Evolution of Wi-Fi and Security Issues

A.Zaman and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Wi-Fi technologies are evolving with quick pace providing high speed broadband access to users at places where it was not possible before using wired technologies. Although, there are several benefits of Wi-Fi over wired technologies, there are several security issues that expose Wi-Fi technologies to hackers and intruders. This paper discusses about adoption of Wi-Fi technologies among users and security threats that can be harmful to Wi-Fi technologies.

Keywords

Wi-Fi, War driving, DoS, Malware, E-mail, Spoofing

1 Introduction

Wi-Fi technologies were introduced around a decade ago with devices providing data rate comparatively low as compared to modern Wi-Fi standards. The utilization of Spread Spectrum (SS) techniques for low power signal transmission over license-free wide band was an important feature of these wireless devices. Although, SS techniques were effectively employed for military-purpose communication during Second World War, it was not unitl mid-1990s that wireless devices were introduced for Internet and local network applications. The elimination of wires between devices for transmission purposes is considered as an attractive aspect of Wi-Fi networks.

2 Benefits of Wi-Fi technologies

Perhaps the biggest advantage of Wi-Fi technologies is the communication without any physical medium between wireless devices. This freedom of Wi-Fi communication provides mobility to the users so they can use their devices at remote locations. However, mobility offered by Wi-Fi devices is not the only benefit of this technology. Wi-Fi technologies also provide high speed broadband facility to their users who can access Internet through wireless connection to infrastructure devices. Wi-Fi solutions are also cost effective as compared to wired technologies for several reasons. There is no need to setup cables for connection between wireless devices and Internet access that reduces the cost of installation of these devices. Wi-Fi technologies are reasonably easy to use and it is not difficult to configure and manage these devices. Wi-Fi technologies are also suitable for providing network access to enterprise users at locations where wired solutions are not feasible. Figure 1 is showing the results of a survey to illustrate the use of Wi-Fi technologies at

various locations with respect to enterprises. It is interesting to observe that around 80% of Wi-Fi usage in enterprises is in guest areas, lobbies, and conference and meeting rooms.

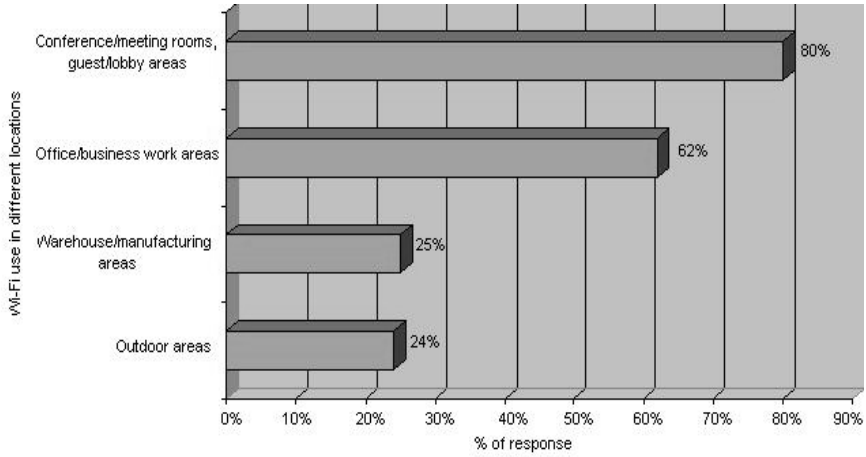

Figure 1: Wi-Fi usage at various locations in enterprises (Wexler, 2006)

3 User Attitude towards Adoption of Wi-Fi Technologies

Earlier Wi-Fi devices were comparatively expensive with respect to data rate support provided on these devices. However, with quick decline in cost of Wi-Fi devices and more data rate support with advanced techniques, users moved quickly towards Wi-Fi technologies. The flexibility provided by Wi-Fi in terms of mobility and ease of use has attracted residential users especially towards this technology. According to IDC, the overall Wi-Fi market value for Western Europe reached to $1.2 billion for first half of 2006 with 22% increase from second half of 2005 (IDC, 2006). The main factor behind this growth is the adoption of Wi-Fi technologies from residential sector that contribute major share of overall Wi-Fi market. The main reason behind this huge popularity of Wi-Fi technologies among residential users besides other factors described above is the lack of technical knowledge of home users. Wi-Fi technologies are generally easy to configure and manageable that requires little or no technical knowledge for installation and configuration purposes. Figure 2 below is also showing predicted increase in Wi-Fi users in different regions of the world from 2004-2009.

