Full paper

Security Issues that Arise in IEEE 802.11x and 3G Wireless Networks

Avinash Shridhar **Donald Joyce** **Sam Kolahi**

Unitec New Zealand
Auckland
avinss1@hotmail.com

ABSTRACT

The aim of the research was to study the security issues/concerns that arise in IEEE (Institute of Electrical and Electronic Engineers) 802.11x and 3G (third generation) wireless networks. From the data gathered through interviews, observations and literature review, security concerns/issues that arise in IEEE 802.11x and 3 G networks were identified and methods that may be used to test for any vulnerabilities and minimize the security loopholes in both these networks were determined. Recommendations are given to improve the security in both IEEE 802.11x and 3G networks.

Keywords

Security, wireless, networks

1. INTRODUCTION

Of all the communication services available in the market today, wireless services are having a tremendous impact on our lives, enhancing personal productivity, mobility and security. Muller (2003, p. ix) states that the wireless industry is going through a process of rapid innovations, increased competition and diversity in service offerings – resulting in reduced prices for consumers and businesses. Wireless networks have become increasingly popular and many organizations seem to want to make their offices "wired free", but the security issues that are attributed to wireless networks have prevented the adoption of wireless devices on a larger scale (Schmidt & Townsend, 2003).

Currently, there are many wireless technologies available in the market, including IEEE 802.11x, 3G and Bluetooth. IEEE 802.11x and 3G technology are gaining popularity as the means for delivering wireless Internet services (Utk.edu, 2004). IEEE 802.11x wireless networks are increasingly used in a wireless local area network environment and there are three common 802.11x wireless standards: 802.11b, 802.11a and 802.11g. The 802.11b wireless standard is the most popular standard used in many homes and offices (Playstation, 2003). Although the data transfer rate in 3G networks is not as high as in IEEE 802.11x , 3G networks can offer the freedom of mobility and being connected to the Internet wherever you go. It has been observed that wireless networks that are based on 3G and IEEE 802.11 standards will exist together, offering Internet services to users. These technologies offer features that actually complement each other (Buddhikot, Chandramenon, Han, Lee, Miller and Salgarelli, 2003).

In this paper the focus is on IEEE 802.11x and 3G networks. The security issues/concerns that could arise are looked into. The steps/techniques that can be taken to manage and tackle the security loopholes that exist in IEEE 802.11x and 3G networks (and when interoperating IEEE 802.11x and 3G networks) are also discussed. A glossary is provided at the end of the paper.

2. METHODOLGY

Qualitative methods were used for data collection and analysis. Multiple case studies were conducted, using interviews and field observations as the primary source of data collection. Key staff were interviewed at four companies involved in providing wireless solutions (three medium-sized and one small) and two educational institutions (one secondary and the other tertiary). The interview questions covered general security concerns, security loopholes in IEEE 802.11x and 3G networks, methods used to test security and minimise security breaches,

and interoperation of IEEE 802.11x and 3G. Field observations were conducted at one company and one educational institution. Literature was used as a secondary form of data collection and the sources referred to included books, websites, journals and conference proceedings. Content analysis of the interview transcripts was used to identify themes and these were related to the literature, with the authors' own interpretations added in where necessary.

3. RESULTS

3.1 Security Concerns with IEEE 802.11x Networks

The results of the research showed us that there are a number of security issues with IEEE 802.11x wireless standard protocols, although work is being done to ensure that there is a more rigid and secure wireless standard that could be used in a wireless local area environment. Currently, the most popular wireless standard used in organizations is 802.11b and there are a number of security issues that are associated with 802.11b. Most of the responses that were obtained during the interviews with regard to the security concerns with 802.11x wireless standard revolved around 802.11b wireless standard and that shows the widespread use of the 802.11b wireless standard protocol as opposed to other variants of the 802.11x wireless protocol.

All of the interviewees agreed that there were security concerns about the 802.11b wireless standard protocol. Surprisingly, not one of the interviewees had faced a security attack from an intruder/hacker either in their own organization or, in the case of some interviewees, at the organizations of their customers. It is the opinion of the authors that this is because a hacker/intruder needs to have enough time and money to stage such an attack. Although one educational institution had faced threats in the form of viruses, there was no intentional attack caused by a hacker. However, as wireless networks and wireless devices start getting more common, a hacker could have access to the equipment needed to exploit the security loopholes that exist in 802.11b networks.

Most of the organizations do not turn on the WEP encryption for the simple reason that turning it on could bring down the speeds by 2Mbps to 4Mbps. This could be dangerous because any person could be part of the network and if the intruder/hacker becomes a part of the network, s/he can start sniffing packets without the organization realizing that the intruder/hacker is part of the wireless network. It is vital that WEP encryption is turned on as it makes the hacker work harder to break into a wireless network. Although wireless cards that are TKIP or AES enabled are available in the market, organizations think twice before purchasing these cards as they are relatively expensive.

