Security Approaches in Wireless Home Networks – The Incipient drifts and Surviving Glitches

Dhowmya Bhatt, Ekata Gupta

Abstract- the usage of wireless Networks have almost become inevitable for the human community. From a simple point to point communication to extra-large-area covering networks, wireless communication is a significant part and parcel of technological progress that mankind has ever made. As the vast convention of wireless has increased than ever before, it also becomes the matter of concern of how to protect these networks from attacks and attackers and ensure the users safe and secured communication. It is worthwhile to note that the Right to the protect the moral and material interests resulting from any scientific production owned by an individual is one of the basics of Human rights declaration. Hence it is very much essential to implement and practice methods to secure wireless networks in a very strict manner so as to ensure confidentiality of the information transmitted and ensure people involved communication some absolutely reliable safety. The attempt to safeguard home wireless networks will greatly benefit mankind which not otherwise would be a huge loss to the entire human community. This Paper is an effort to throw light on the upcoming trends in securing wireless networks and the external threats to these networks. Possible future directions are also addressed towards the end.

Keywords – security, privacy, attacks, intruders

I. INTRODUCTION

The Wireless networks add an extra level of security complexity compared to the wired networks because propagate through the air and are naturally easier to intercept. Signals from most wireless networks pass through exterior walls and into nearby houses where an intruder can easily access them. Network engineers and other technology experts have closely scrutinized wireless network security because of the open-air nature of wireless communications. In earlier times, two computers were together involving some physical medium running between them such as a cable [2]. But, one of the easiest and least messy ways to network computers throughout is to use the wireless technology. The problem with having the signal broadcast through a wireless network is difficult because its tough to predict where that signal may travel.Also it is very essential that every home must determine themselves the level of risk they are comfortable in taking when implementing a wireless network. The better a wireless network is administered, the more secure it becomes for home usage. The risks to users of wireless networks have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced because it took time for intruders to find a way to crack down networks [6]. As the innovative trends are increasing in the wireless networks so have become the problems to safeguard them.

Manuscript received September 02, 2012.

Dhowmya Bhatt, Research Scholar, Mewar University, Chittorgarh (Rajasthan), India.

Ekata Gupta, Associate Professor, Department of Mathematics, Krishna Institute of Engineering and Technology, Ghaziabad(U.P.), India.

II. THE LEADING EDGE IN WIRELESS NETWORKING

The wireless networking concept is rapidly evolving, both as a technology and in the merging with adjacent technologies. The standards are surfacing in a number of areas, especially the 802.11n. This standard will enable high-throughput wireless communications ranging from 100Mbps - 300Mbps based on the situation [3]. This is considered to be a dramatic improvement over the current effective throughput of 36Mbps, but more often in the 1 to 10Mbps range for most wireless network users.

The wireless networks have become popular and used widely because of few of its features that are user friendly as well as fast. Their frontiers have become ever expanding and limitless. Some of the trends set by the wireless networks that deserve mentioning are their,

- Speed and additional data download
- Availability of Better methods to secure transactions
- Easy sharing of resources
- Integration of more functions to a single handheld device
- Variety of devices - more and better options for users to choose
- Easy connectivity
- Usage of Self- healing techniques

It is interesting to note that few trends have recently emerged in wireless networking and have gained immense popularity among the users because of the advance features incorporated by them for better security. To mention some of them,

- Wireless LAN's comfy with the wireline network
- The rise of the WAN
- Networking the data center
- Perimeter defense - Network behavioral analysis and data loss prevention
- Fixed-Mobile Convergence and Dual Mode

III. THREATS TO WIRELESS NETWORKS

It is actually difficult to say why using wireless networks can be unsafe when it is the most efficient and flawless way of communicating with much less fuss. At the same time it is again tough to say when intrusions started and intruders and crackers began to access information when transmitted through wireless networks [7]. Not all crackers intrude network to access information. Some do it just for pleasure without bothering what the information is actually, while few others particularly intrude for some confidential information such as program code, keywords or passwords.

A User within the geographical network range of an open or an unencrypted wireless network can 'sniff' or capture and record the traffic, gain unauthorized access to internal

network resources as well as to the internet, and then use the information and resources to perform disruptive acts. Most of these are illegal usage. Such security breaches have become important concerns for home networks, especially when the user does not know that his network is being misused by some third party [5]. If router security is not activated or if the owner deactivates it for convenience, it creates a free hotspot. Since most of the latest laptops have wireless networking built in they do not need a third-party adapter such as a PCMCIA Card or USBdongle. Built in wireless networking might be enabled by default, without the owner realizing it, thus broadcasting the laptop's accessibility to any computer nearby [7].

