ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 10, December 2012

Various Security Threats and Issues in Wireless Networks: A Survey

D.Prabakar, Dr.M.Marikkannan , Dr.S.Karthik

Abstract -**In rapid change of wireless transmission, the organizations are need to understand the range of security threats endemic to wireless technologies, including eavesdropping, wireless denial-of-service (DOS) attacks, and various encryption issues. The security threats of wireless networks are (1) Interception of law enforcement data on specialized mobile radio, private radio (2) Interception of credit card authorizations over wireless networks (3) Stealing of cellular airtime (4) Interception of e-mail messages on wireless Internet connections (5) Physical breach of security at unmanned base stations or other communications centers. In this paper clearly points out the various threats and issues in Wireless Networks.**

Index Terms- **Eavesdropping, DOS attacks, Security threats.**

I.INTRODUCTION

Tremendous advantages can be realized by using wireless technology. Wireless technology gives users the freedom of mobility, gives network designers more options for connectivity, and gives many new devices the capability to connect to networks. However, wireless technology brings significantly more threats than traditional wired networks. The major difference between wired and wireless networks is the anonymous, uncontrolled coverage areas between the end points of the network [1][5]. In wide area cellular networks, the wireless medium cannot be controlled at all. Current wireless networking technology offers little to control the coverage area. This enables attackers in the immediate vicinity of a wireless network to perform a number of attacks that are not found in traditional wired networks. This chapter will review the threats that are unique to wireless environments, the equipment required by the attacker to successfully leverage the threats, the problems that occur when roaming from one cell to another, the covert wireless channels, and the cryptographic pitfalls prone to open medium communications. Some Security Goals every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

- Authentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified.
- Secrecy or Confidentiality: Usually this function (feature) is how most people identify a secure system. It means that only the authenticated people are able to interpret the message (date) content and no one else.
- Integrity: Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.
- Non-Repudiation: This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.
- Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems should provide a way to grant their users the quality of service they expect.

D.Prabakar - *Assistant Professor, Dept of CSE, SNS College of Technology- Coimbatore, India*

Dr.M.Marrikkannan - *Professor, Dept of CSE, Institute of Road and Transport Technology- Erode, India.*

Dr.S.Karthik - *Professor and Dean, Dept of CSE, SNS College of Technology- Coimbatore India.*

II. RELATED WORKS

Wireless data networks have spread between home users and companies in an increasing fashion. The main reason behind this fast adaptation is due to the nature of wireless networks where it provides the flexibility and freedom that wired networks lack. The increasing of bandwidth capabilities has inspired people to think seriously about replacing wired networks with wireless networks especially in places where it is hard or expensive to have wired networks [4]. One of the main places that can benefit from these ideas is rural areas, where wired networks infrastructure is either difficult or impossible to create due to physical obstacles. In order to protect these networks, here we described the various possible threats and issues in wireless networks, the following section briefly introduce the various threats and issues related to wireless networks, like us Eavesdropping , Communications Jamming ,Denial of Service (DoS) Jamming ,Injection and Modification of Data, Man-in-the-Middle (MITM) Attacks, , Attacker Equipment ,Covert Wireless Channels , Roaming Issues ,Cryptographic Threats.

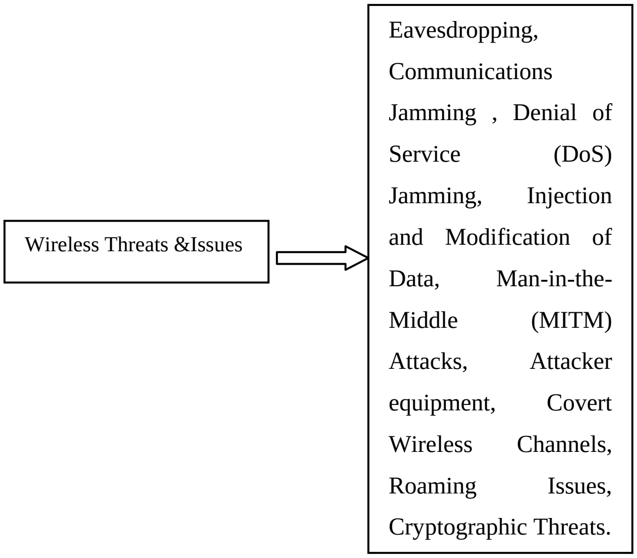
Wireless Threats &Issues
Eavesdropping, Communications Jamming , Denial of Service (DoS) Jamming, Injection and Modification of Data, Man-in-the-Middle (MITM) Attacks, Attacker equipment, Covert Wireless Channels, Roaming Issues, Cryptographic Threats.

