Securing PDAs in the Healthcare Environment

Emiko Terado
School of Computer and Information Science, Edith Cowan University
eterado@student.ecu.edu.au

Patricia A H Williams
School of Computer and Information Science, Edith Cowan University
trish.williams@ecu.edu.au

Abstract

Wireless networks have become a key element in healthcare institutions for streamlining access to clinical information. With the advent of wireless technology, handheld devices such as PDAs, pagers and Pocket PCs are now being deployed into modern hospital systems. However, putting confidential data on the airwaves using wireless technology introduces significant risk and adds a new level of threat to sensitive medical information. This paper investigates the fundamental concepts required to understand PDA security issues in the health sector. It examines the various risk and threat issues, the security measures needed to secure PDA use, and the appropriate security infrastructure for healthcare settings.

Keywords

Wireless technology, security, mobile computing, health, PDA

INTRODUCTION

For many healthcare institutions, introducing an Electronic Medical Record (EMR) system to store digitalised patient information has become a key element in streamlining enormous volumes of clinical information. However, in the healthcare environment, clinical staff are constantly moving within the facility, making it difficult for them to interrupt their patient care activities to enter patient data into a computer. Gruman (2003) found that "even though many hospitals began installing data-access terminals a decade ago at nurses' stations and near hospital wards, staff members still tend to scribble notes a few hours before they enter data and place orders. That can lead to transcription errors, delays in test results and incomplete records when other staff look up a patient's status".

To manage this problem, many healthcare institutions are beginning to create mobile environments using wireless technologies. This has seen the introduction of Personal Digital Assistants (PDAs) into medical centres and hospitals at the point of care. Utilising PDAs is one solution that assists staff to instantly access information about patients, drugs, and diagnostic treatment at any time, anywhere. "This reduces errors and delays, and fits into the doctors' and nurses' workflow. And they're inexpensive to deploy, costing a few percent of the total budget of an EMR system. Plus, they can be a springboard to services such as communications badges and mobile sensors" (*ibid*).

Usage of PDAs by physicians is increasing and LaRochelle (2002, p.68) asserts that the "number of physicians who use handheld computers increased from 15% in 1999 to 26% in 2001 and concluded that 50% of all physicians will use a handheld by 2005". In addition, in 2003 it was reported that medical professionals are using PDAs primarily to access clinical information (70%), view medical news (58%) and as medical calculators (57%) (Marsh & Bulanti, 2003).

Despite the advantages of mobility and data access, using PDAs creates significant risks and new challenges. One major concern is security. The main objective of this paper is to investigate the risks, threats and vulnerabilities that exist in using PDAs in the healthcare environment, and how we can employ countermeasures to increase security.

PDA SECURITY RISK, THREATS AND ATTACKS

Many institutions allow the use of handheld computers but are not prepared to manage the security risks inherent in their use (Blanton, 2001). This section discusses the risks and threats associated with PDA technology in terms of the hardware, software and data, and the management issues.

Hardware risks

The hardware risks include issues related to the technology battery life, signal interruption potential and physical loss of the PDA. Limited battery power is an inherent problem of PDA technology, as is limited memory and processing power capabilities. Kleinberg and Dulaney (2001) explain that the development in battery life technology is not keeping pace with the developments of the technology itself. This can detrimentally impact workflow in a healthcare environment. As long as no dramatic evolution of power supply methodology emerges, this issue will continue to be a problem in the foreseeable future.

Limited battery power also influences PDA network performance causing signal interruption. The weaker radio signals, used to save on battery life, mean a physical barrier can interrupt a PDA connection in a wireless environment. In such situations where clinical staff constantly move from room to room or from floor to floor, interruption of PDA network connection can be a nuisance. Gruman (2003) found that the use of routers and virtual LANs can also affect network connection as signal delays occur when users roam between wireless access points. Therefore roaming is a likely cause of dropped PDA connections. This also results in difficulty in managing continuous workflow for staff.

