ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (296-301), Month: July - September 2016, Available at: www.researchpublish.com

AN OPTIMIZATION OF WIRELESS NETWORK SECURITY SYSTEM

Nandhini P[1], Dr .B. Jagadhesan[2], Anusuja D[3]

Research scholar[1,3] , Assistant Professor[2], PG & Research Dept. of Computer science, D.B. Jain College (Autonomous)

Abstract: **The purpose of this study is to review contemporary wireless network protocols and areas that affect the ability of wireless fidelity (Wi-Fi) technology to secure data transmitted over wireless networks. The research approach takes the form of a case study, in collating the methods used by existing protocols in the implementation of wireless Security Trust Models within their networks Wireless protected access Wi-Fi protected access; version 2 (WPA2) protocol has provided a more secure means for securing wireless networks but has only provided stronger encryption as it has a longer key which takes longer to decipher. In the current world, the high value objects such as ipads, laptops, are prone to the theft and are required to be monitored to ensure safety. Monitoring the objects within a short distance by the use of a wireless security system is implemented with the help of modules which are capable of communicating with each other.**

Keywords: **wifi, wimax, wireless network equipments, wireless networks attacks.**

1. INTRODUCTION

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. The use of wireless technology is quickly becoming the most popular way to connect to a network. Wi-Fi is one of the many available technologies that offer us the convenience of mobile computing. The thought of working anywhere and sending data to and from a device without physical connection is becoming increasingly attractive for many consumers and businesses .The secure use of wireless networks is based on users connecting to the network via

Predetermined access points using protocols in order to access the network securely. The existing protocols are the wired equivalent privacy protocol (WEP) and the wireless fidelity (Wi-Fi) Protected Access Protocols (WPA or WPA2) However the protocols still require the use of radio waves as a transmission medium and as such data can be intercepted and used by unauthorized persons. The increased use of Hotspots and Wi-Fi areas in the City of London region, which is densely, populated with financial organizations means that other alternative security arrangements need to be made.

2. WIRELESS NETWORKING

Wireless networking refers to the "utilization of cross-vendor industry standards, such as IEEE 802.11, where nodes communicate without needing to be wired". The infrastructure of wireless networks makes use of standard protocols that are oriented according to the demands of the network. This makes the capacity as well as the quality of services of wireless networks vary based on the devices. Wireless networks are typically expected to deal with devices that are made from various manufactures. The networks are therefore supposed to be able to support different hardware technologies, architectures, and transport protocols and also control the flow of traffic within the network. All wireless networks make use of waves in the electromagnetic spectrum range. For example, Wireless local-area networks (Wireless LANs) make use of high frequency electromagnetic waves to transmit data. Modulation and demodulation of the radio waves used to transmit data occurs at the transmitter and receiver respectively [1].

Wifi and wimax:

If you've been in an airport, coffee shop, library or hotel recently, chances are you've been right in the middle of a wireless network. Many people also use wireless networking, also called Wi-Fi or 802.11 networking, to connect their computers at home, and some cities are trying to use the technology to provide free or low-cost Internet access to residents. In the near future, wireless networking may become so widespread that you can access the Internet just about anywhere at any time, without using wires [2].

Security issues in Wi-Fi:

Wireless networks are inherently less secure than wired networks. The signal is broadcast, the network is shared and any network device can listen to network traffic for any other network device in range. This means that maintaining network security is potentially difficult. The signal spreads outside buildings so physical security is ineffective and it could be very difficult to locate unauthorized devices. The current wireless networking standards have very poor encryption facilities which cannot be regarded as Secure. Efficient operation of wireless networks depends on coordinated management of the available spectrum. Unauthorized wireless equipment may interfere with and degrade the performance of authorized services [2].

