

Data Security and wireless networks: mutually exclusive?

A. J. Woodward

School of Computer and Information Science
Edith Cowan University
Perth, Western Australia

Abstract - *The increased use and popularity of wireless networks has seen their adoption in medical information systems. They provide the advantages of mobility and instant information availability. Since its inception, wireless has had problems with providing adequate security measures. This paper examines previous papers dealing with securing data in a wireless network for medical use, and analyses current wireless security measures. Measures listed by previous researchers were found to be unsatisfactory, with some of the current security methods also having problems. The conclusion is that wireless cannot be made completely secure, and should only be used where an absolute medical need, rather than one of convenience, can be demonstrated.*

Keywords: Wireless, medical wireless, data security, mobile.

1 Introduction

There have been numerous papers discussing the use of mobile devices, such as personal data assistant (PDA) type devices [1,2], and a few which discuss the use of wireless networks in a medical environment [3,4]. While some of these papers discussed security [3], the pace at which the technology has advanced has meant that the information provided in these works is no longer current. For example, it is no longer relevant to discuss wired equivalent privacy (WEP), the initial security measure used by wireless networks, as it has been repeatedly shown to be fatally flawed [5,6]. Although there have been further advances in wireless security so too has there been an increase in the knowledge of the wireless network protocol, and more importantly, any flaws they may contain.

Whilst data security is important for any user, it is obviously of paramount importance in a medical environment [7]. The use of mobile devices to provide access to patient records at the point of clinical care is being trialled worldwide and is providing both access to medical records and clinical decision support [8,9].

There are two aspects of wireless networks which lead to their insecurity. The first aspect is that it uses a broadcast medium. The information is effectively broadcast and propagated over a wide area (up to 150m) with a suitably equipped entity within the signal locus capable of capturing or modifying this information. The second are the embedded vulnerabilities in the *modus operandi* of the 802.11 protocol. The inability to verify 802.11 management and control frames is one such vulnerability, leaving the network susceptible to attacks such as denial of service (DoS) and man-in-the-middle (MITM) attacks [8].

2 The vulnerabilities with wireless networks

The risks with using wireless networks can be broadly categorised into four categories: denial of service, eavesdropping, protocol vulnerabilities and rogue access points (AP).

2.1 Denial of service

This type of attack can be perpetrated in one of two ways. It can either be conducted through the use of a jamming technique, or by exploiting the OSI Layer Two vulnerabilities that exist within that the 802.11 protocol suite. The first type of attack, that of jamming, is fairly easy to perpetrate, and is reasonably difficult to detect. A jamming attack can be either intentional or unintentional. An intentional attack is one in which the attacker broadcasts a very high-power signal at the same frequency that the wireless network is operating on, causing interference to the network [9]. The likelihood of this type of attack being conducted is fairly low as there is no real benefit to an attacker, unless it is to force a client to roam to a rogue AP. This type of attack may also occur unintentionally, through the placement of a device which operates at the same frequency in the vicinity of the wireless network. For devices that operate in the 2.4GHz frequencies, this includes microwave ovens, some cordless phones, baby monitors and Bluetooth devices. Bluetooth devices are known to

interfere with the operation of wireless networks [10].

The second category of attack, the so-called layer 2 attacks, exploits the lack of verification of control frames in the wireless network [6]. This control and management information is broadcast clear text by wireless networks, and can be captured by an attacker using a freely available packet capture tool, such as Kismet [11]. Once gathered this information can then be used against the wireless network that it was captured from, and used to force a client to leave and rejoin a network by issuing false disassociation or deauthentication frames [12]. During the reassociation process, the user's logon and authentication details can be captured by the attacker. This information can then be used to further exploit the wireless network. This type of attack can also be used to launch a man in the middle attack against the wireless network, and can even be used to circumvent virtual private network (VPN) systems. These layer 2 attacks are probably one of the most concerning to IS managers as there appears to be no adequate means to prevent them from occurring [13,14].

2.2 Eavesdropping

The functionality of wireless network presents one of its biggest problems. Because wireless is a broadcast medium, there is no way to control where the information is sent and who therefore has access to it. By modifying the drivers used with the wireless client devices, many individuals and organisations have developed analysis tools, known as "sniffers". There are both freeware (Kismet) [11] and commercial (Airopeek) [15] versions of this type of software. When used within the broadcast range of a wireless network, these can be used to capture every packet travelling the wireless network. If an access point is set up and used in its default configuration, then the user of such a system is vulnerable to attack, because anyone running sniffer software can see and capture everything that a user does across that network. This includes data (medical records), passwords and email messages. Even when encryption is used, there is still important information which is available to anyone within range of a wireless network. This includes the network name (SSID), the MAC addresses of both AP and clients, and a range of other information.

