



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

PDA – Asset or Liability?

SANS Security Essentials
Course GIAC1 Certification
Version 1.4b

Graham Pond
December 2003

Contents

| | |
|---|-----------|
| 1.0 Abstract..... | 3 |
| 2.0 PDAs and Mobile Computing | 4 |
| 2.1 History of the PDA..... | 4 |
| 2.2 Towards the Future..... | 5 |
| 2.2.1 Hardware Capacities..... | 5 |
| 2.2.2 Power Consumption..... | 5 |
| 2.2.3 Applications..... | 5 |
| 3.0 The Corporate Asset..... | 6 |
| 3.1 Characteristics of the Modern PDA..... | 6 |
| 3.2 Software and Attachable Devices..... | 7 |
| 3.3 Benefits for Information Management..... | 8 |
| 3.3.1 Organisational Support | 8 |
| 3.3.2 Information Portability | 8 |
| 3.3.3 Information Mobility..... | 8 |
| 3.3.4 Information Harvesters | 8 |
| 4.0 The Corporate Liability | 9 |
| 4.1 PDA Security Concerns | 9 |
| 4.1.1 Physical Security..... | 9 |
| 4.1.2 Connection to Networks | 9 |
| 4.1.3 Exchange of Information | 9 |
| 4.1.4 Lack of User Awareness | 9 |
| 4.1.5 Security Compliancy | 9 |
| 4.2 PDA Vulnerabilities | 10 |
| 4.2.1 Outsider attack from the Internet..... | 10 |
| 4.2.2 Outsider attack using 802.11x or Bluetooth..... | 10 |
| 4.2.3 Outsider attack using Infrared | 10 |
| 4.2.4 Insider attack from a local Network | 10 |
| 4.2.5 Attack from malicious code | 10 |
| 4.3 Attacking PDAs..... | 11 |
| 4.3.1 Social Engineering | 11 |
| 4.3.2 Brute Force | 11 |
| 4.3.3 Session Hijacking..... | 12 |
| 4.3.4 Man in the Middle..... | 12 |
| 4.3.5 Sniffer Attack..... | 13 |
| 5.0 Protecting Corporate Information..... | 14 |
| 5.1 Corporate PDA Policy..... | 14 |
| 5.2 Characteristics of Security Software | 15 |
| 6.0 Conclusion..... | 16 |
| 7.0 References..... | 17 |

1.0 Abstract

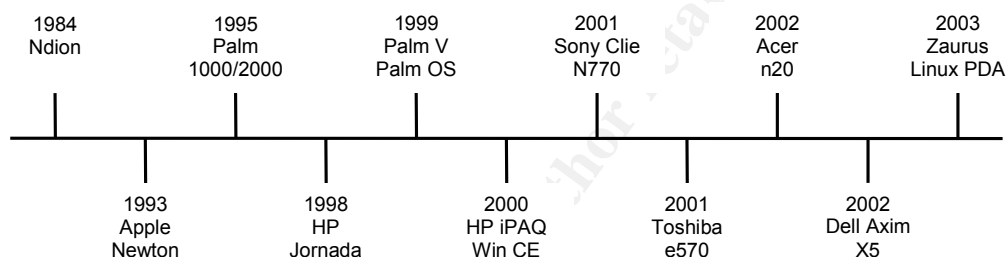
The corporate interest and wide spread use of Personal Digital Assistants (PDAs) has increased dramatically over the last five years. This is a as result of the corporate focus switching towards information management and portability. Mobile computing devices such as Tablet PCs, Notebooks and PDAs are becoming a more effective means of accessing corporate Information Systems. In the corporate environment there are many advantages and practical uses for the modern PDA, however increased functionality results in larger security concerns. This paper will provide the reader with a general overview of the features and the security concerns regarding PDAs and their use in a corporate environment. Detailing extensively the many different security vulnerabilities and risks that face PDAs and weighing them up against their benefits. This document also attempts to make the reader consider whether managers and executives should categorise PDAs and similar mobile computing devices as an asset or a security liability for their organisation.

© SANS Institute 2004, Author retains full rights.