Wimax:

WiMAX is a wireless digital communications system, also known as IEEE 802.16 that is intended for wireless "metropolitan area networks". WiMax can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations. In contrast, the WiFi/802.11 wireless local area network standard is limited in most cases to only 100 - 300 feet (30 - 100m). With WiMax, Wi-Fi-like data rates are easily supported, but the issue of interference is lessened. WiMAX operates on both licensed and non-licensed frequencies, providing a regulated environment and viable economic model for wireless carriers. WiMax can be used for wireless networking in much the same way as the more common Wi-Fi protocol. WiMax is a second-generation protocol that allows for more efficient bandwidth use, interference avoidance, and is intended to allow higher data rates over longer distances. The IEEE 802.16 standard defines the technical features of the communications protocol. The WiMax Forum offers a means of testing manufacturer's equipment for compatibility, as well as an industry group dedicated to fostering the development and commercialization of the technology. WiMax.com provides a focal point for consumers, service providers, manufacturers, analysts, and researchers who are interested in WiMax technology, services, and products. Soon, WiMax will be a very well recognized term to describe wireless Internet access throughout the world.

The risks of using WiMAX:

Some of the attacks conducted at the various layers of WiMax are –

Physical Layer Threats:

1. Jamming

Jamming is the process of introducing a strong source of noise powerful enough to significantly reduce the signal to noise ratio.

2. Scrambling

Scrambling is another form of jamming, but for short intervals and is used to disorder targeted frames (mostly management messages).

Mac Layer Threats:

1. Eavesdropping

During basic and primary connection, MAC management messages are sent in plaintext and are not properly authenticated which can be used by an attacker to launch an attack.

2. Masquerading threat

Identity theft occurs in which a fake device can use the hardware address of another registered device by intercepting the management messages and launch an attack.

3. Denial of Service (DoS)

An attacker can force a BS to digest a large amount of handoffs and then launch a denial of service attack. In an 802.16 mesh network deployment routers or gateways that reside between base station and client are susceptible to attacks in the application layer.

3. WIRELESS NETWORKING EQUIPMENT

A. Antennas:

There are 2 types of antennas . . . Omni-directional and directional. Omni directional antennas have 360° coverage [or almost]. Directional antennas only go one direction, and have varying beam widths and areas they cover. Why would you

Use a directional antenna over an Omni? Paths of signals only covering a smaller beam width are less susceptible to noise, and tend to go really far. Also, directional antennas are usually cheaper. Basically, if your signal needs to go to more than

One place, you should have an Omni directional antenna. If you're going the directional route, buy or build a yogi. The next factor in choosing an antenna is how much gain do you need? Gain is measured in Decibels [dB]. Your signal Doubles in strength every 3 dB, so if you're putting out 32mW and you have a 6 dB gain antenna, you will be outputting 128mW. Likewise, if you have a cable that attenuates 3 dB after an initial output of 32mW, you will be outputting 16mW at the end of the cable. So how much gain do you really need? There are many things that affect a signal, so it's hard to say. Your best bet is to get the highest gain you can, but there is rarely a need for anything greater than 16 or 18 dB. Anything past that, and you start running into safety and problems with cards not being able to push that much power [2].

B. Transceivers:

Need a PCMCIA card? Get Orinoco Gold. Best you can buy, well worth the price, and they have a nifty external antenna connector on them already. Need a PCI or ISA card? Don't ask me, I haven't used any, but what I'd do is get one of those PCI to PCMCIA adaptor things, and plug an Orinoco Gold into it. The Linksys WET11 Ethernet Bridge is excellent. It's also extremely fast. As for access points, I'd probably also recommend Linksys, unless you are an ISP or something, and have some money to throw around. I haven't tried Cisco's stuff, but I see no point in it. You'd just be buying a name with them. 3Com's equipment is also nice, and is usually affordable.