The lack of knowledge among the users about the security issues inherent in setting up such systems often may allow others nearby access to the connection. Such "piggybacking" is usually achieved without the knowledge or the permission of the wireless network operators [9]. But some time an unusual situation might be encountered when intrusion occurs without the knowledge of the intruding user, or if their computer automatically selects a nearby unsecured wireless network to use as an access point.

I. Types of Attacks On Home Networks

There are a number of attacks that wireless home networks may face. There are certain attacks that take place without the knowledge of the user himself that are more dangerous than the ones that are expected to take place. A particular wireless network may face threats of more than one type. Such situations become very critical to handle for the host system. Many system hang or get corrupted when the information gets hacked by two or more intruders [4]. It is always essential for users to beware of such threats to their wireless networks.

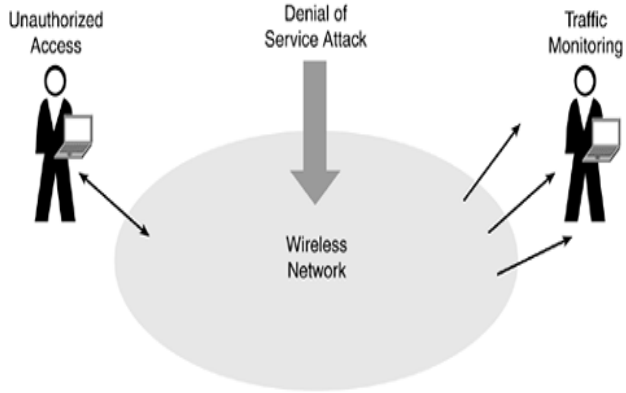

Fig.1. Common attacks on wireless home Networks

Few of such that can make wireless home networks unsafe are,

- Rogue Access Points or Ad-hoc Networks
- Denial of Services
- Configuration Problems
- Passive Capturing
- Unauthorized Access
- Man-in-middle attacks
- Warchalking

IV. ATTACKS ON WIRELESS HOME NETWORKS – A CURSE

I. Rogue Access Points

Even if the user implements all security controls on access points, the possible connection of a rogue access point is a significant threat. A rogue access point is an unauthorized access point on the network. A common example of this can be that an employee might purchase an access point and install it within his office without knowing the security implications and sell information to the rival corporate [10]. A hacker could also plant a rogue access point within a facility by purposely connecting an unprotected access point to the corporate network. Rogue access points are mainly used to steal from the parent network some part of the confidential information from which the entire information can be easily retrieved. Specific weak points are identified by the intruder from where he could gain control of the information and those points are attacked [9].

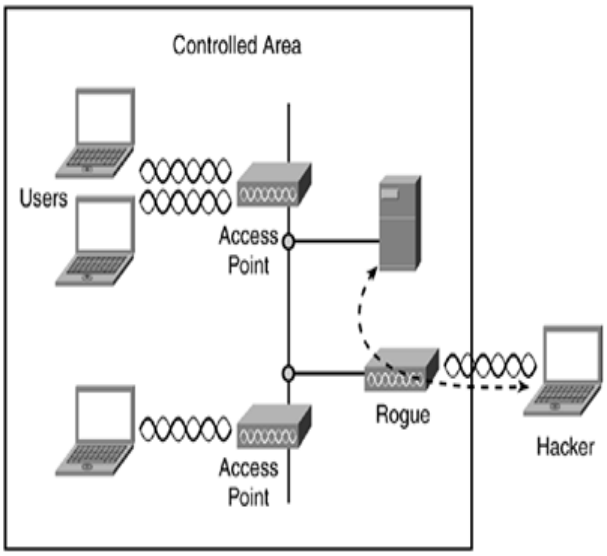

Fig.2. Rogue Access Points

II. Denial of Services

Denial of Service (DoS) attack is an assault that can cripple or disable a wireless network. In this attack, the network is unavailable to the user for an indefinite period of time.

The severity of the DoS attack depends on the impact of the attack on wireless networks becoming inoperative. For example, a hacker could a user's home wireless LAN, but the result will probably just inconvenience the homeowner [12]. A DoS attack that shuts down a huge wireless inventory system could cause major financial loss.

III. Configuration Problems

Simple configuration problems are often the cause of many vulnerabilities, this is because many consumer or the SOHO grade access points gets marketed with no security configuration [1]. An intruder who pretends to be like any common user can set up one of these devices quickly and gain access. However they also open up their network to external use without further configuration.

Other potential issues with configuration include weak passphrases, weak security deployments like the WEP vs WPA vs. WPA2 and default SSID usage among others. This issue has to be dealt keenly by the user while installing the wireless network.

IV. Passive Capturing

Passive capturing is performed by simply getting

within range of a target wireless LAN and then listening and capturing data. This information can be used for a number of things including attempting to break existing security settings and analyzing non-secured traffic. It is almost impossible to really prevent this type of attack because of the nature of a wireless network; what can be done is to implement high security standards using complex parameters.