2.0 PDAs and Mobile Computing

2.1 History of the PDA

The history of the PDA began in 1984 when a little known technology company from the United Kingdom released the Psion, the world's first handheld computer¹. The Psion One comprised mainly of an electronic organiser and it proved successful enough to obtain the interest of major technology companies rapidly identifying the market possibilities of these miniature computers. Apple Computers Incorporated was the first to take advantage of this in 1993 when they released the Apple Newton. The relatively simplistic Apple Newton proved to be a starting point for the replacement of commonly used personal organisers such as the filofax. Palm Incorporated joined the mobile computing market in March of 1996, introducing its palm sized Pilot 1000 and Pilot 5000², consequently increasing the popularity of the PDA.



In 1998 Hewlett Packard launched its first PDA with the Jornada 820 pocket sized PC, operating on Windows CE. The Jornada 420 quickly followed, being the first Windows CE pocket size PC to incorporate a colour screen, paving the way for the release of the iPAQ Pocket PC in April 2000.³ However, it was the Palm V organiser that was released in 1999, which revolutionised mobile computing, incorporating intelligent graffiti or scribble tool and together with an advanced Palm Operating System (Palm OS) it improved applications with increased functionalities. This developed the interest beyond the executive office to the waiters in fashionable cafes.

Over the last five years other major technology companies have increased their focus on developing handheld devices for the growing mobile computing market. Dell Computers Axim range, HP's iPAQ, Acer's n-Series, Toshiba's Pocket PC and Sony's Clie PDA devices are all competitive in the developing marketplace. (Refer to section 3.3 Characteristics of the Modern PDA.)

Although the history of these mobile computers is relatively brief, their popularity has rapidly increased to be an essential organisational tool for use from the boardroom to the mailroom.

¹ <http://ww6.investorrelations.co.uk/psion/EditHistory.shtml>

² <http://www.palm.com/us/company/corporate/timeline.html>

³ http://www.hp.com/hpinfo/about/hp/histnfacts/timeline/hist_00s.html

2.0 PDAs and Mobile Computing

2.2 Towards the Future

Considering the comparatively brief history of the PDA together with their high paced technological advancements, these mobile computers are rapidly evolving to meet future needs. The main areas that the PDAs will continually develop in are hardware capacities, power consumption and applications.

2.2.1 Hardware Capacities

Processor speeds, memory and storage space will be the major technological advances in PDAs, thus making them more competitive with notebooks or even desktop PCs. Faster and larger hardware devices will become more compatible with PDAs, though the use of compact flash, PCI or even USB ports. Built in wireless devices are already standard on most high quality PDAs and the power and signal quality will only increase in the future. Employed mainly for security purposes, the use of biometrics is increasing and becoming a more prominent feature on modern PDA, using finger print scanners for access control.

2.2.2 Power Consumption

Power supply will become more sophisticated as power consumption improves and battery life increases, this inevitably will allow users to remain mobile for longer.

2.2.3 Applications

To support the increased developments in hardware and power consumption, applications designed for the PDAs will develop to become more sophisticated and less CPU intensive. Sharp has recently released its Zaurus SL-5500, which is the first commercially available PDA to support a Linux based Operating System.⁴ Opening up a commercial PDA to Linux based applications may increase the competition and consequentially lead to the increased development of PDA applications. The Intel Corporation have recently released information on its next generation XScale technology based processors for the use in PDAs, mobile phones and similar mobile wireless devices.⁵ These new generation Intel processors, known as “Bulverde” will increase both multimedia and application performance, for example enabling the wireless devices to capture higher quality pictures while preserving the battery life.

"The ability to send and receive pictures, play rich 3D games or download ring tones, video clips and music are growing in popularity. To support the ongoing adoption of data services and applications, the underlying technology must be able to deliver enhanced multimedia capabilities and lower power."⁶

This comment from the Intel vice president, summarised the need for these next generation processes. It is this type of technology that will reduce the distance between the PDA and a sophisticated mobile phone.