Another issue, common to handheld devices, is that due to the small size of PDAs, relatively low cost, location of use and ease of concealment, the likelihood of theft, misplacement, or loss increases (Karygiannis and Owens, 2002). Since PDAs are not continuously connected, it is harder for hospitals to manage this equipment. Thus medical institutes have more difficulty in enforcing security policies and monitoring security procedures (Bluefire, 2003). Stolen or lost PDAs result in severe security risks. These include theft of passwords or other confidential IDs, unauthorised access to the hospital network, leakage of patient's confidential data, and violation of the privacy act. Furthermore, damage of PDAs makes information unavailable at the least and unrecoverable at the worst (Blanton, 2001).

Software and data threats

The issues related to software and data threats include data leakage, availability of software security tools and virus protection. Leakage of confidential patient data stored in a PDA can be caused by infrared (IR) beaming. PDAs are capable of communicating via IR with other handheld devices and computers. Accidental data beaming and unwitting transfer of viruses are a risk in this type of technology (Blanton, 2001). Incorrect configuration and use of insecure point-to-point settings can expose data to other wireless devices (Karygiannis & Owens, 2002). Whilst such risks are present, as close proximity is required for interception, these types of attack are relatively low risk threats. Although minimal, users should not overlook such risks as they are handling patient confidential data, and any leakage of information could represent a breach in security.

Currently there are few advanced built-in security features in PDAs. Ahmad (2003) found that privilege access structure, protected memory space, virus protection and access control lists (ACL) based permissions do not exist. Also, the hardware limitations prevent usage of strong encryption methods. Table 1 indicates the available security tools that most PDAs lack.

Security Feature	Description
Memory protection for processes	All applications execute within the same memory space
Protected operating system kernel domain	Untrusted applications execute within the same memory space as code critical to the correct operations of the device and applications running on it.
File access control	Although some PDAs allow one to assign a password to "private" information, PDA OSs do not provide file and folder access controls, nor is the password protection strong.
Strong user authentication	Although some PDAs do enable users to password protect device access, this protection generally is quite weak. Biometric authentication is becoming more commonplace for authenticating users on enterprise platforms, but even simple user name and passwords have not been implemented in PDA OSs.
Differentiated user and process privileges	PDA OSs do not implement a privilege structure
Java language protections	Java implementations for PDAs generally omit security features such as type checking, fine-grained "sandboxes" to contain code execution, and stack introspections. Handheld devices have a number of communication ports

	from which they can send and receive data, but they have limited capabilities in authenticating the devices with which they exchange data.

Table 1- Lack of security features in PDAs (Baker, 2003)

PDAs are also potentially vulnerable to viruses, worms, Trojans, and spyware. Bluefire (2003) reports that 70% of those surveyed report finding at least one virus on a mobile laptop or PDA last year [2002]. Although, viruses have not been widely considered a security threat in PDA technology because of limited memory and processing power, they can be utilised as carriers rather than targets for virus distribution as they synchronise with a PC (Karygiannis & Owens, 2002).

Management Issues

There are many users who are keen on learning new technologies and are enthusiastic to introduce these into their workplace. However, lack of familiarity with the technology and lack of security awareness can cause potential risks. This issue relates to user knowledge and compliance with the security standards. Indiscriminate downloading of productivity programs without security awareness, including freeware and shareware programs from untrusted sources may unwittingly compromise the security of the device.

In regards to the increased use of electronic patient information, the US produced federal standards to secure the privacy of electronic patient data, called the Health Insurance Portability and Accountability Act of 1999 (HIPAA) (Blanton, 2001). Adoption of the HIPAA standards has become increasingly important to all medical institutions, yet Dragoon (2003) found that "less than 10 percent of health-care organizations recently polled by Gartner Research have implemented the security policies and procedures required by HIPAA". This was due to the rapid changes in technology and the final regulations setting numerous functional requirements which were perceived as difficult to meet. Table 2 gives a summary of the HIPAA security requirements.