Another problem with the broadcast medium is that the range is not only dictated by the transmitter, but also by the receiver. Effective range of the wireless network is an intersection of where the two antenna coverage patterns overlap. An attacker can increase the distance at which they can

perform an attack simply by using a larger antenna. Depending on the antenna type used, the range is only limited by the ability to obtain line of sight between attacker and victim.

2.3 Protocol Vulnerabilities

This category examines the flaws or exploits that exist in wireless networks due to vulnerabilities with the protocol itself, and with its implementation in various operating systems. The 802.11i security extension was developed by the IEEE to provide increased security through stronger authentication and encryption. This was done through the use of port based access control (802.1x) and extensible authentication protocol (EAP) for authentication and the use of the advanced encryption standard (AES) for data encryption. The initial measures found in the draft version of 802.11i were released under the banner of Wi-Fi protected access (WPA), with the final measures called WPA2. Whilst the measures included in the 802.11i extension have increased security, there have been a number of areas identified which are of some concern. These include: the implementation of the temporal key integrity protocol (TKIP) in WPA, problems with 802.1x authentication, and (EAP) weaknesses. Further, it appears that no attempts have been made to address the problem with Layer 2 vulnerabilities that exist in the 802.11 protocol. This flaw in the protocol has potentially serious consequences for wireless systems when used in certain environments.

2.3.1 802.1x protocol weaknesses

Although it is stated as being a very secure method of authenticating wireless clients, a denial of service attack against the four-way handshake has been discovered [16]. The researchers examined the finite states of the authentication process and discovered a problem with the handshake process which would allow an attacker to deny clients access to the network. The vulnerability in the protocol would allow an attacker to block the handshake process by inserting one forged message. Although this attack requires precise timing, having to be launched between message 1 and message 3 of the legitimate handshake, it is possible. The authors have suggested a repair to the IEEE 802.11i working group, which is apparently to be implemented.

2.3.2 EAP weaknesses

While each of the EAP methods listed previously provides additional security and compatibility, they do all have potential weaknesses, and provide different strengths [17].

Their major weakness is that they can be vulnerable to offline dictionary attacks.

The proprietary Cisco lightweight EAP (LEAP) is probably the most vulnerable, as it is subject to offline dictionary attack [18]. This protocol has an interesting history, being developed by CISCO in response to a research paper by Mishra and Arbaugh [19] suggesting that EAP was vulnerable to both session hijacking and man-in-the-middle attacks. Cisco responded to this by producing a release which indicated that Cisco EAP (LEAP) would prevent these attacks from occurring [20]. Shortly thereafter, Wright [18] discovered a serious flaw in the LEAP protocol that left it vulnerable to offline dictionary attacks. This meant that an attacker could capture the password information, take it away and use a database of known words to attempt to decode the password. The researcher examined the Cisco website and found one small brief note on it in relation to the problem. The author contacted Cisco about this problem and they released a security bulletin [21], and asked Wright to hold off on an attack tool called "Asleap" that he had developed. After some time, and no notification from Cisco, the Asleap tool was released. This tool can be used amongst other things, to recover weak LEAP passwords [18]. Cisco has since developed the EAP FAST method which it claims is more secure [22].

2.3.3 TKIP Pre-shared key (PSK) weaknesses

There are two WPA TKIP modes that wireless systems can use: enterprise or consumer. The enterprise is a per-user authentication based protocol with the combination of the 802.1x security framework, authentication server, TKIP key management and message integrity checking (MIC). The consumer version uses a pass phrase to generate the encryption key instead of the 802.1x process, and this system was only meant as an interim data encryption method until the full version of WPA became available. The aim of the consumer version of encryption was ease of deployment, rather than strong security. The simplified system used for this consumer mode leaves it open to an offline dictionary attack, due to the broadcasting required to create and verify a session key [23].

When a pre-shared key (PSK) is used instead of 802.1X, the PSK becomes the pair-wise master key (PMK) that is used to drive the 4-way handshake that would normally occur with an 802.1x authentication [24].

The problem is not with WPA itself, but implementation of the PSK can create a problem. If a PSK is used that is less than 20 characters in

length, and can be found in a dictionary, then it can easily be cracked. The problem can easily be solved by using a pass-phrase longer than 20 characters made up of random characters. The problem occurs because most consumer level users are unlikely to do this. Tools such as Cowpatty [25] allow for an attack to be made against a weak pass-phrase.