⁴ <http://www.vnunet.com/News/1131034>







⁵ <http://www.intel.co.in/pressroom/>

⁶ <http://www.intel.co.in/pressroom/archive/releases/20030917net.htm>

3.0 The Corporate Asset

3.1 Characteristics of the Modern PDA

There are many different PDA products globally available to consumers. Below is a table which details the specifications of six popular PDA from leading manufacturers.

| |  TUNGSTEN C ⁷ |  iPAQ h5555 ⁸ |  Clie NX80V ⁹ |  e750 ¹⁰ |  Axim X3i ¹¹ |  n20w ¹² |
|----------------------------------|--|--|--|--|---|---|
| Operating System | Palm OS V5.2.1 | Microsoft Windows Mobile 2003 | Palm OS V5.0 | Microsoft Pocket PC 2003 | Microsoft Pocket PC 2003 | Microsoft Powered Pocket PC |
| Processor | Intel 400Mhz | Intel 400Mhz | 200Mhz | Intel 400Mhz | Intel 400Mhz | Intel 400Mhz |
| System Memory | 64MB | 128MB SDRAM | 32MB | 64MB SDRAM | 64MB SDRAM | 64MB SDRAM |
| Memory Flash | - | 48MB | 32MB | 32MB | 64MB | 32MB |
| Screen | 320 x 320 Colour | 3.8" Colour TFT LCD | 320 x 420 TFT Colour | 3.8" Colour TFT | 3.5" Colour QVGA TFT | 3.8" Colour TFT LCD |
| Built-In Wireless 802.11b | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ |
| Bluetooth | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Infrared | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ |
| Built -In Hardware | Keyboard | ✗ | Digital Camera & Keyboard | ✗ | ✗ | ✗ |
| Expansion Pack (CF) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Biometrics | ✗ | Finger Print Reader | ✗ | ✗ | ✗ | ✗ |
| Weight | 6.3oz | 7.29 oz. | 8 oz. | 6.9 oz. | - | 235g |

⁷ <http://www.palmone.com/us/products/handhelds/tungsten-c/>

⁸ <http://welcome.hp.com/country/us/en/prodserv/handheld.html>

⁹ <http://sonyelectronics.sonymstyle.com/micros/clie/models/nx80v.html>

¹⁰ <http://www.toshiba.com/tai-new/Services.jsp>

¹¹ <http://www.dell.com/>

¹² <http://global.acer.com/products/pda/n20w.htm>

3.0 The Corporate Asset

3.2 Software and Attachable Devices

There is a large range of hardware accessories and software available for most PDA devices, which helps to enable corporations to utilise their mobile computers to the maximum capacity.

- **SD Memory Cards** – These are storage devices that plug into the PDAs compact flash card slot. They are available from most PDA manufactures and usually range from 64MB to 1GB. Using encryption software, these memory cards can be individually protected and be used to transfer large amounts of data throughout corporate networks.
- **Connectivity Devices** – These are usually in the form of compact flash cards, consisting of Modems, Bluetooth, Infrared and Wireless LAN compact flash cards. They can be used to connect PDA devices to corporate network access points, printers, other mobile devices and even GPS navigational hardware. These can also be used as a security tool for detecting other wireless devices, which could be a threat to the corporate network.
- **Barcode Scanners** – These can be connected to PDAs using the compact flash or PC card expansion pack slots. Barcode scanners have the potential to turn a PDA into an integral asset control device, suitable for any corporation.
- **Expansion Packs** – These are available to suit most of the popular PDA models, giving the possibility for compact flash slots or even a PC Cards, allowing users to connect multiple devices.
- **Digital Cameras** – These and similar multimedia devices could be useful for a wide range of tasks. Other peripherals, such as connectable keyboards, protection cases are commonly available for most PDA models.
- **Operating Systems** – Depending on the manufacturer, PDAs are loaded with different operating systems including, Palm OS, Pocket PC and Linux for the PDA. All of these operating systems support the implementation of third party software and the standard features such as file management, word processing, Internet browsing and organisational capabilities.
- **Security Software** – This is an essential requirement for any corporation that takes security seriously. Security software can provide access control, data encryption, anti virus scanners, firewalls and policy controllers.
- **Third Party Software** – Games and multimedia applications are the most common commercial software available for the PDA. However, corporate specific software can be tailored to for different business needs and requirements. Anti virus and security software are widely available for PDAs, however due to lack user awareness these applications are usually neglected.

