Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The PDA as a Threat Vector

Personal Digital Assistants (PDAs) have been steadily increasing in numbers since their inception in the early 1990s. Explosive growth in their numbers, particularly within the enterprise, is expected during the next three years. This presents a number of management challenges, both operational and technical. This paper addresses the threat to information security posed by the PDA (including related devices such as smartphones). It discusses the drivers behind the PDA's increasing numbers and the changing nature of PDA...

Copyright SANS Institute

Author Retains Full Rights

AD

The PDA as a Threat Vector

Richard Price
GSEC Practical Assignment V.1.4b
March, 2003

Abstract **2**
The Evolution of The PDA **2**
Organisations' Attitude To The PDA **3**
Snapshot of the PDA **3**
Drivers For Change **4**
The Changing Threat Profile of The PDA **4**
PIM Functions *5*
Communications *5*
Desktop-Compatible Applications *5*
Vertical Applications *6*
Enterprise Applications *6*
The Nature of The Threat **7**
Portability Is A Threat *7*
Poor Native Security Mechanisms *7*
Unencrypted Storage *7*
Stored Credentials *8*
Malicious Software *8*
Social Engineering *9*
Malicious Use *9*
Wireless Threats *9*
Organisational Remedies To Secure PDAs **10**
PDA Policy *10*
Purchasing Control and Standardisation *10*
Support Mechanisms *10*
Development and Application Guidelines *11*
Technical Remedies And Tools To Secure PDAs **11**
Authentication and Access Tools *11*
Biometrics *11*
Encryption Tools and Applications *12*
Antivirus Tools *12*
Integrated Security Tools and Policy Tools *12*
Systems Management Software *13*
VPN Software *13*
The PDA as a Security Tool **13**
Future Trends **14**
Conclusion **15**
References **16**
Appendix A Selected PDA Security Tools **17**

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Personal Digital Assistants (PDAs) have been steadily increasing in numbers since their inception in the early 1990s. Explosive growth in their numbers, particularly within the enterprise, is expected during the next three years. This presents a number of management challenges, both operational and technical. This paper addresses the threat to information security posed by the PDA (including related devices such as "smartphones"). It discusses the drivers behind the PDA's increasing numbers and the changing nature of PDA use. The changing threat profile of the PDA is examined and specific threats and areas of weakness are explored in detail.

Methods for securing PDA's within an organisation, including management approaches and technical measures are considered. Finally, the opportunities which the PDA may present to security management are also examined.

This paper assumes that the reader has a basic understanding of IT security and PDA technology, but in-depth technical understanding of the issues discussed is not required.

The Evolution of The PDA

The PDA has evolved from being a device of very limited function, compatibility and capacity to being a highly functional extension of users' desktop environments. Capacity, connection options and processing power have all increased dramatically, while the applications and uses for PDAs are becoming increasingly complex. At the same time, decreasing prices and the increasing proliferation of multifunction devices such as "smartphones" are both helping to fuel the rapid proliferation of PDAs.

As they become more capable and affordable, and wireless networking options extend the reach of the corporate network to include them, PDAs are increasingly considered for use as an enterprise tool. The implications for their management and security are coming under scrutiny as a result. However, PDAs are already present in large numbers in many organisations.

Sales of PDAs are expected to increase threefold by 2006, compared to 2002 figures. Driven by their advantages for deploying enterprise applications, Pocket PC PDAs (those using Microsoft's Pocket PC operating system) will account for at least 50% of sales in the enterprise.[1]

A recent survey conducted by Novell Inc. among readers of its web site and printed publications, found that over a quarter of employees in the sampled companies already carry a PDA today. Most have more than 10 applications installed.[2]

Evidently, PDAs are already here in numbers. As their numbers increase and their uses diversify further, the impact of failing to address their associated security threat will only grow.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Organisations' Attitude To The PDA

In most organisations PDAs have been poorly managed, if they have been acknowledged at all. PDAs are most often bought and owned by individual staff members who connect them to their desktop PCs and install the software which was bundled with the unit.

This "back door" characteristic of PDAs creates a poor environment for securing them and for mitigating their security impact on the organisations into which they are introduced. For the IT professional, highlighting the security implications of PDAs draws attention to other management aspects of the devices – such as user support and software control – which organisations are often poorly positioned to address. Thus, organisational inertia often makes it difficult to get management buy-in to addressing the security threat posed by PDAs.

Widespread failure to properly address the PDA as an element of the organisation's IT environment has resulted in a proliferation of network-connected devices whose organisational cost and security implications are poorly recognised. However, as the PDA's penetration into the enterprise increases and the nature of their use and ownership changes, the necessity of properly managing them as an IT element is being more widely recognised.