2.3.4 Hotspotter - Automatic wireless client penetration

This tool exploits the Windows XP zero wireless configuration (ZWC) in order obtain information about a client. Hotspotter listens passively for probe request frames sent by other clients to identify their preferred network, and compares it to a supplied list of common hotspot network names [26]. If the probed network name matches a common hotspot name, Hotspotter will act as an access point to allow the client to authenticate and associate. Once associated, Hotspotter can be configured to run a command, possibly a script to kick off a DHCP daemon and other scanning against the new victim. Once associated to the rogue network, it is possible to interact with the client directly, and to perform actions including port scanning the victim, exploiting Windows-based vulnerabilities, deploying malware or spyware, and simulating an otherwise "real" network using faked services (honeynet) and intercepted DNS queries.

2.4 Rogue Access Points

One of the biggest dangers faced by users of a wireless network is that of so-called rogue access points. These may not necessarily have been placed by an attacker, but possibly by an employee who is not familiar with the dangers of wireless networks. Regardless of who it was placed by, such a device is equally dangerous. A rogue AP may be placed by an attacker, or an employee, which creates a portal into the corporate network. It is an extremely high security breach, and is basically the equivalent of running a CAT5 cable into your wired network from the car park or anywhere else that has line of sight to your wireless network. If an attacker can successfully carry out such an attack, they can potentially have full access to your entire network

2.4.1 Aircsnarf - A rogue AP setup utility

The Aircsnarf utility effectively allows an attacker, with very little knowledge of wireless or programming, to steal data from a wireless network [27]. This utility contains the appropriate software to issue a client with an IP address, DNS and gateway information. It also allows for the user to configure or use whatever web page they wish. An attacker only needs to obtain the SSID and MAC

address of a valid access point, and they can effectively pretend to be a legitimate device. Once this information has been gained, a wireless user's device may automatically connect to the rogue device without realising that it is not a valid one. Once connected, an attacker can be able to collect a wide range of information including user names and passwords. For example, in the case of a system where users are forcibly redirected to a login or portal page, the Airsnarf device can emulate this and collect logons and passwords. It is even capable of allowing users to access the internet, allowing for other information to be captured.

3.0 Implications of these vulnerabilities for medical data in a wireless environment

The major problems with wireless networks discussed here must be contextualised for their implications in a medical environment. The major issues of using wireless LANs in a medical environment can be broadly summarised into two areas key to information security, that of availability and data security. This discussion includes some basic suggestions are offered in the event that a WLAN is to be installed and used.

3.1 Availability

If the wireless network is being used to distribute information in real time to a practitioner, and that information becomes unavailable, then people's lives may be at risk. As discussed above, denial of service attacks are easy to carry out in a wireless network, and nearly impossible to prevent. The point of denial of service is to do exactly this: prevent availability. Whilst this is a seemingly a trivial attack, and one which yields little or no information for an attacker, it could have fatal consequences in a medical environment. As has been pointed out previously in this paper, interference may be caused by a seemingly innocuous event, such as another device operating on the same frequency, and may not even be a malicious action. The risks of using wireless networks for this type of role cannot be overstated. There is no preventative measure for a denial of service attack, due to the physics of the wireless medium. The only way to make sure that such an eventuality does not occur is to not rely on wireless networks for time sensitive data. A user of wireless must always assume that at some point the network will become unavailable, and plan accordingly.

3.2 Data Security

Depending on the context in which the WLAN is to be used, data security may be just as important as availability. To put it simply, data security is the means by which you prevent an unauthorised person capturing or reading the information as it travels over the WLAN. However, data security is not just about having data read or stolen. Network security should be thought about as making both deposits and withdrawals. It is possible that an attacker may use the network to place false data on the network, in addition to stealing it. An example is a disgruntled former employee uploading inappropriate content, such as pornography, to a workstation or server. A more extreme example may involve changing patient's medical records.

Depending on what encryption method is used, protection of patient information is one area in which wireless security has progressed to a satisfactory level. The adoption of AES encryption in the finalised 802.11i extension, also known as WPA2, provides a high level of data protection. It is estimated that it would take 10^{56} years, using \$10 million worth of computers to break the 256 bit AES encryption used in WPA2 [30]. Unfortunately, this encryption method, the only one which provides a strong enough level of protection, requires a dedicated chip which consumes more processing power than PDA type devices are able to support [30]. This means that a less strong, and ultimately less secure, form of encryption must be used, potentially exposing confidential information to an attacker. Available options are WEP or WPA with PSK, neither of which provides strong encryption, as discussed previously.