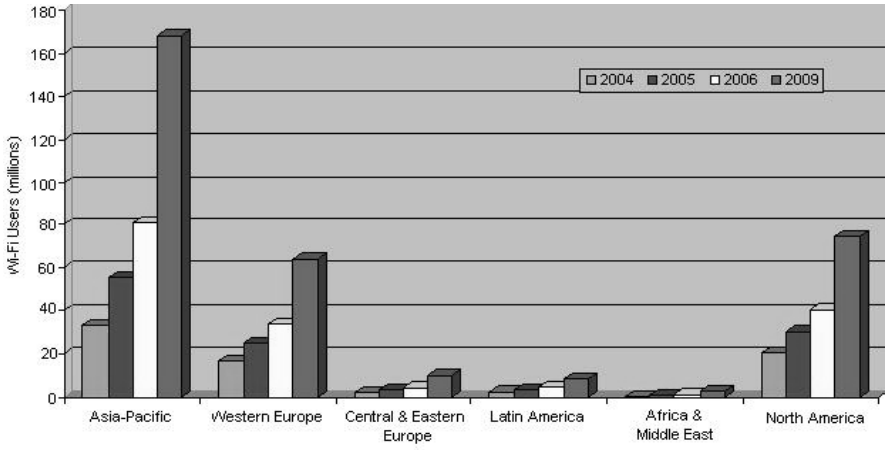

Figure 2: Expected Wi-Fi users with respect to different regions from 2004-2009 (Pyramid Research, 2005)

The introduction of new Wi-Fi solutions from manufacturers for better performance through centralized management and control capabilities is also attracting enterprise users to Wi-Fi technologies. WLAN switches are the example of centralized Wi-Fi solution for better management. According to Infonetics Research, wireless LAN switch market is expected to reach $4.1 billion by 2008 (ITFacts Wireless data, 2005). This figure clearly illustrates the interest of enterprise users in Wi-Fi technologies.

4 Security Issues of Wi-Fi Technologies

Although, mobility and flexibility provided by Wi-Fi devices to the users have many benefits and Wi-Fi can be useful in many situations. Wireless communication between Wi-Fi devices without any physical medium between these devices leads to many problems. There is no guarantee that the communication that occurred between Wi-Fi devices cannot be received by unauthorized users. Wi-Fi provides no mechanism to detect that the transmission of signal is secure in the air and no intruder or attacker is receiving wireless signals. Many enterprise users have concerns over security of Wi-Fi devices for these reasons. According to Wexler, 70% enterprise users have concerns about security of Wi-Fi devices that is preventing these users to deploy Wi-Fi technology (Wexler, 2006). Another important factor about the security of Wi-Fi devices is the lack of expertise in technical users who manage these devices. Some of the important security issues related to Wi-Fi technologies are discussed below.

4.1 War Driving

War driving is among one of the top security threats for Wi-Fi technologies. It is carried out by people who travel from one place to another in order to discover open

or insecure Wi-Fi networks. These people utilize various types of tools such as Airopeek, NetStumbler, AirMagnet to gather information of Wi-Fi networks (Moerschel et al., 2007). The information obtained from these applications is usually uploaded on some websites for other war drivers. War drivers also use special symbols to inform other war drivers and hackers about Wi-Fi networks near that sign. Figure 3 is highlighting some important statistics about war driving for 2002 & 2004. The increasing number of Wi-Fi networks in 2004 clearly shows user interest in Wi-Fi technologies.