Extracts from HIPAA Security Requirements
Establishment of trust partnership agreements with all business partners
Formal mechanisms for accessing electronic health records
Procedures and policies to control access of information
Maintaining records of authorising access of information
Assuring that system users receive security awareness training and the training procedures are periodically reviewed and updated
Maintaining security configuration including complete documentation of security plans and procedures, security incident reporting procedure
Communication and network control including maintaining message integrity, authenticity and privacy. Encryption of messages is also advocated for the open network transmission portion of the message
Data authentication to ensure that data is not altered or destroyed in an unauthorised manner.

Table2 - HIPAA Requirements (Misra, Wickramasinghe, and Goldberg, n.d., p.19)

COUNTERMEASURES

Subsequent to identifying the potential risks associated with PDAs, we need to consider how to protect this technology, which includes assurance planning for enforcement of proper security mechanisms. The PDA security countermeasures, like the threats, can be split into hardware, software and data, and management solutions.

Hardware security

Physical security, control of the technology settings, and PDA choice all contribute to hardware security countermeasures. The best way to protect PDAs from theft or loss is by good physical security. Physical security items such as an anchored steel cable and a lock to secure a PDA to an immovable object, a lanyard neck chain, or a holster/vest that fits under a coat and holds PDAs, can help prevent theft or loss (Dvorak, n.d.). Simple measures such as labelling with hospital's name and contact details in case of loss should be used. Furthermore, providing secure places to store PDAs when not in use is essential.

The control of the physical set-up of the technology is also important. For instance, to minimise data leakage from IR ports, and to minimise exposure to remote programming, keeping IR ports closed or disabled during period of non-use is vital (Blanton, 2001). Similarly, PDA connection issues such as disruption and delay when roaming among access points should be minimised. Gruman (2003) found that St. Vincent's Hospital solved this problem by reconfiguring the access points' radio power level. Additionally, adjustment in LAN settings within the hospital to optimise traffic between the wireless and wired segments was made to prevent signal gaps that caused firewalls to reject some roaming users.

Detecting unauthorised changes to sensitive data or components of the PDA, known as tampering, is another important security function (Bluefire, 2003). As there is no specific PDA available recommended for handling medical activities and considering the lack of security features in PDAs, network administrators should carefully select and keep the mix of devices limited. Wilcox and La Tella (2001) regard the following factors as important to consider when choosing a PDA for medical practices:

- **Battery life:** Efficient point-of-care computing demands a battery life at least as long as your medical workday. Most PDAs have battery lives of 2-8 weeks, with colour displays depleting batteries about twice as fast as monochrome screens.
- **Adequate memory:** Medical applications, especially e-texts, tend to be large (1-5 MB). Thus, 8 MB memory should be considered the minimum for a PDA. Many medical users will soon find they require the memory expansion slots.
- **PC synchronisation:** Choose a PDA which can easily synchronise with your PC. Newer PCs may require USB (universal serial bus) synchronisation docks and cable connectors.

Software and data protection

Software protection encompasses such matters as passwords, encryption, antivirus programs and secure networks. Firstly, allowing strong password protection, such as using six to eight characters combined with digits, is a low-cost initial step to secure PDAs (Lyon, 2002). Although PDAs have weak password protection by simply entering a code, there are higher levels of password security becoming available. Such techniques include biometrics (e.g. fingerprinting), inscription of a unique character on the PDA screen using a stylus, specific button sequences and unique ID entry. A password protection program limiting the number of unsuccessful login attempts can enhance this security measure, as does enforcing password re-entry after a period inactivity and marking certain records as password protected. On the other hand, such measures must be balanced with the time and distraction caused to clinicians by persistent password entry. In order to protect some files on PDAs, particularly in the environment in which multiple doctors and nurses work and share the patient information, may need higher level of security than password protection. One of the solutions is to apply encryption techniques.