3.0 The Corporate Asset

3.3 Benefits for Information Management

As corporate focus switches towards information management, portable devices such as Tablet PCs, notebooks and PDAs are becoming a more effective means of accessing corporate information systems. PDAs provide a unique alternative to other mobile computers, given their size and mobility.

3.3.1 Organisational Support

Regardless of the Operating System and brand of PDA, most models are usually fully equipped with organisational support applications, the motivation for the original PDA. Applications such as the calendar, scheduler, Internet browser and email agent are all applications that can be synchronised with desktop applications, using programs such as Microsoft's ActiveSync¹³. The ability to carry a pocket or palm sized computer around as a personal organiser or wireless link to the network for email or Internet access is an asset for any individual in a corporation that focuses on productivity.

3.3.2 Information Portability

Progressively PDAs are acquiring the same capabilities as those of laptop computers. Documents and files can be produced or stored on these mobile computers and can be simply transferred between devices using a cable or wireless link. This provides PDAs the capability to function like a thumb drive with the bonus ability to edit and compose the documents. This would be valuable asset for users when revising before presentations, quoting figures during meetings or simply as a miniature notebook.

3.3.3 Information Mobility

As shown in section 3.1 *Characteristics of the Modern PDA* most new PDAs come fully equipped with wireless technologies such as 802.11b, Bluetooth or Infrared. These technologies can be used with wireless LANs or access points to retrieve information within a campus, building, office or workspace. This provides information mobility for organisations, which aspire to have the ability to access data instantly away from the desktop computer or server.

3.3.4 Information Harvesters

PDAs offer a much cheaper and simpler solution to information harvesting, such as surveying, inventory control and general data collection. As previously stated plug-in hardware such as barcode scanners could be used to account for and manage any corporate asset. Surveys of clients or employees could be conducted more personally and efficiently with the use of a PDA, also enabling instant reporting using wireless technology solutions.

¹³ <http://www.microsoft.com/windowsmobile/resources/downloads/pocketpc/activesync35.msp>

4.0 The Corporate Liability

4.1 PDA Security Concerns

PDA security is a major concern for all IT Security professionals in the corporate, government or business environment. The extensive uses and advantages of the PDA unfortunately bring about major security concerns.

4.1.1 Physical Security

Physically securing a PDA is an important security concern as they are very susceptible to loss and theft because of their size, portability and value. After a PDA is obtained, without adequate security software stored information can be accessed or removed usually without any difficulty.

4.1.2 Connection to Networks

Connecting a PDA to a network or stand alone PC is relatively easy providing the correct software and hardware is available. The security concern with PDAs connecting to other computers or networks is that they have the ability to distribute viruses through the exchange of information, often bypassing network firewalls or network defence mechanisms.

4.1.3 Exchange of Information

PDAs allow the simple exchange of business and personal information from one PC to another. Sensitive information such as an address book or a private document can be easily relayed between computers using PDAs. This enables information to leave networks without passing through appropriate corporation specific security applications.

4.1.4 Lack of User Awareness

Users are often unaware of the security issues and associated security procedures relating to PDAs. For example the implications of losing a PDA that contained a personal address book, listing contacts details such as, email and home addresses, telephone numbers and work group related information. Security awareness procedures are often ignored or avoided by users because they do not understand the security threats associated with PDAs.

4.1.5 Security Compliancy

Lack of security procedures and high compliancy is a major problem that security advisors and administrators often confront. Weak or no (blank) passwords is one the most prominent security risk facing PDAs today. Since a PDA looks small and compact, users can be ignorant when considering security risks, as they do not appear to be as powerful or versatile as a notebook, making them more dangerous security risk.

4.0 The Corporate Liability

4.2 PDA Vulnerabilities

When considering the implementation of PDAs in a corporation, as for any new product, it is essential to derive a list of possible vulnerabilities. This provides administrators or managers with knowledge of areas that are susceptible to intrusion or compromise the integrity of the product. An integral step in determining possible vulnerabilities is to construct a Threat Vector Lists¹⁴. This will determine the different avenues that can be used to compromise or present a threat to PDAs.

4.2.1 Outsider attack from the Internet

This type of threat uses the corporate network to obtain access to the PDA. This can be achieved by exploiting network vulnerabilities such as a weak or insufficient firewall, which leads to accessing the PDA through an access point or web server.