Figure 1.1 Various Wireless Threats and Issues

A. Eavesdropping

Eavesdropping is used to gather information on the network under attack. The primary goals of the attacker are to understand who uses the network, what is accessible, what the capabilities of the equipment on the network are, when it is used least and most, and what the coverage area is. This information is needed to launch an attack on the target network. Many commonly used network protocols transmit sensitive data such as username and password information in clear text. An attacker may use captured data to gain access to network resources [3]. The equipment used to perform eavesdropping on the network can be as simple as the equipment used to gain access to the network itself. The attacker must be in proximity to the transmitter in order to receive the transmission. These types of attacks are nearly impossible to detect and even harder to prevent.

B.Communications Jamming

Jamming occurs when an intentional or unintentional interference overpowers the sender or receiver of a communications link, thereby effectively rendering the communications link useless. An attacker can apply jamming in several ways. Most of the wireless networking technologies utilizes unlicensed frequencies. Therefore, many devices such as cordless phones, baby monitors, and microwave ovens may interfere with wireless networking and effectively jam the wireless communications [2]. The following figure 1.2 despites Jamming attack in Networks

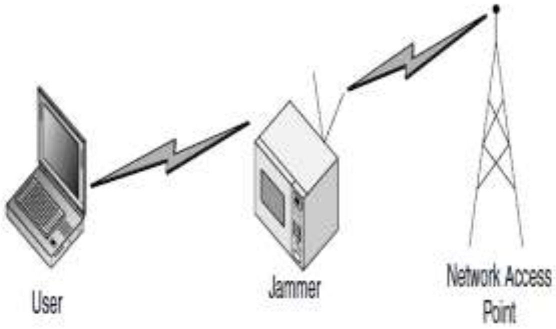

Figure 1.2 Jamming attack in Networks

C.Denial of Service (DoS) Jamming

Jamming the entire network can cause a denial of service (DoS) attack. The entire area, including both base stations and clients, is flooded with interference so that no stations can communicate with each other. This attack shuts down all communications in a given area. This type of attack can require a significant amount of power if applied to a broad area [6]. DoS attacks on wireless networks may be difficult to prevent and stop. Furthermore broad into two categories (1) Client Jamming a client station provides an opportunity for an anonymous client to take over or impersonate the jammed client. Jamming also can be used to DoS the client so that it loses connectivity and cannot access the application.

A more sophisticated attack may attempt to interrupt connectivity with the real base station to then reattach with a problem in station.(2) Base Station Jamming a base station provides an opportunity for a problematic base station to stand in for the legitimate base station. The jamming can also deprive clients of service or a telecom company from revenue.

D .Injection and Modification of Data

Injection attacks occur when an attacker adds data to an existing connection in order to hijack the connection or maliciously send data or commands. An attacker can manipulate control messages and data streams by inserting packets or commands to a base station and vice versa. Inserting control messages on a valid control channel can result in the disassociation or disconnection of users from the network. Injection attacks can be used for DoS [8]. An attacker can also flood the network access point with connect messages, tricking the network access point into exceeding a maximum limit, thereby denying authorized users access to the network.

E. Man-in-the-Middle (MITM) Attacks

MITM attacks can take many forms and are designed to subvert the confidentiality and integrity of the session. MITM attacks are more sophisticated than most attacks and require significant information about the network [5]. An attacker will normally impersonate a network resource. When a victim initiates a connection, the attacker will intercept the connection, and then complete the connection to the intended resource and proxy all communications to the resource. The attacker is now in a position to inject data, modify communications, or eavesdrop on a session that would normally be difficult to decode, such as encrypted sessions.