C. Cables, Connectors, and Other Doo- hickies:

First off, you'll probably need a pigtail. this is nothing but a short little adapter cable that plugs into your 802.11 card, or other device, and has an N type connector on the other end. Next thing you need is a chunk of coax. Get LMR-400 if you can. Note that it sometimes goes under other names. You'll need N connectors on both ends of that coax. Yes, you can put your own on, but sometimes it's just easier to buy a 20' section of it with the ends already on. Keep in mind when getting coax. The shorter the cable runs, the less signal loss you have. Don't use more than you have to.

4. WIRELESS NETWORK ATTACKS

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.[3]

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.

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.

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 nontraditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.

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.

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 A International 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.

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).

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.

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.

5. SECURING WIRELESS TRANSMISSIONS

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

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].

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 off the 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.

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.

6. SECURING WIRELESS ACCESS POINTS

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

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.

Eliminate Rogue Access Points:

The best method for dealing with the threat of rogue access points is to use 802.1 xs 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.

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 well known and can be exploited by attackers.

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.

Security Challenges in Wireless Networks:

Securing wireless networks posses unique challenges compared to a wired network due to the open nature of the access medium. In general, wireless networks suffer from security threats of wired networks and additional vulnerabilities making it more challenging to secure. Wireless network security is different from wired net-work security primarily because it gives potential attackers easy transport medium access. Hence the security schemes in wired network can not be used directly in wireless network. The concerns are that of authentication, data confidentiality and privacy, data integrity, availability and rogue access point. Authentication-Most password-based protocols in use today rely on a hash of the password with a random challenge. The server issues a challenge, the client hashes that challenge with the password and forwards a response to the server, and the server validates that response against the user's password retrieved from its database. Legacy password protocols are easily subjected to eaves- dropping and man-in-the-middle attacks. An eavesdrop-ping attacker can easily mount a dictionary attack against such password protocols. A man-in-the-middle attacker can pass through the entire authentication and then hi-jack the connection and act as the user. Data

Privacy-Another concern is the security of the wireless data connection between the client and access point subsequent to authentication. While client and access point could easily negotiate keys subsequent to authentication, if the keys are not cryptographically related prior to the authentication, the data session would be subject to a man-in-the-middle attack. Therefore it is incumbent upon the authentication negotiation to result in keys that may be distributed to both client and access point to allow the subsequent data connection to be encrypted [9].

7. CONCLUSION

This paper set out to discuss wireless networks which are increasingly becoming preferred over wired networks by many users. The paper began by offering an overview of networking and then proceeded to define wireless networking and discuss the various technologies that are used. From the discussions provided in this paper, it is clear that wireless network solutions are increasing in popularity as they become more affordable and are adopted by more people. This paper has elaborated how wireless networks provide freedom from place restriction, scalability and flexibility. The most popular technologies are; Wi-Fi, WiMax. 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. It also stressed the importance of training and educating users in safe wireless networking procedures.

REFERENCES

[1] International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

[2] International Journal of Innovative Research in Computer and Communication Engineer in Vol. 1, Issue 4, June 2013

[3] International Journal of Multimedia and Ubiquitous Engineer Vol. 3, No. 3, July, 2008

[4] Kumar, a 2010, "Evolution of Mobile Wireless Communication Networks: 1G to 4G", International Journal of Electronics & Communication Technology, 1(1): 68-72.

[5] Malone S, 2004, Case Study: A Path towards a Secure, Multi-role Wireless LAN in a Higher Education Environment, SANS Institute, Massachusetts.

[6] Mamaukaris, K V and Economides, AA 2003, Wireless technology in educational systems. International PEG Conference, St. Petersburg.

[7] Reynolds, J 2003, Going Wi-Fi: A Practical Guide to Planning and Building an 802.11 Networks, CMP, New York.

[8] Schmidt, A & Lian, S 2009, Security and Privacy in Mobile Information and Communication Systems, Springer, Boston.

[9] Singh,L 2009, Network Security and Management, PHI Learning Pvt. Ltd., New Delhi.

[10] Int. J. Communications, Network and System Sciences, 2013, 6, 443-450