4.2.2 Outsider attack using 802.11x or Bluetooth

This threat exploits the PDAs compatibility to communicate with other devices wirelessly. This can be achieved when the attacker is in close proximity and can connect to the PDA wirelessly.

4.2.3 Outsider attack using Infrared

This threat requires line of sight with the infrared panel on the PDA. Despite this important factor these attacks can be quite effective, for example a microphone could be activated using malicious code and live audio streaming could be beamed via Infrared to a receiver complete with an audio decoder. Although in most cases range of an Infrared beam is quite small they can be dramatically increased using directional telescopes.

4.2.4 Insider attack from a local Network

This is a threat that evades corporate firewalls and intrusion detections systems as the attacker is inside the network. These attacks are usually very *“advance and subtle, and there is potential for trouble”*¹⁵ as the attacks have bypassed the different layers of defence and defence in depth principals.

4.2.5 Attack from malicious code

This threat includes viruses, trojans, worms or specific code that has been developed to complete a particular requirement. As previously stated malicious code can be most effective when used in conjunction with hardware or network devices, such as the microphone and Bluetooth beam.

¹⁴ Cole, Fossen, Northcutt, Pomeranz “SANS Security Essentials with CISSP CBK”. The SANS Institute, April 2003. Volume One, Pages 849-862.

¹⁵ Cole, Fossen, Northcutt, Pomeranz “SANS Security Essentials with CISSP CBK”. The SANS Institute, April 2003. Volume One, Page 853.

4.0 The Corporate Liability

4.3 Attacking PDAs

There are many different methods and techniques that can be used to attack or compromise information security on PDAs. In the majority of cases the most successful attacking techniques are performed inconspicuously, unknown to the user.

4.3.1 Social Engineering

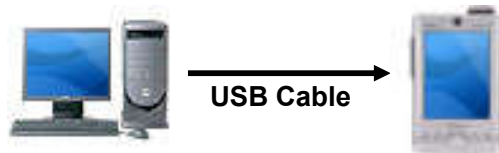
This is a technique that relies on human nature's weakness to trust and help others to access or obtain information about computer systems. The Hyper Dictionary website defines social engineering as the,

*"aim to trick people into revealing passwords or other information that compromises a target system's security"*¹⁶

This can be achieved using various different techniques, including fake assistance calls, telephone/email/online surveys or technician imposers. Any information obtained by any of these methods can be extremely useful for attackers who are trying to obtain access to a PDA. An example of this would be a support call from the IT Help Desk instructing the user to leave their PDA at the reception desk so that a company technician can upgrade the battery. To the unaware victim this seems like a reasonable, genuine request. The victim's PDA could then be collected by the fraudulent technician, information could be directly accessed and spy or tracing software could be installed, totally oblivious to the victim.

4.3.2 Brute Force

A common and effective means to access a computer system is by cracking passwords. Brute force programs use customised cracking applications that attempt to guess passwords by using every possible combination of alphabetic, numeric and special characters. These applications can be tailored attack passwords on different computer systems and the time period evolved depends on the strength of the password and the speed of computer.



17

Processor speeds of PDAs are relatively insignificant compared to a desktop PC, therefore the most powerful brute force attacks can be done using a direct connection, such as a USB cable. Chief Security Officer of Softnet Security, John Nevado stated,

*"A good PC can manage 1,000,000 combinations per second ... a big dictionary contains 100,000-200,000 words"*¹⁸