F. Attacker Equipment

The equipment used by the casual attacker can minimally consist of a wireless network interface. This can either be a wireless Ethernet network interface card (NIC), a General Packet Radio Service (GPRS), or a Cellular Digital Packet Data (CDPD) cellular telephony handset connected to a laptop either as a Personal Computer Memory Card International Association (PCMCIA) card or through some communications link [6]. Advanced attackers will sometimes employ this wireless interface in conjunction with jammers and specialized software. Cellular network attackers will generally use a configuration as depicted in Figure 1.3, because the network coverage is understood and generally covers a large area.

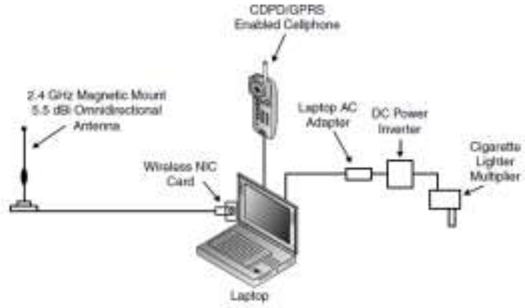
CDPD/GPRS Enabled Cellphone
2.4 GHz Magnetic Mount 5.5 dBi Omnidirectional Antenna
Laptop AC Adapter
DC Power Inverter
Cigarette Lighter Multiplier
Wireless NIC Card
Laptop

Figure 1.3 Attacker hardware Configuration

G. Covert Wireless Channels

Due to the low cost of wireless access points and the ease of creating software-based access points consisting of a standard desktop or laptop computer and a wireless NIC, one must be vigilant in detecting incorrectly configured or unintentionally deployed wireless equipment on the wired network, such as the network backdoor shown in Figure 1.4 This equipment can poke very damaging holes in the fabric of the wired infrastructure, which will be exposed to attackers within several miles of a target network[8].

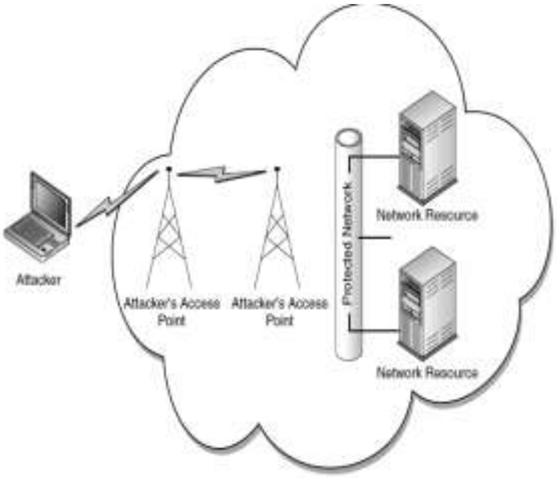

Figure 1.4 Attacker can access the data through Access point

A similar configuration can also bridge air-gap networks via a wireless channel and funnel data from an air-gapped network outside a protective building by chaining access points together until the final leg of the link leaves the confines of the building.

This configuration can effectively increase the amount of coverage area to many miles. The equipment needed for this configuration is very inexpensive and may be purchased at most electronic stores.

H. Roaming Issues

The concept of roaming on Code-Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), and wireless Ethernet are all very similar. Many Transmission Control Protocol/ Internet Protocol (TCP/IP) network applications require the IP address of the server and the client to remain static; however, when roaming among a network, you will undoubtedly be required to leave and join across subnets. This requirement is the drive behind mobile IP and other wireless network roaming mechanisms [6].

K. Cryptographic Threats

Wired Equivalent Privacy (WEP) is a cryptographic mechanism designed to provide security for 802.11 networks [2]. Implementation flaws and key management issues have proved WEP almost useless. WEP was designed with a single static key that was to be used by all users. Controlling access to these keys, changing the keys frequently, and detecting compromises is nearly impossible. An examination of the implementation of the RC4 algorithm in WEP has revealed weaknesses that enable an attacker to completely recover the key after capturing minimal network traffic. Tools are available on the Internet that allows an attacker to recover the key in a number of hours. Therefore, WEP cannot be relied on to provide authentication and confidentiality on a wireless network.

