ISSN (Online): 2230-7893
www.IJCEM.org

Protection of Data for Unauthorized Access in Wireless Networks Security Aspects

Ravneet Kaur

Department of Computer science & Engineering
Beant College of Engineering & Technology,
Gurdaspur Punjab, India
reet.kahlon@gmail.com

Abstract

Modern communication networks have been becoming more and more large-scaled and complicated due to rapid development and interconnection among heterogeneous communication networks. Therefore, the management and maintenance of modern communication networks have posed many grand challenges to both industrial and academic communication communities. To overcome these challenges, it is very necessary to find new levels of autonomy and intelligence in designing, deploying, managing, and maintaining communication networks. Embedded software and systems are closely related to our daily life, which reside from smart appliances to unmanned trains. The present paper deals with the Protection of data for unauthorised access in Wireless Networks -security Aspects.

Keywords: *Wireless Network, Security, WLAN.*

1. Introduction

Security problems with the TCP/IP protocol suite were known (as noted by Steven Bellovin), but the Internet was a closed network for academics and researchers at the time. Spam and malware were minor problems, and the Web had not been invented. Security was understandably not one of the high priority concerns of the Internet designers 20 years ago, but the consequences of an open public Internet are now apparent 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. [1-3]

2. Security threats

The fundamentals of wireless security are largely similar to those of the wired Internet, wireless data networks present a more constrained communication environment compared to wired networks. Because of fundamental limitations of power, available spectrum and mobility, wireless data networks tend to have less bandwidth, more latency, less connection stability, and less predictable availability. Similarly, handheld wireless devices tend to have limited battery life, less powerful CPUs, restricted power consumption, smaller displays, and different input presenting a more constrained computing environment compared to desktop computers. [4, 5]

With a WLAN, transmitted data is broadcast over the air using radio waves. This means that any WLAN Client within an access point (AP) service area can receive data transmitted to or from the access point. Because radio waves travel through ceilings, floors, and walls data may hence easily reach unintended recipients. Tools like Ethereal; AirSnort can easily be used to passively collect data of any Client within the broadcast range. Users have no way of knowing if they are connecting to rogue access point set-up as part of a man-in-the-middle attack.

WLAN security, involves concern in three separate issues:

- Authentication
- User Privacy
- Authorization.

Multihop wireless networks are more unsafe as compared to wired or single hop wireless networks. Multilayer security attcks need to be considerded before the design of any security mechanism or intrusion detection system. [6-18]

Figure 1 shows Wireless Security Issues

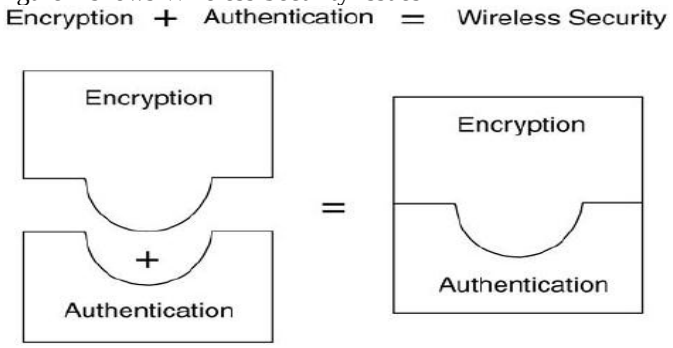

Fig. No. 1. Wireless Security Issues

3. Different Attacks

3.1 Layer Label

"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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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).

3.7 Network injection

In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcast 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.

3.8 Counteracting risks

Risks from crackers are sure to remain with us for any foreseeable future. The challenge for IT personnel will be to keep one step ahead of crackers. Members of the IT field need to keep learning about the types of attacks and what counter measures are available.

4. Mitigation of counteracting security risks

There are many technologies available to counteract wireless network intrusion, but currently no method is absolutely secure. The best strategy may be to combine a number of security measures. The following steps are required for security mechanism:

A. All wireless LAN devices need to be secured

B. All users of the wireless network need to be educated in wireless network security

C. All wireless networks need to be actively monitored for weaknesses and breaches

5. Conclusion

As the fastest growing industry, embedded systems will have great societal and environmental impacts. Therefore, the design and implementation of safe and efficient embedded software and systems have utmost importance. This paper concludes the latest steps taken to the security of wireless networks for the protection of the data from the unauthorised access.

6. Impact of study

Wireless mesh networking has been a cost-effective technology that provides wide-coverage broadband wireless network services. They benefit both service providers with low cost in network deployment, and end users with ubiquitous access to the Internet from anywhere at anytime. However, as wireless mesh network (WMN) proliferates, security and privacy issues associated with this communication paradigm have become more and more evident and thus need to be addressed.[19] The present study will be useful to provide a good foundation to implement real time detection.