¹⁶ <http://www.hyperdictionary.com/computing/social+engineering>

¹⁷ Hardware images from <http://www.dell.com>

4.0 The Corporate Liability

4.3 Attacking PDAs

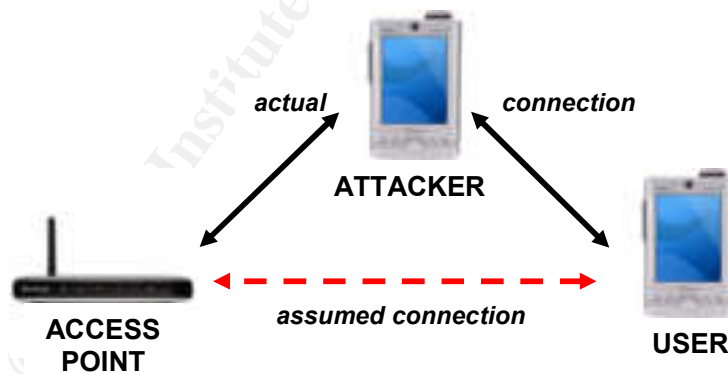
The brute force method of compromising PDA security relies on the fact that login attempts will not be disabled after any number of attempts. If this security feature is present, as it is with Microsoft's ActiveSync 3.5, additional software can be available to disable it.

4.3.3 Session Hijacking

Session Hijacking can be used to overtake a connection after authentication has been completed. This technique can be easily applied to PDAs connecting to network access points. It exploits a well known problem with Wi-Fi, the ability to take over or hijack a TCP session. PDAs are just as vulnerable to this form of attack as other Wi-Fi devices. It works by the hacker waiting until a user (the victim) successfully authenticates itself with the network access point. After this has occurred, the hacking then sends a disassociate message to the user, spoofing the message so it appears that it was sent from the network access point. The hacker now has the necessary details of the user and the user believes that they have been disconnected, so the hacker can exploit the original connection with the access point.

4.3.4 Man in the Middle

These attacks can be used to monitor or intercept, modify or even block messages or information sent between two PDAs. Man in the Middle attacks could be used to masquerade as an access point to a PDA and a PDA to an access point. Hence giving the *middle* computer the ability to monitor and control the flow of traffic.



19

This relies on an inherent security problem of 802.1x, in that they use one-way authentication, allowing PDAs to authenticate with access points but not the other way round.

*"Instead of one-way authentication, wireless LANs need to implement mutual authentication to avoid this problem"*²⁰

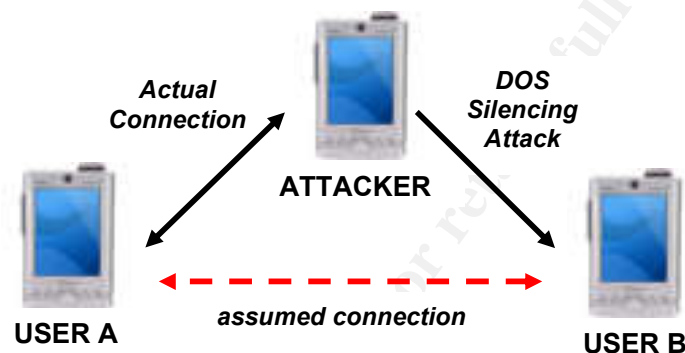
¹⁸ <http://www.itsecurity.com/asktecs/jul101.htm>

¹⁹ Hardware images from <http://www.dell.com>

4.0 The Corporate Liability

4.3.4 Man in the Middle

Man in the Middle attacks can also monitor traffic between two PDAs. Even with secure connections these attacks can compromise information security, giving hackers the ability to modify, monitor and control the flow of information. During the exchange of public keys, an attacker could block the messages and replace the public keys with its own, essentially establishing two secure connections. Assuming the attacker continues to exchange the information sent and received, in most scenarios this security compromise would be unknown to the users. As shown below Denial of Service (DOS) attacks could also be used to effectively silence a PDA or connecting device.



21

Denial of Service (DOS) attacks occur when connection requests are repeatedly sent to the victim effectively crippling their ability to respond to new or existing requests. This technique can be utilised in Man in the Middle attacks to ensure that *User B* is silence and *User A* does not receive two responses.

4.3.5 Sniffer Attack

Applications specifically designed for PDAs can be used to silently monitor and sniff network traffic. These can be used to obtain information such as user names, passwords and confidential corporate information. Software specifically designed to sniff access points, Wi-Fi devices and network traffic can be freely downloaded and installed on Wi-Fi compatible PDAs. An example of this an application called MiniStumbler, which is the PDA compatible version of NetStumbler, written by Marius Milner²². Although MiniStumbler was predominantly designed to be a practical 802.11b based wireless network auditing tool, the website states that it was developed with the following users in mind.