III Conclusion

Understanding the threats to wireless technology is the first step in securing wireless implementations. The advantages of using wireless are tremendous. Therefore, these threats need to be considered, but should not stop the deployment of wireless applications. Taking a few simple security measures can dramatically reduce the impact of many common attacks. The further study on wireless security will help to show what steps can help to reduce wireless threats.

REFERENCES

[1] J. WELCH, S. D. LATHROP, A Survey of Wireless Security Threats and Security Mechanisms. United States Military Academy West Point,New York, (2010).

[2] I. MARTINOVIC, F. A. ZDARSKY, A. BACHOREK, C.JUNG, J. B. SCHMITT, Phishing in the Wireless: Implementation and Analysis. Kaiserslauterer Uniweiter Elektronischer Dokumentenserver, Universitatsbibliothek Kaiserslautern, (2011).

[3] F. RANGO, D. C. LENTINI, S. MARANO, Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack inWi-Fi Protected Access and IEEE 802.11i. EURASIP Journal on Wireless Communications and Networking, Hindawi Publishing Corporation, pp. 1–19, (2009).

[4] N. BORISOV, I. GOLDBERG, D.WAGNER, Intercepting mobile communications: the insecurity of 802.11. In Proceedings of the 9th Annual International
Conference on Mobile Computing and Networking, Rome, Italy, (2011).

[5] L. BLUNK, J.VOLLBRECHT, B.ABOBA, J. CARLSON,H. LEVKOWETZ, Extensible Authentication Protocol (EAP). Internet Draft draft-ietf-eap-rfc2284bis-06.txt, (2008).

[6] G. RUPINDE, S. JASON, C. ANDREW, Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks. Proceedings of the 2006 Australasian workshops on Grid computing and e-research, Vol. 54, pp. 221–230, (2010).

[7] IBM Corporation, “Security Research: Wireless Security Auditor (WSA),” 2011. Available:http://www.research.ibm.com/gsal/wsa

[8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Request for Candidate Algorithm Nominations for the Advanced Encryption Standard. Federal Register, September 12, (2009).

[9] Yi P, Wu Y, Zou F, Liu N. A Survey on Security in Wireless Networks. IETE Tech Rev [serial online] 2010 [cited 2012 Dec 26];27:6-14. Available from: http://tr.ietejournals.org/text.asp?2010/27/1/6/58969

AUTHORS PROFILE

PRABAKAR.D, received B.E Degree in Computer Science and Engineering from the Anna University, Chennai, in 2004 and Master's Degree in Computer Science and Engineering in Anna University of Technology, Coimbatore, in 2008. At present, He is an Assistant Professor of Computer Science and Engineering in SNS College of Technology, Coimbatore. His research interest focuses on Wireless Communication, Mobile Computing and Wireless Sensor Networks.

Dr.M.Marikkannan, received the B.E. degree in computer science and engineering from the Government College of Engineering, Tirunelveli, India in 1994, M.E.degree in computer science and engineering from College of Engineering, Anna University, and Chennai, India in 1999. PhD in computer science and engineering from College of Engineering, Anna University, and Chennai, India in 2009.Currently, he is a professor at the Department of Computer Science and Engineering, Institute of Road and Transport Technology (IRTT), Erode, India. His research interests include temporal database management systems and object oriented systems.

Dr.S.Karthik, is presently professor & Dean in the department of computer science and engineering, SNS College of Technology, affiliated to Anna University-Coimbatore, Tamilnadu, India. He received the M.E. degree from Anna University-Chennai and Ph.D. degree from Anna University of Technology, Coimbatore. His research interests include Network security, web services and wireless systems. In particular, he is currently working in a research group developing new Internet Security architectures and active defense systems against DDoS attacks. Dr.S.Karthik published more than 35 papers in refereed international journals and 25 papers in Conferences and has been involved many international conferences as Technical chair and tutorial presenter. He is an active member of IEEE, ISTE, IAENG, IACSIT and Indian Computer Society.