V. Unauthorized Access

Similar to monitoring a wireless application, a hacker can effortlessly access a home wireless network from outside the facility if the proper precautions are not taken. Hackers can do this with much ease just by sitting in a parked car or can associate with one of the wireless base stations located inside a building [11]. Without proper security, this hacker can even access servers and applications residing on the network service providers thereby gain control over any home network he wants to access connected to this.

Unfortunately, many service providers to home networks deploy their networking service using the default, unsecured base station configurations, making it possible for the intruders to interface with their application servers. In a survey in the capital recently, it has been found that 30 percent of the wireless LAN access points in an average do not deploy any form of security. This allows easily the intruders to access hard drives and use resources such as the dedicated internet connections.

The Windows XP operating system makes it easy to interface with any home wireless network, especially on a given public-wireless LANs. When a laptop associates with a wireless LAN, the user can navigate with or to any other laptop associated with the same wireless LAN. Without personal firewall protection, the intruder can easily browse through the hard drive. This is a tremendous security risk.

VI. Man – In – Middle Attacks

In man-in-the-middle attack, the hacker places a fictitious device between the users and the wireless network. For example, a common man-in-the-middle attack exploits the common address resolution protocol (ARP) that all TCP-IP networks utilize. A hacker with the right tools can exploit ARP and take control of the entire wireless network causing great damage to the whole information [13]. A hacker can fool a station by sending, from a rogue network device, a fictitious ARP response that includes the IP address of a legitimate network device and the MAC address of the rogue device. This causes all legitimate stations on the network to automatically update their ARP tables with the false mapping.

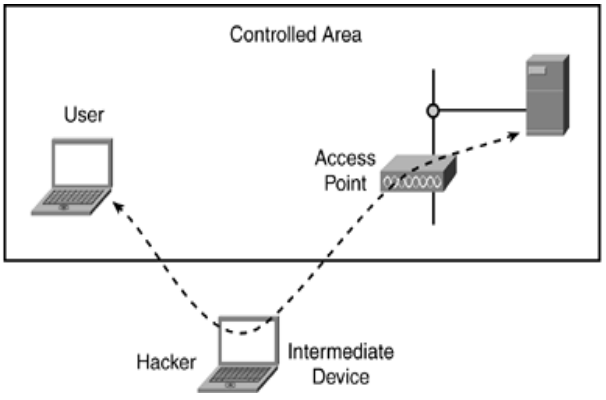

Fig.3. Hacker in between user and service provider

VII. Warchalking

Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network.

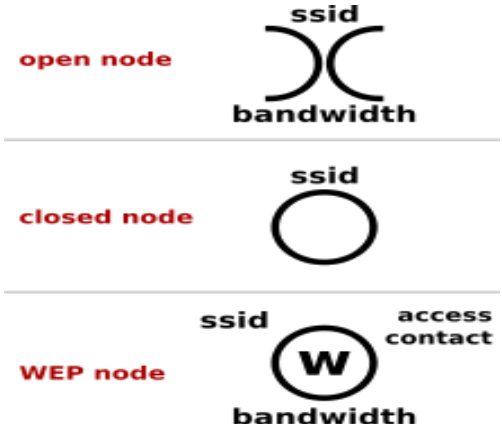

Fig.4. First introduced symbols of warchalking

Inspired by hobo symbols, the warchalking marks were conceived by a group of friends in June 2002 Of Matt Jones who designed the set of icons and produced a document containing them. There are three basic designs that are currently used: a pair of back-to-back semicircles, which denotes an open node, a closed circle, which denotes a closed node, a closed circle with a "W" inside, which denotes a node equipped with WEP [5]. Warchalkers also draw identifiers above the symbols to indicate the password that can be used to access the node, which can easily be obtained with sniffer software.

The word is formed by analogy to wardriving, the practice of driving around an area in a car to detect open Wi-Fi nodes. That term in turn is based onwardialing, the practice of dialing many phone numbers hoping to find a modem.

Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. Those offering Wi-Fi service might also draw such a symbol to advertise the availability of their Wi-Fi location, whether commercial or personal.

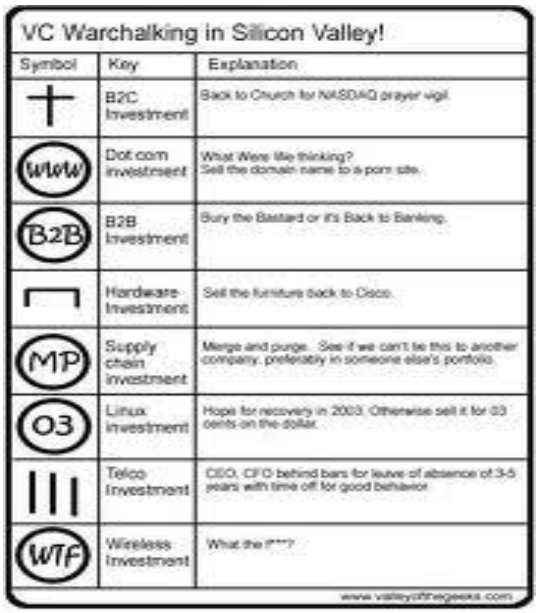

Fig.5. Latest set of symbols used by warchalkers

V. SECURING WIRELESS HOME NETWORKS

The nature of a wireless network is to provide easy access to end users, but this ease of access creates a more open attack surface. Unlike a wired network that requires an attacker to physically access part of the network, a wireless network only requires that the attacker be in close proximity.