“Security folks wanting to check that their corporate LAN isn't wide open; Systems admins wanting to check coverage of their Wireless LAN; Gatherers of demographic information about 802.11 popularity, Drive-by snoopers; Overly curious bystanders”²³

²⁰ <http://www.wi-fiplanet.com/tutorials/print.php/1377171>

²¹ Hardware images from <http://www.dell.com>

²² <http://www.netstumbler.com/modules.php?op=modload&name=FAQ&file=index>

²³ <http://forums.netstumbler.com>

5.0 Protecting Corporate Information

5.1 Corporate PDA Policy

It is essential for all corporations or government departments to have specific policies regarding the use of PDAs in their network environment. This is important to attempt to control the devices connecting to the corporate network and minimise the security risks and threats. Before corporate policy is decided upon there should be extensive research into the impact both positive and negative that PDAs would have in the corporate environment.

“Few organisations invest in proper risk assessments before implementing controls. Even fewer have the capability to understand and qualify threats to their information assets in order to accurately assess risk.”²⁴

It is important to perform a detailed risk assessment before constructing a corporate policy. There are many different techniques that can be used to determine and categorise threats and risks when constructing such a policy. The first step is to identify and list all risks, threats and vulnerabilities and categorise the severity of their occurrence. Here is an example of risks associated with using PDAs in the corporate environment.

| Risk # | Risk Detail | Impact |
|--------|---|---------|
| 1 | Loss of PDA, remote access to the corporate network. | EXTREME |
| 2 | Loss of PDA, access to locally stored information only. | HIGH |
| 3 | User activates Bluetooth, Infra Red or 802.11b without adequate security, sending information without encryption. | MEDIUM |
| 4 | Loss of PDA, security software deletes stored information. | LOW |

The next step is to determine the likelihood of these risks occurring and the cost to the corporation if they occurred. Once the vulnerabilities, risks and threats have been identified and categorised the next step in constructing a corporate policy would be to perform a Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis.

This type of assessment is important when constructing corporate PDA policy, as it helps to determine whether the strengths and opportunities outrank the weaknesses and threats. This method of assessment helps in providing initial research when constructing the corporate policy. There are eight characteristics of an adequate security policy²⁵, they include;

| | |
|--|--|
| Describe each job function, with an individually tailored policy. | Make the policy meaningful and specific to the corporation. |
| Keep the policy, relevant to the developments and changes that arise | Ensure the policy is endorsed and signed, by adequate personnel. |
| Define appropriate limits in the policy. | Inform upper management of policy. |
| Ensure the policy is clear and concise. | Keep the policy up to date and current. |

²⁴ Cole, Fossen, Northcutt, Pomeranz “SANS Security Essentials with CISSP CBK”. The SANS Institute, April 2003. Volume One, Page 383.

²⁵ Cole, Fossen, Northcutt, Pomeranz “SANS Security Essentials with CISSP CBK”. The SANS Institute, April 2003. Volume One, Pages 365-366.

5.0 Protecting Corporate Information

5.2 Characteristics of Security Software

Most of the PDA operating systems that are available today fail to provide the necessary security that is required to adequately protect a PDA. Corporations that permit the use of PDAs must strongly consider the use of third party security software. These applications usually focus on access control and data encryption, however, there are many different features effective third party security software.

- **Anti virus** – Virus and malicious code scanners are just as crucial for PDAs as they are for notebooks or PCs. The main problem with anti virus software for PDAs is that they require a great deal of processor speed and memory space for virus definitions. It is for this reason that mobile anti virus software is often installed on a PC, which scans the PDA as an attached device.
- **Authentication and Access Control** – This is essential to control weak or simple passwords or paraphrases. Most PDA security applications have the ability to control the characteristics of passwords, for example eight characters including at least one special character.
- **Biometrics** – Hand writing or signature access control can be used to authenticate users for original logon or specific folder access. This success of this strongly depends on the quality of the recognition software and the user's ability to consistently reproduce a signature or block of text.
- **Centralised Management** – For large corporations it is important for security administrations to have the ability to manipulate centralise management for PDAs. This enables the security administrators to update the security policy on individual PDAs, account for each device and produce access.
- **Data Encryption** – This is the main focus and selling point for the majority of PDA security software vendors. The ability to strongly encrypt the information stored on the PDA is a vital security aspect. Different encryption software incorporates different types and strengths of the algorithm, the ability to choose the files to encrypt and the option to automatically encrypt data.
- **Flash card** – It is important that the security application has the ability to handle plug in memory as it was incorporated in the PDA. For example, scanning and encrypting compact flash card memory.
- **Lock Out Format** – This can sometimes be referred to as 'bombing memory'. It occurs when all information stored on the PDA is erased, after a security breach has occurred, for example after a password is incorrectly entered three times. Stored information can be easily backed up on PCs to avoid the loss of data.
- **Multiple OS Support** – Large corporations could have different types of PDA which in turn have different OS, such as Linux, Palm OS, and Windows Pocket PC. It is important to have a consistent PDA security policy, regardless of the OS.