Acknowledgement

The author is thankful to Dr. Jatinder Singh Bal (Dean and Professor, Computer Science & Engineering Desh Bhagat Enggineering College, Moga) for critical discussion as onell as constant help during the present study. The constant encouragement provided by Dr. H S Johal as onell as Mr. Dalwinder Singh and Deepak Prashar, Lovely Professional University Jalandhar is also acknowledged.

1.1.1.1.1 References

[1]. B.Mukherjee, L.T.Heberlein, And K.N.Levitt (1994) "Network Intrusion Dtetction", Ieee Network,May/June pp 8-10.

[2]. Dasgupta, D., et.al. (2002). *Cougaar Based Intrusion Detection System (Cids).* Cs Technical Report No. Cs- 02- 001, February 4.

[3]. Debar, H., Dacier, M. And Onespi, A. (1999). "Towards A Taxonomy of Intrusion-Detection Systems". Computer Networks, 31, Pp. 805-822.

[4]. Denning D., (1987) "An Intrusion-Detection Model", IEEE Transactions On Software Engineering, Vol. Se-13, No. 2, Pp.222-232.

[5]. Jeyanthi Hall (2005) "Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting" IEEE Transactions on Dependable And Secure Computing 12, July. Pp 18-22.

[6]. Lim, Y, T. Schmoyer, J. Levine and H. L. Oonen. June (2003). "Wireless Intrusion Detection and Response." In Proceedings Of The 2003 IEEE Workshop On Information Assurance United States Military Academy, Ny: Onest Point. Pp 22-26.

[7]. Rakesh.S, (2010) "A Novel Cross Layer Intrusion Detection System in MANET "24th Proc. IEEE International Conference on Advanced Information Networking and Applications. Pp 38-48.

[8]. S.Madhavi,(2008)"An Intrusion Detection System In Mobile Adhoc Networks**"** International Journal of Security and Its Applications Vol. 2, No.3, July. Pp 11-17.

[9]. Shafiullah Khan (2010) "Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks", The International Arab Journal of Information Technology, Vol. 7, No. 4, October.pp 50-55.

[10]. I.F. Akyilidz, "Cross layer design in wireless mesh networks", available online at http://www2.ing.unipi.it/ meshtech08/files/meshtech08 _akyildiz.pdf.

[11]. W.steven,jan kryus, kyeongsoo kim, juan carlos zuniga "802.11s tutorial overview of the amendment for wireless.

[12]. Shafiullah Khan, Kok Keong Loo, Zia Ud Din, "cross layer design for routing and security in multi-hop wirelessnetworks" in Journal of Information Assurance and Security pp.170-173, 2009.

[13]. Akyildiz, I.F, Xudong Wang "Cross-Layer Design in Wireless Mesh Networks" in Vehicular Technology, IEEE Transactions on Volume 57, Issue 2, pp. 1061 – 1076, March 2008.

[14]. Hu Onenjie, "Cross layer design in wireless mesh networks" available online at: "http://www.asiafi.net/meeting/2008/ presentations/2-20/PDF-oneb/Onenjie%20Hu.pdf.

[15]. Muhammad, M. Salleh, N.M.; Zakaria, M.S.; Gannapathy, V.R.; Husain, M.N.; Ibrahim, I.M.; Johal, M.S.; Ahmad, M.R.; Aziz, M.Z.A.A, **"**Physical and MAC Cross Layer Design for Wireless Mesh Networks" in Applied Electromagnetics, 2007, APACE 2007. Asia-Pacific Conference on Volume, Issue, 4-6, pp.1 – 5. December 2007 local area networking" in ieee802 plenary, dallas , November ,2006.

[16]. Zhang, Y and W. Lee, (2000)." Intrusion Detection In Wireless Ad-Hoc Networks. "In Proceedings Of The Sixth Annual International Conference On Mobile Computing And Networking, Boston: Massachussetts, August 6-11, pp 26-31.

[17]. Xia Wang, Johnny S. Wong, Fred Stanley and Samik Basu (2009) "Cross-layer Based Anomaly Detection in Wireless Mesh Networks "Ninth Annual International Symposium on Applications and the Internet.

[18]. J.S. Bal et.al. (2009), "A cross layer based intrusion detection technique for wireless network", International Journal of Computer Science & information security. Vol 5, Paper No. 25080924, Sept. 2009

[19]. Akyildiz, I.F.; Xudong Wang A survey on wireless mesh networks in Communications Magazine, IEEE Volume 43,Issue 9, pp. S23 - S30, September 2005.

Author - Ravneet kaur did his B.tech and M.Tech in Computer Science Engineering in 2008 and 2010 respectively. She has been working as a lecturer in Departmernt of Compter Sceince and Engineering in Beant College of Engineering Gurdaspur for last 3 years. She has attended several workshops/ courses. She has published research papers of international/National repute in different journals /conferences. Her areseasrch area interest includes wireless security as well as computer communication network.