It might be thought that changing the SSID could provide an additional level of security, but the field observations suggested that changing the SSID has no particular advantage and provides no real security because a wireless card on a client's machine can scan for the SSID without any hurdles. This is the case when the broadcasting is not turned off. On further literature review, the authors realized that as the SSID can be sniffed in plain text format, it does not provide any kind of security. Organizations tend to have this false sense of security and feel that changing the SSID can provide them with increased level of security. The interviewee at one educational institution stated that amongst the first steps that they took in increasing the security was to turn the broadcasting off, but the observations indicated that turning off broadcasting did not have any particular advantage because as soon as one user was part of the network, it was always possible to for a hacker/intruder to sniff the SSID.

Interference is one of the main concerns with IEEE 802.11x wireless networks. The 802.11b wireless standard uses the 2.4 Ghz spectrum and any other device that operates in that frequency can cause interference and disrupt the data packets that are transmitted. Also Bluetooth-enabled devices are known to cause some kind of interference. Surprisingly, none of the interviewees mentioned interference when using the IEEE 802.11x wireless standard. Although the organizations interviewed did not face any threat of particular kind in the form of interference, a hacker/intruder could intentionally cause serious trouble by disrupting the services to users of the wireless network. Another kind of security threat noticed during the observations is that two computers could bypass the access point and communicate with each other, giving access to

each other's files. A hacker using a "rogue computer" could make use of this and gain access to sensitive information.

During one interview at an educational institution it was noted that initially the WEP encryption code had not been turned on and as a result of this anyone could come in with their wireless LAN card and be a part of the network. It should be noted that any worm or virus could propagate through a TCP/IP interface including wireless. As a result a particular worm found its way through the wireless network and although the wired network was not affected by the worm, any laptop that was connected to the wireless network started getting infected with the worm. Although a threat that still exists in the wired world, denial of service attacks are comparatively easier to stage in the wireless world. Jamming devices or techniques can be used to develop large volumes of illegitimate traffic, thus affecting the legitimate traffic in the wireless networks.

3.2 Recommendations for Improving Security in 802.11x Networks

Although turning off broadcasting does not greatly improve security, it is one of the steps that could be taken to enhance the security in a wireless network. Depending on the capability of the wireless access point and the wireless cards, WEP, TKIP, AES or WPA encryption could be turned on. If access points with 802.1x security standards built-in are available, then they should also be used as they provide much better security and are well integrated with Windows XP, which has the features of the 802.1x wireless architecture built in.

Once those two steps have been taken, the next step is to limit the MAC addresses to connect to the network. Nowadays, access points limiting the IP addresses are available. Hence it is important that this step of filtering the MAC addresses or IP addresses is undertaken because computers that are not within the allocated range will not be able to connect to the wireless network. Network monitoring software could be used to check for any unusual activity that takes place across the network. The interviewee at one company claimed that the software called "AirMagnet" that they are distributing in New Zealand has the capability of checking for any unusual activity that goes on in the wireless network.

Interference is a problem that cannot be tackled easily, because most of the other devices operate in the 2.4 Ghz spectrum and it is possible for a hacker/intruder to cause intentional jamming, although it has not been experienced in any of the organisations that were interviewed. One option that could reduce, if not solve, the problem is to use 802.11a devices. 802.11a wireless devices work in the 5Ghz spectrum and hence there is a minimal chance of interference related issues, although the devices are not backward compatible with 802.11b devices and are more expensive than 802.11b devices. In one company where the 802.11x wireless standard is used on a larger scale, spectrum analysers are seen as an excellent tool to determine who is broadcasting on the same channel. The threat of viruses and worms exists and it is always recommended that employees of the organization keep themselves updated with the latest definitions and ensure that all the patches are downloaded and installed in their laptops.

By limiting the field coverage to just the area where it is needed, any leaking signals can be restricted. This is done by using directional antennas and/or lowering the transmitting power by using the appropriate wireless devices. Capkun, Hubaux and Buttyan (2003) suggest that "mobility" can be very useful for the purpose of having a secure connection between two mobile nodes and further suggest that if people want to communicate securely they just get close to each other in order to exchange information and to establish (or reinforce) mutual credentials. They also suggest that in a wireless ad-hoc network if the users are static it becomes easier for a hacker to know the exact location of the users and thereby it is easy for him/her to be in the middle of two communicating nodes, but if some kind of mobility is created between the two nodes and the two mobile nodes are brought closer to each other, it is possible to have a secure means of communication. Other steps that organisations could take include developing and implementing security policy guidelines to protect the wireless network and hiring wireless security experts to provide added protection.