6.0 Conclusion

As with all areas of Information Technology, it is important to apply solid security techniques when considering PDA security. Security is an investment for corporations and governments, consequently it can be an area that is often neglected. Prior to the introduction of PDAs or other mobile computing devices, appropriate policy and security measures should be implemented to ensure information security and integrity. Third party security software should be strongly considered by corporations to provide maximised security. These security applications include different techniques to protect information that is stored on PDAs. However in order for these applications to be effective other security procedures outlined in corporate policy need to be followed. Corporations should carefully consider both the value of PDAs as an asset or the possible security liability they could present if the information they held was compromised.

© SANS Institute 2004, Author retains full rights.

7.0 References

1. Webopedia Online Dictionary, PDA,
<http://www.webopedia.com/TERM/P/PDA.html>
2. History of PDAs,
http://www.thecore.nus.edu/writing/ccwp10/james/pda_history.html
3. PC TechGuide, The PC Technology Guide,
<http://www.pctechguide.com/25mob3.htm>
4. PDA Accessories – Prices and Reviews at DealTime,
http://hardwarecentral.dealtime.com/xPP-PDA_Accessories
5. PDastreet : Software,
<http://www.pdastreet.com/software.html>
6. Internet | Security | Systems, Session Hijacking,
http://www.iss.net/security_center/advice/Exploits/TCP/session_hijacking/default.htm
7. Computer Cops – The danger of PDAs – information security portal & forums
<http://www.computercops.biz/article1710.html>
8. Computer Cops – PDA Security 101 - information security portal & forums,
<http://www.computercops.biz/article2317.html>
9. Security Team.com (IPC@Chip Multiple Security Vulnerabilities)
<http://www.securiteam.com/securitynews/5CP001F4AC.html>
10. BlueSys Home Page, PDA Security 101,
http://www.bluesys.be/default.asp?p=DisplayNews.asp?Ncat_ID=3&NewsID=194
11. Intranet Journal, PDA Security,
http://www.intranetjournal.com/articles/200304/ij_04_07_03a.html
12. Info World: Researches crack new wireless security spec:L Feb 14, 2002: By Ephraim Schwartz,
http://www.infoworld.com/article/02/02/14/020214hnwifispec_1.html
13. CNET Reviews: Security Watch,
http://reviews.cnet.com/4520-3513_7-5021256-1.html
14. Computer Security Dictionary: Man in the Middle Attack,
<http://www.itsecurity.com/dictionary/middle.htm>
15. Developer.Com, Secure Coding: Attacks and Defences,
http://www.developer.com/tech/article.php/10923_2235901_2
16. Man In the Middle Attack,
http://www.tools4ever.com/resources/manual/monitormagic/Man_in_the_middle_attack.htm
17. SANS InfoSec Reading Room – Security White Papers,
<http://www.sans.org/rr/>
18. INFOTECH, A brief history of PDAs, Hawking would not narrate, Dec 11 2000,
http://www.inq7.net/infotech/dec2000wk2/info_12.htm
19. Cole, Fossen, Northcutt, Pomeranz “SANS Security Essentials with CISSP CBK”. The SANS Institute, April 2003. Volume One.
20. Cole, Fossen, Northcutt, Pomeranz “SANS Security Essentials with CISSP CBK”. The SANS Institute, April 2003. Volume Two.