditional IPSec VPN.. Toeffectively control these risks, managing access by user identity alone is no longer enough. You also need to focus on the safety of that user'senvironment enterprise network. The Points are you should be able to offer:

- Security access from multiple environments
- Policy Zones rather than an "access" policy
- Device Interrogation
- Control of administration

VII. SUMMARY AND CONCLUSIONS

Although Wi-Fi technologies have significantly improved their security capabilitiesequipment for IT-managed infrastructure. Meanwhile, cellular data networksrely on a completely separate security architecture that emphasizesprotection of the radio link and does not provide end-to-end encryption.By using an SSL VPN, you can secure all forms of wirelesscommunication, both externally and internally. Moreover, this approachaccommodates a wide range of user equipment .it's too soon to tell whether WNS encryption problems willexploited vulnerabilities.However, they point out that you shouldn't rely too heavily on encryptionor any other security technologies.

REFERENCES

[1] Scott Robinson, "Strengthen Your Wireless Security By Avoiding These Missteps,"Copyright ©2005 CNET Networks, Inc. All rights reserved. TechRepublic, 235 SecondStreet, San Francisco, CA 94105, 2005.

[2] "End Point Control: Secure Anywhere Access With Reduced Risk And Increased ITControl," © 2004 Aventail Corp. All rights reserved. Aventail Corporation, 808 HowellSt., Second Floor, Seattle, WA 98101, 2004.

[3] John R. Vacca, Firewalls : Jumpstart for Network and Systems Administrators, DigitalPress, 2004.

[4] John R. Vacca, Net Privacy: A Guide to Developing and Implementing an Ironcladebusiness Privacy Plan, McGraw-Hill, 2001.