The best attitude to take towards wireless security by any user is to be constantly vigilant and ensure that the security used on a wireless network is adapted as the standards change to ensure a high level of security [14]. Besides standard and conventional methods suggested by companies providing security services to users, the end-users can themselves note and take some simple precautionary methods to secure their home networks and PC's. Some of simple yet effective ways to safeguard home networks are as suggested below,

- Enabling encryption on Access Points
- Setting passwords for Routers
- Changing the SSID's from that of the original manufacturer
- Enabling always the SSID broadcasting
- Enabling MAC Address filtering on access points and routers
- Disabling remote Logins
- Disabling wireless administrating

VI. LATEST SECURITY TRENDS IN WIRELESS HOME NETWORKS – THE FUTURE

Home wireless networks need to employ latest methods of security so as to ensure users that their transaction is completely safe. The faster the technology of wireless networks have improved, the problems posed to the security of these networks have increased than ever before. The hackers are themselves using latest techniques to steal information even from the heavily guarded networks [3]. Hence it has become essential to introduce and practice innovative trends to protect information shared across wireless home networks.

Fig.6. security implementation pattern in the present day wireless home networks

As mentioned earlier, the users themselves need to realize, understand and implement the apt trend that suits their system. Not following the universal trend of security and trying to find out what is suitable for a specific network will help to secure wireless networks better. The users can also follow these latest methods of securing their home networks besides following the already existing conventional measures for security.

- Installing features like WEP, SSID, MAC filtering
- Installing a monitored home security system
- Unified threat management System
- Multilayered security approach with segmentation

VII. CONCLUSIONS

Security of any form to guard networks, users, and information has become the primary concern of service providers, organizations and most importantly the consumers. Hence it has become the responsibility of all to safeguard the confidentiality of the information sent shared and received across the wireless networks. Though home networks are only a part of wireless networks, these days working from home using wireless networks has become very common and so it is equally important that home wireless network are as safe as to use like the corporate players guard their networks. While organizations largely investments in securing their networks, home users should also be keen in regularly updating security trend to guard their PC's. zero level tolerance should be exhibited towards any kind of security breach when detected. These measures along with technical implementations of trends will help to make home wireless networks safer and better to use.

REFERENCES

1. C. Rapier and B. Bennett, "High speed bulk data transfer using the database chainingl", MG '08: Proc. of 15th ACM Mardi Gras Conference. pp. 1-7, 2008.
2. M. Mathis, J. Heffner, P. O'Neil, P. Siemsen, "Pathdiag: Automated SVChosting", PAM 2008.
3. A. Adams, M. Mathis, "A System for Flexible Network Performance Measurement," Proceedings of INET 2000, July 2000.
4. V. Paxson, A. Adams, M. Mathis, " Experiences with chaining," Proceedings of the Passive and Active Measurement Workshop 2000, April 2000.
5. A. Adams, A. J. Lee, and D. Mossé, "Receipt-Mode Trust Negotiation: Efficient Authorization Through Outsourced database Interactions," in Proceedings of the Sixth ACM Symposium on Information, Computer, and Communication Security (ASIACCS 2011), March 2011.
6. J. C. Honig, D. Katz, M. Mathis, Y. Reckhter and J. Y. Yu, "Applications of database chaining in the Internet", June 1990, RFC1164 USC/Information Sciences Institute.
7. R. L. Clay, J. Mahdavi, G. J. McRae, "Scheduling in the Presence of Uncertainty in database chaining. The Linear Assignment Problem," Proceedings of AICHE National Meeting, August, 1991.
8. www.quikr.com.
9. http://dbmmo.com/
10. www.it.iitb.ac.in/~palwencha/assg/wlan_sec.pdf www.ece.tamu.edu/~reddy/ee689.../indira-monica.pdf
11. www.wireless-technology-advisor.com/ wireless-technology-trends.html
12. www1.cse.wustl.edu/~jain/cse574-06/ftp/j_2trn.pdf
13. www.afn.org/~afn48922/downs/wireless/wireless_wan.pdf
14. www.smallbusinesscomputing.com/.../Wireless-Network-Security-A