	Group A	Group B	Group C
Level of Expertise	High level of expertise, with adequate security levels in place	Adequate. Although could have more levels of security in addition to the ones that are already existing.	Low level of expertise. Although enough for the moment, could prove inadequate in future.
Strategic focus/direction in terms of building high levels of security in the wireless networks	High level of strategic focus	Focus not on improving security nor are there any plans for the installation of wireless networks on a large scale.	No strategic focus at all.
Level of Security	High levels of security	Although the networks have some level of security, they are not really high	The network does not have any levels of security. Even the WEP (in 802.11x networks) key is not turned on at some places.
Methods used for detecting any intrusions in both IEEE 802.11x and 3G networks	Methods used for testing the network are reasonable.	Used software tools like Angry IP Scanner to monitor the network	No tools used to monitor the network

Table 1: Organisations categorised according to level of security

3.3 Security Concerns with 3G Networks

The security architecture in 3G networks is much better and they are relatively more difficult to break into than 802.11x networks. If there is any problem that exists in 3G networks, then the possibility of denial of service attacks. One interviewee maintained that a single cell site could hold 500 users. When there are more than 500 users in a single cell site, denial of service is possible although it might not be intentional and for a hacker/intruder to cause any intentional attacks s/he must have access to highly sophisticated devices.

The data encryption technique in 3G technology is highly advanced and very difficult to break into. The TD-CDMA standard used by one company involved the use of both CDMA and TDMA multiple access techniques, thereby providing a greatly increased level of security, which is very difficult for any hacker/intruder to bypass because in addition to needing to access highly sophisticated equipment, the hacker/intruder also has to know how the data is encrypted and the time intervals between the successive bits of encrypted data that is transmitted. When a number of people congregate at a particular location the traffic load will be high. Although not an attack carried intentionally by a hacker/intruder, the connection may be lost and service may be disrupted due to overload conditions (Balachander, Bahl and Voelker, 2003).

3.4 Recommendations for Improving Security in 3G Networks

3G networks have excellent security features, but the networks could be made more secure by having in place CHAP protocols. The best way to ensure that distributed denial of service attacks do not take place intentionally or unintentionally is to monitor the number of users who might be connected to a single cell site at the same time. Once the number of users exceeds the allocated limit, the service can be denied to the new user who intends connecting to the cell site, thereby

ensuring that the other users who are already connected to the network are not affected.

4. CONCLUSION

The seven organisations in this study can be categorised according to level of security, level of expertise, strategic focus/direction and methods that are used to detect any security intrusions (see table 1). Group A consists of three companies and an educational institution that have installed wireless networks in their own organisation or have implemented wireless networks on a large scale in other companies. Group B consists of one company and one educational institution that have a wireless network installed in their own organisation, but not on a large scale. Group C contains one company that has implemented wireless networks in other companies, but not on a large scale.

The authors believe that many organisations in New Zealand would fall into groups B and C and it is vital that they take steps to upgrade their expertise, security and strategic focus to the levels shown by the organisations in group A.

GLOSSARY

3G - Third Generation
AES - Advanced Encryption Standard
CDMA - Code Division Multiple Access
CHAP - Challenge Handshake Authentication Protocol
IEEE - Institute of Electrical and Electronics Engineers
IP- Internet Protocol
LAN - Local Area Network
MAC - Media Access Control
SSID - Service Set Identifier
TCP/IP - Transmission Control Protocol/ Internet Protocol
TDMA - Time Division Multiple Access
TD - CDMA - Time Division Code Division Multiple Access
TKIP - Temporary Key Integrity Protocol
WEP - Wireless Equivalent Privacy
WPA - Wi-Fi Protected Access

REFERENCES

Balachander, A., Bahl, P., & Voelker, M.G. (2003). "Wireless hotspots: Current challenges and future directions." Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, 1.

Buddhikot, M., Chandramenon, G., Han, S., Lee, W. Y., Miller, S., Salgarelli, L. (2003). "Interoperation of 802.11 and third-generation wireless data networks." Paper presented at the 22nd IEEE Infocom Annual Joint Conference of IEEE Computer and Communications Societies, San Francisco, CA.

Capkun, S., Hubaux, J., & Buttyan, L. (2003). "Mobility helps security in Ad-Hoc networks." **Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing, 46-47.**

Muller, J. N. (2003). "Wireless A to Z." New York: McGraw-Hill.

Playstation (2003). "What are wireless standards – like 802.11a, 802.11b and 802.11g." Retrieved December 18th, 2003 from http://eu.playstation.com/networkgaming/story.jhtml?storyId=300304_en_GB_SUPPORT

Schmidt, T., & Townsend, A. (2003). "Why Wi-Fi wants to be free." Communications of the ACM, 46(5), 49-52.

Utk.edu (2004). "Overview of Wireless Technologies." Retrieved March 15th, 2004 from:http://wireless.utk.edu/overview.html#broad