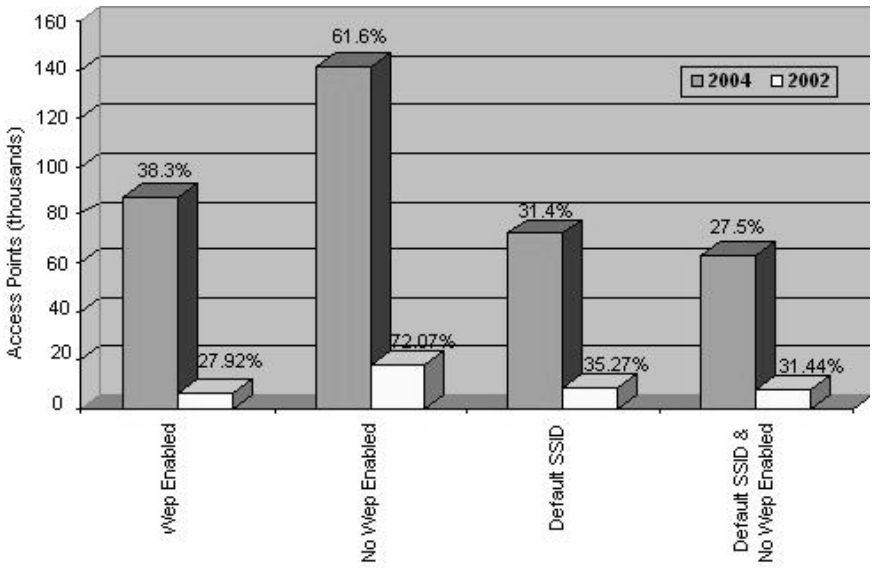

Figure 3: War Driving statistics for 2002 & 2004 (Audin, 2003; Wigle, 2007)

4.2 Denial-of-Service (DoS)

Another security threat to Wi-Fi networks is the Denial-of-Srvice attack against Wi-Fi devices to cause delay and interruption in the network. DoS attacks on Wi-Fi networks are usually carried out at physical or MAC layer. According to Internet security threat report, 38% ISPs were affected by DoS attacks for the period of Jan-Jun 2006 (Symantec, 2006). Most of the Wi-Fi networks are used by residential users for Internet access through ISPs that were also expected to be affected by these DoS attacks. DoS attacks on Wi-Fi networks are easily carried out through packet generators that are easily available in market such as Tamosoft's Commview (Tamosoft, 2007). These packet generators are easy to use applications and provide options such as packet size, packet transmission rate, and source and destination MAC addresses. Table 1 is showing top wireless attacks with highlighting different types of DoS attacks against Wi-Fi devices contributing 15% of overall attacks.

Rank	Threat	Percentage
1	Device probing for an access point	30%
2	MAC address spoofing	17%
3	Unauthorized NetStumbler client	16%
4	Rogue access point	8%
5	Unauthorized association DoS attack	6%
6	RF jamming DoS attack	4%
7	CTS DoS	3%
8	Illegal 802.11 packet	2%
9	Honeypot access point	2%
10	Authorized DoS attack	2%

Table 1: Top wireless attacks for the period of Jan-Jun 2006 (Symantec, 2006)

4.3 Viruses, Worms, and Malware

Name	Type	Operating System
Brador	Trojan	Windows Mobile
Cabir	Worm	Symbian
Commwarrior	Worm	Symbian
Dampig	Trojan	Symbian
Duts	Virus	Windows CE
Fontal	Trojan	Symbian
Lasco	Worm	Symbian
Locknut	Trojan	Symbian
Skulls	Trojan	Symbian

Table 2: Malware threats to wireless devices operating systems (Furnell, 2005)

Modern wireless handheld devices such as smartphones and PDAs are now coming with Wi-Fi support. Most of these mobile devices are equipped with widely used operating systems such as Windows Mobile and Symbian OS. These operating systems provide many benefits to the manufacturers and vendors who develop variety of applications for these operating systems. However, it is also easy for malware developers to penetrate wireless devices running these operating systems. Mobile device users usually left their Wi-Fi connections open while they are not

using it. These high speed hidden paths can be very useful for malware penetration into Wi-Fi devices and network that are providing services to these Wi-Fi devices.

Table 2 is showing some malware applications designed for mobile devices running Windows Mobile and Symbian OS. A careful analysis of table reveals that most of the Trojans and worms are used against Symbian OS. It is due to the fact that Symbian OS is the most used operating system on mobile devices. However, manufacturers are now introducing different versions of Windows Mobile family operating systems. Windows operating systems are widely supported on most of the devices and users are more familiar with Windows family of operating system. However, due to its wide use in different types of devices including Wi-Fi technologies, it is also easy for malware writers and hackers to launch viruses and worms attacks on Wi-Fi devices running Windows family operating system.

5 Protection Mechanisms for Wi-Fi Technologies

There are various types of security methods in order to secure Wi-Fi devices from threats and attacks from intruders and hackers. Wi-Fi enabled mobile devices such as smartphones and PDAs can be better protected through personal firewalls and antivirus applications. These handheld devices usually have low processing power and limited power resources that restrict these devices from using other security methods. Although, most of the Wi-Fi devices including Wi-Fi enabled mobile devices provide WEP for protection, it should never be use to secure Wi-Fi devices due to the known weaknesses in its implementation (Boland & Mousavi, 2004).