Encryption is a more advanced level of security using mathematical algorithms to encode passwords and other confidential information. Using encryption programs can ensure that the PDA is effectively inaccessible (automatically locked) without being switched off (Karygiannis & Owens, 2002). Normally encryption needs to be at least 128 bit and the Palm's OS 5 already supports 128-bit file encryption (Bluefire, 2003). However, due to the memory and storage limitations some PDAs cannot utilise strong encryption involving computing-intensive algorithms and larger keys (Ahmad, 2003). This means that IT managers must analyse their specific security requirements before adopting PDA encryption.

Antivirus software is another important security measure for PDAs. The software should scan all entry ports (i.e., beaming, synchronising, e-mail, and internet downloading) as the data is imported into the device, provide online signature update capabilities, and prompt the user before it deletes any suspicious files. Popular products currently available include Trend Micros' 'PC-Cillin for wireless' and Symantec's PDA antivirus for Palm OS.

Secure networks are important in PDA security also. Firstly, the use of a firewall that is responsible for filtering all incoming and outgoing packets consistent with a protection policy can be used. Firewall methodologies include the use of media access control (MAC) address filtering and wired equivalent privacy (WEP). MAC address filtering helps to restrict access to authorised MAC address devices associate with the wireless network. WEP is an encryption methodology for protecting wireless communications from eavesdropping, modification, and prevent unauthorised access. Secondly, protection from wireless vulnerabilities can be achieved by installing a Virtual Private Network (VPN) client on the PDA (Jupitermedia Corporation, 2003). This method is particularly important in the healthcare environment, which handles patient confidential data. A VPN is a private communication network that is built using shared public infrastructure. It is constructed by building an encrypted virtual "tunnel" between two entities whose identities are mutually authorised prior to construction

(Baker, 2003). A VPN benefits from secure wireless communications using both authentication and encryption methods that are stronger than those specified in WEP. Moreover, because it is based on open standards, device interoperability can be maintained. The main disadvantage of installing a VPN client on a PDA is that it can result in slower session establishment times (Greene, 2001). However, access to patient record or related confidential resources should be through a VPN to provide effective countermeasures against threats to the confidentiality, integrity, and authenticity of the information being transferred (Karygiannis & Owens, 2002).

Management solutions

The management of the technology users and related organisational security polices is another important aspect of an overall security plan. These include risk assessment and development of appropriate security policies. Risk assessment to determine the required level of security and periodic audits should be part of the management processes due to the growing and shifting security threats.

Dragoon (2003) suggests that to ensure the HIPAA security and privacy standards are met, that the organization should establish a security team to oversee security and therefore increase corporate responsibility. The security policies must be created and implemented to provide adequate protection for the PDA equipment and the associated data (Blanton, 2001). User responsibility and liability, together with authorised use, inventory and security audits should be part of the policies. Additionally, user education is an intrinsic part of this measure.

Finally, the security policies should also cover issues such as backups. Frequent backups can reduce loss of data and downtime when a PDA is lost, stolen, wiped clean, or damaged beyond repair (Bluefire, 2003). Sensitive information stored on the PDA device should be deleted when no longer required. Such information can be archived on the PC during synchronisation and transferred back to the PDA when needed.

CONCLUSION

It is clear that the use of PDA technology creates location independent access to information and provides a mobility which can benefit clinical staff in healthcare environments. However, the risks and threats associated with the use of the technology can interfere with effective continuous workflow. This is affected by battery life and signal access, and potential data leakage and confidentiality risks. The problems are compounded by a lack of built-in PDA security features, lack of security awareness by users, and the perceived difficulty in meeting security standards. The institutions must understand the importance of compliance with security and privacy mandates such as the HIPAA regulations. However, these issues are not insurmountable using appropriate countermeasures. Good physical security, addressing signal disruptions and careful selection of equipment are basic hardware and setup measures. Use of improved encryption techniques and creating secure networks using VPNs, firewalls and antivirus protection are obligatory. However, such measures need to be balanced with data access and session establishment delays often associated with increased security on PDA technology. Finally, good risk management assessment, security policies and their implementation, together with educating users in security risk and protection is important.