Another issue in relation to data security is rogue APs. These present a real and high level security risk to a wireless LAN user. There are both commercial and freeware wireless intrusion detection systems available, but their effectiveness in protecting wireless networks is questionable [31]. They work by monitoring wireless traffic and alerting system administrators to any unauthorised traffic or devices. However, these systems do have drawbacks, and are only as good as the rules that determine what traffic is classified as legitimate or unauthorised [32]. If the rules are not strictly defined, then legitimate traffic can be classed as a potential attack, particularly when clients signal strength is low. Another problem with these systems is that they are a reactive system rather than an active, meaning that attacks are not prevented, but are reported after they occur. Another possibility is that they can be used to attack legitimate activities or systems.

3.3 Suggestions for security

If the decision has been made to use a wireless network in a medical environment, then the following suggestions may be of benefit:

- Reduce the transmitted power level on all devices to the lowest possible level while still allowing for connectivity. This makes it difficult for an attacker to find the network, and also to then attempt to connect to it
- Use WPA2 with 802.1x and EAP; choose an EAP method which is secure. This makes it difficult for non-legitimate users to connect to the network.
- If PDA devices are to be used, then WPA with PSK encryption and a key at least 20 characters in length, and change keys regularly. These devices are not capable of running stronger encryption, so this is the best that is available. The long key length makes it difficult to use an off-line dictionary attack
- Investigate WLAN hardware that has the facility for automatic rogue AP detection. Removes the requirement for a high level of technical knowledge, and of constant scanning for rogue devices
- User education. It cannot be overstated how important it is for users to be aware of the basic risks when using WLANs
- Turn off when not in use! If it is not on, it cannot be attacked.

4.0 Conclusion

Wireless networks, whilst providing the advantage of mobility and portability also come with a long list of problems. Data security cannot be guaranteed, and neither can availability. This situation is not likely to improve in the near future, and in fact, it is likely that more vulnerability will be discovered over time. A high level of knowledge, technical expertise and expense is required if a wireless network is to be used safely and securely. Whilst many practitioners may have the financial resources to secure their WLAN, finding a skilled person with the right knowledge to do the job may be an issue. Future research will examine the use of wireless networks in the medical environment, and the knowledge of the risks by those who use it.

In relation to the title of this paper, are wireless networks and medical information systems mutually exclusive? This discussion proves that they are not. However, that is not to say that wireless networks are 100% secure, or that they should be used in every circumstance. There needs to be a serious risk assessment made in any medical

practice intending to use wireless networks to determine whether the benefits outweigh the risks. The threats to wireless networks are very real, and new vulnerabilities are being discovered frequently. If wireless networks must be used, then they must be used with due care.

5.0 References

- [1] R. A. Wilcox and R. R. La Tella, "The personal digital assistant: a new medical instrument for the exchange of clinical information at the point of care", *Medical Journal of Australia*, Vol 175, pp. 659-662, 2001.
- [2] E. Terado and P. A. H. Williams, "Securing PDAs in the healthcare environment", *Journal of Information Warfare*, Vol 4, No. 1, pp. 61-68, 2005.
- [3] T. J. Owens, S. Tachakra, K.A. Banitsas and R.S.H Istepanian, "Securing a medical wireless LAN system", in Proceedings of the IEEE EMBC Conference, Istanbul, 2001.
- [4] K. A. Banitsas, S. Tachakra. and R.S.H. Istepanian, "Operational parameters of a medical wireless LAN: Security, range and interference issues", in Proceedings of the IEEE EMBC Conference, Houston, Texas, 2002
- [5] S. Fluhrer, I. Mantin and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4", URL: http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf, retrieved 27/10/05, 2001.
- [6] A. Woodward, "An analysis of current 802.11 wireless network layer one and two attacks and possible preventative measures", *Journal of Information Warfare*. Vol 3, No. 3: pp. 37-47, 2004.
- [7] P.A.H. Williams, "Information security awareness of medical practitioners", In Developing Partnerships. Ist Colloquium of Information Systems Security Education - Asia Pacific (CISSE-AP). 32-41. Mawson Lakes, SA: School of Computer and Information Science, University of South Australia, 2005.
- [8] N.S. Bower, "Put technology at your fingertips with a PDA", *Nurse Practitioner*, Vol 29, No. 2, pp. 45-46, 2004.
- [9] A. E. Carroll, P. Tarczy-Hornoch, E. O'Reilly and D. A. Christakas, "The effect of point-of-care personal digital assistant use on resident documentation discrepancies", *Pediatrics*, Vol 113, No. 3, pp. 450-454, 2004
- [10] A. Woodward, "Wireless Jacks - An analysis of 802.11 wireless denial of service attacks and hijacks", 3rd European conference on Information