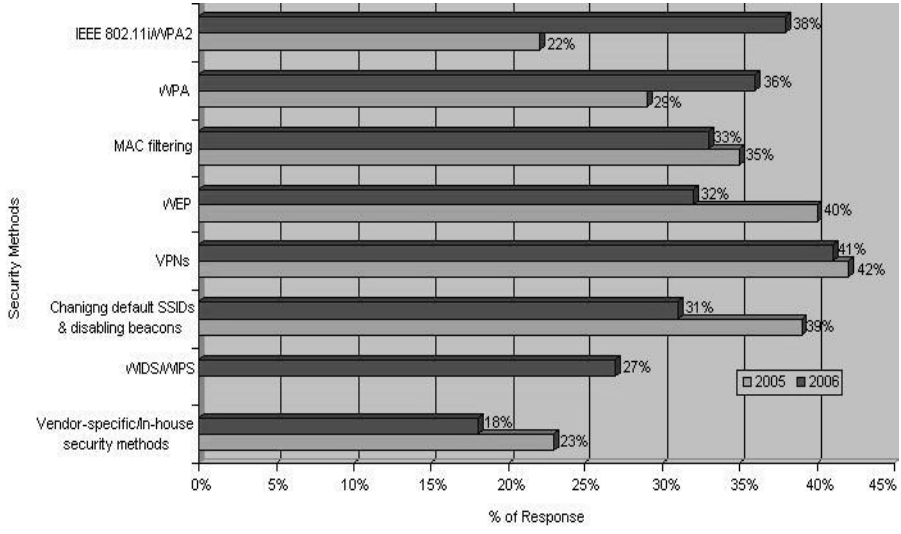

Figure 4: Users preference towards various protection methods (Wexler, 2006)

WPA and WPA2 are more secure security solutions for protection of Wi-Fi devices compared to WEP as these methods offer better authentication and encryption

support. There are various other protection methods as well that can provide better security to Wi-Fi devices. VPN solutions such as provides flexibility to users due to its vendor neutral nature for security purposes. However, it is not a good choice in case of residential and small office users due to the cost involved with this solution. It is also not suitable for real time applications such as voice and video especially when large amount of traffic is moving across VPN. Figure 4 is showing preference of enterprise users towards various protection methods.

6 Conclusion

As Wi-Fi technologies are coming with better data rate support for broadband Internet access, users are attracting to Wi-Fi devices due to many benefits provided by Wi-Fi devices. Residential users are more adopting Wi-Fi technologies compared to enterprise users due to mobility, flexiblilty, and ease of use they are getting from these devices. However, due to the nature of Wi-Fi devices to communicate with each other through wireless signals, Wi-Fi devices and users are becoming victim of various security attacks. These security threats can only be addressed through better security solutions to protect Wi-Fi devices in a layered manner.

7 References

Audin, G., (2003), 802.*11: Are You Sure You're Secure?*, Delphi Inc, http://www.webtorials.com/main/resource/papers/delphi/paper1.htm, (Accessed 15 December 2006).

Boland, H., and Mousavi, H., (2004), *Security Issues of the IEEE 802.11b wireless LAN*, IEEE Electrical & Computer Engineering Conference, Volume 1, pp. 333-336.

Furnell, S., (2005), *Handheld hazards: The rise of malware on mobile devices*, Computer Fraud & Security, May, 2005.

IDC, (2006), *Western European WLAN market generated $1.2 bln in January-June 2006*, ZDNET. http://blogs.zdnet.com/ITFacts/?p=11971, (Accessed 3 Feburary 2007).

ITFacts Wireless data, (2005), *WLAN switch sales up 52% in Q2 2005*, ITFacts. http://www.itfacts.biz/index.php?id=P4584, (Accessed 18 February 2007).

Moerschel, G., Dreger, G., and Carpenter, T., (2007), *Certified Wireless Security Professional-Official Study Guide*, Planet3 Wireless Inc., McGraw Hill, 2nd Edition.

Pyramid Research, (2005), *Wi-Fi Adoption*, BusinessWeek Online, http://www.businessweek.com/technology/tech_stats/wifi051003.htm, (Accessed 1st October 2006).

Symantec, (2006), *Symantec Internet Security Threat Report Trends for January 06- June 06*, Volume 10, http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport, (Accessed 5th January 2007).

Tamosoft, (2007), Tamosoft's CommView, http://www.tamos.com/products/commview/, (Accessed 15 January 2007).

Wexler, J., (2006), *Wireless LAN State-of-the-Market Report*, Webtorials, http://www.webtorials.com, (Accessed 14 January 2007).

Wigle, (2004), World Wide War Drive 4 Stats, http://wigle.net/gps/gps/GPSDB/stats/?eventid=1, (Accessed 22-03-2007).