Clinical and IT staff need to work together in order to successfully make effective and secure use of PDAs in the healthcare environment. The next generation of PDA technologies will include speech recognition, handwriting recognition, bar code scanners and compatibility with digital thermometers and blood pressure monitors, all of which will allow for increased connectivity and ease of use. Therefore it is essential that clinical and IT staff share their knowledge to make effective use of handheld technology, and create secure environments for PDA use and similar future technology.

REFERENCES

Ahmad, Z. (2003). *Wireless security in health care.* Retrieved April 25, 2004, from http://www.cs.mu.oz.au/~bir/auscc03/papers/ahmad-auscc03.pdf

Baker, D. (2003). *Wireless (in) security for health care (HIMSS).* Retrieved April 18, 2004, from http://www.himss.org/content/files/WirelessInsecurityV11.pdf

Blanton, S. H. (2001). *Securing PDAs in the health care environment* (*SANS Institute).* Retrieved April 15, 2004, from http://www.sans.org/rr/papers/41/256.pdf

Bluefire Security Technologies. (2003, January). *Mobile insecurity: A practical guide to threats and vulnerabilities*. Retrieved May 22, 2004, from http://www.bluefiresecurity.com/downloads/Bluefire%20Whitepaper-Mobile%20Insecurity.pdf

Dragoon, A. (2003). Eight (not so) simple steps to the HIPAA finish line. *CIO Magazine.* Retrieved May 22, 2004, from http://www.cio.com/archive/070103/eight.html

Dvorak, R. D. (n.d.). *Use of personal digital assistants to store medical information - a growing HIPAA issue*. Retrieved 20 April, 2004, from http://www.veteranspress.com/pages/quarterly2.pdf

Greene, T. (2001). VPN software aims to safeguard handheld devices, *Network World Fusion.* Retrieved May 26, 2004, from http://www.nwfusion.com/archive/2001/117214_02-19-2001.html

Gruman, G. (2003). Wireless: just what the doctor ordered. *CIO Magazine.* Retrieved May 16, 2004, from http://www.cio.com/archive/080103/mobile.html

Jupitermedia Corporation. (2003). *PDA security 101.* Retrieved May 24, 2004, from http://www.intranetjournal.com/articles/200304/ij_04_07_03a.html

Karygiannis, T. & Owens, L. (2002). *SP 800-48, Wireless network security 802.11, Bluetooth and handheld devices.* Retrieved 1 April, 2004, from http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

Kleinberg, K. & Dulaney, K. (2001). PDAs, smart phones and wireless computing in healthcare. *Gartner.* T-13-9251

LaRochelle, B. (2002). PDAs and the emerging security crisis. *Health Management Technology, 23*(10), 68-67

Lyon, D. M. (2002). *The dilemma of PDA security: An overview (SANS Institute).* Retrieved May 22, 2004, from http://www.sans.org/rr/papers/41/257.pdf

Marsh, M. A. & Bulanti, R. (2003). *Doctor Recommended: PDAs are Good Medicine.* Retrieved May 25, 2004, from http://www.sybase.com/detail/printthis/1,6907,1026297,00.html

Misra, K.S., Wickramasinghe, N. & Goldberg, S. (n.d) *Security challenge in a mobile healthcare setting (INET International Inc).* Retrieved May 1, 2004, from http://www.itacontario.com/policy/wireless/WES-v4-conf.pdf

Wilcox, R. A. & La Tella, R. R. (2001). The personal digital assistant: a new medical instrument for the exchange of clinical information at the point of care, *Medical Journal of Australia 175*(12), 659-662. Retrieved May 27, 2004, from http://www.mja.com.au/public/issues/175_12_171201/wilcox/wilcox.html#box1

COPYRIGHT