Warfare and Security, Royal Holloway, UK June 2004

[11] R. Hoad and A. Jones, "Electromagnetic (EM) threats to information security – Applicability of the EMC directive and information security guidelines", 3rd European conference on Information Warfare and Security, Royal Holloway, UK June 2004

[12] J. Geier, "Minimising 802.11 interference issues." URL: <http://www.wi-fiplanet.com/tutorials/article.php/953511> retrieved 27/10/05, 2002.

[13] M. Kershaw, "Kismet readme", URL: <http://www.kismetwireless.net/documentation.shtml> retrieved 11/10/05, 2004.

[14] J. Bellardo and S. Savage, "Disassociation and De-auth attack", 2003 USENIX Security Symposium, USENIX, 2003.

[15] R. Baird, and M. Lynn, "Advanced 802.11b Attack", Blackhat Briefings 2002, Caesars Palace, Las Vegas, Nevada. URL: <http://www.blackhat.com/presentations/bh-usa-02/baird-lynn/bh-us-02-lynn-802.11attack.ppt>, retrieved 17/10/05, 2002.

[16] R. Floeter, "Void11", URL: <http://www.wlsec.net/void11/>, retrieved 17/04/2004, 2003.

[17] Wildpackets, "Airopeek - Real-Time Network Analytics for Enterprise WLANs", URL: <http://www.wildpackets.com/products/airopeek/overview>, retrieved 19/10/05, 2005.

[18] C. He, and J. C. Mitchell, "Analysis of the 802.11i four way handshake" WiSe'04, October 1, 2004, Philadelphia, Pennsylvania, USA, 2004.

[19] L. Barken, "How secure is your wireless network?: A guide to safeguarding your Wi-Fi LAN", Prentice Hall, New Jersey, 2003.

[20] J. Wright, "Asleep", URL: <http://asleep.sourceforge.net/>, retrieved 9/8/05, 2004.

[21] A. Mishra and W. A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", URL: <http://www.cs.umd.edu/~waa/1x.pdf>, retrieved 9/8/05, 2002.

[22] Cisco, "Product Bulletin - Cisco Aironet Response to University of Maryland's Paper, An Initial Security Analysis of the IEEE 802.1x Standard", URL: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.htm, retrieved 9/8/05, 2002

[23] Cisco, "Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability", URL: <http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml>, retrieved 9/8/05, 2003

[24] Cisco, "Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling – QA", URL: http://www.cisco.com/application/pdf/en/us/guest/products/ps430/c1167/ccmigration_09186a00802030dc.pdf, retrieved 9/8/05, 2004

[25] T. Takahashi, "WPA passive dictionary attack overview", URL: http://www.tinypeap.com/docs/WPA_Passive_Dictionary_Attack_Overview.pdf, retrieved 7/8/05, 2004.

[26] R. Moskowitz, "Weakness in Passphrase Choice in WPA Interface" URL: <http://wifinetnews.com/archives/002452.html>, retrieved 7/9/05, 2003

[27] J. Wright, "CoWPAtty – Offline PSK Dictionary Attack Tool", URL: <http://www.securiteam.com/tools/6L00F0ABPC.html>, retrieved 15/10/05, 2004

[28] Hotspotter, "Hotspotter - Automatic wireless client penetration" URL: http://www.remote-exploit.org/index.php/Hotspotter_main, retrieved 17/10/05, 2005

[29] Shmoo, "Airsnarf - A rogue AP setup utility", URL: <http://airsnarf.shmoo.com/>, retrieved 25/10/05, 2005

[30] M. Ciampa, "CWNA Guide to wireless LANs", 2nd Edition. Thomson Course Technology, Canada, p296, 2005

[31] C. Valli, "WITS – Wireless Intrusion Tracking System", 3rd European conference on Information Warfare and Security, Royal Holloway, UK June 2004

[32] J. Farschi, "Wireless Intrusion Detection Systems". URL: <http://www.securityfocus.com/infocus/1742> retrieved 11/10/05, 2003.