Snapshot of the PDA

PDAs currently used within organisations often share characteristics which are increasingly being recognised by the organisation as unsatisfactory:

- More than 80% of PDAs are introduced into the organisation by the end-user.[3] This is the main reason that they have been allowed to proliferate without formal management for so long – many organisations have found it convenient to regard them as a zero-cost item.
- Support for PDAs is often minimal and informal. Few IT departments support PDAs with formal service levels or processes. Instead support for these devices is often "best efforts" or, more often, provided by colleagues supporting each other – "shadow support". Again, the productivity and cost implications of this support have been largely ignored, even by organisations which use TCO models to determine the cost of their IT operation. Support from the IT department is often limited to creating exceptions for "standard builds" so that desktop synchronisation software may be installed. The numbers, uses and security implications of these PDAs are therefore largely invisible to the organisation.
- Security considerations are for the most part ignored by PDA users, who regard their PDA as a personal tool, outside the purview of the organisation. Little thought is given to keeping their PDAs and the information on them secure. Most PDAs have limited (and often clumsy) security "out of the box" – securing them more effectively incurs extra cost which users have little incentive to pay.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Drivers For Change

The organisation's attitude to PDAs is changing, and the management challenge which they present is being recognised. This is being driven by a number of factors:

- The uptake of PDAs is increasing as costs decrease. Penetration rates are expected to reach 50% of all knowledge workers by 2006.[4] The scale of their use means that PDAs can no longer be ignored.
- Wireless connectivity options are increasing the profile of PDAs within organisations. The security challenges posed by wireless networks are widely publicised and the implications for PDAs and other devices connected by wireless networks are becoming better understood on the back of this publicity.
- As the capability of PDAs increases, they are more often being used to deploy enterprise applications. Tactical "mobile application server" packages are giving way to extensions from core application vendors and middleware from heavyweights such as Microsoft (the .Net framework). The provision of access to the organisation's "crown jewels" in this way means that the proper management of PDA security is becoming unavoidable.
- Largely influenced by the previous three factors, organisations, rather than individuals, will increasingly be responsible for the purchase of PDAs. By 2006/7 25-30% of PDAs deployed in the enterprise are expected to be purchased by the enterprise.[2] These PDAs cannot be considered "zero-cost" items and will attract more attention from management as their purchase and TCO is controlled by business-cases or purchasing processes.

Increasingly, the PDA is becoming an integrated business asset, and the organisation's expectation is that it will be managed and secured appropriately by the IT department. Understanding the security implications of the PDA, and developing appropriate organisational and technical measures to address this threat, has never been so important, or timely.

The Changing Threat Profile of The PDA

As the capability and compatibility of PDAs increase, the uses to which they are put is changing. We are also witnessing a bifurcation in the types of PDA – high-end devices, largely based on the Pocket PC standard are being increasingly used to deploy enterprise applications, while commodity devices with a relatively short life-cycle are being used for traditional PDA (Personal Information Manager - PIM) functions.[3] All of these functions have different levels of threat associated with them:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

PIM Functions

These are the cornerstone of PDA functionality, and are provided by core software (usually preinstalled), and supported by bundled, desktop software. They typically include:

- Address book
- Calendar
- Notes
- To-Do lists

The impact of information stored in these applications being compromised is usually considered as being low, as they are neither mission critical, nor commonly used to store large amounts of information. However, PIM information would often be extremely advantageous in conducting a social engineering attack (see *Social Engineering,* below). The threat from PIM-type information falling into the wrong hands cannot be ignored.

Communications

Commonly, the first applications which are installed to augment the PDA's core functionality are communications applications. Most PDAs come bundled with at least some communication applications, and this is one of the most popular categories of add-on application (after games) for PDAs. Note that communication applications do not necessarily imply the use or either wired or wireless networking – most communications applications are able to work via synchronisation mechanisms.

The most common communications applications are:

- E-mail
- Web browsers

Information stored in communications applications is often sensitive. Many users carry a copy of their entire email inbox with them. Corporate intranets are increasingly cached on PDAs inside "offline" Web browsers, such as AvantGo.[5] Such information, as well as being a valuable target in itself, can be a goldmine of information for those wishing to penetrate an organisation's security. Further, if a PDA falls into hostile hands it is often very easy to use the device itself to impersonate its owner by sending email or using stored login information to access Web-based applications.

Desktop-Compatible Applications

Increasingly, PDA versions of popular desktop applications, or PDA applications which are compatible with desktop file formats are becoming popular as PDA capacity increases. The upsurge in Pocket PC devices is accelerating the use of these applications, based largely on the popularity of applications such as Pocket Word and Pocket Excel. The increasing capability of similar third-party applications for other PDA platforms, such as Dataviz's *Documents To Go*[6], and viewers for other file types such as PDF and database formats, contribute further to the rate of adoption of these applications.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The combination of easy-to-use, highly-compatible applications and large storage capacity encourages users to store all manner of documents on their PDAs. It is even feasible to use these applications to create and edit documents.
The threat here is obvious. More portable and more easily misplaced, hidden or stolen than laptops, and usually with only minimal security protection (if any), PDAs are now being used to transport, create and edit documents of all types and security classifications.
Additionally, the ability to view documents in common, proprietary file formats means that users are more often including attachments when using communications applications – especially email. This exacerbates the threat presented by PDA communications applications.

Vertical Applications
Vertical, function-specific applications comprise the majority of applications installed on PDAs. Most PDAs have at least ten applications installed, and significant numbers have between 30 and 50 applications installed.[2] These tend to be very specifically aimed at one function or interest. Examples include:

- Games
- Special interest calculators
- Special interest knowledgebases
- Vertical application databases

These offer varying levels and types of threats. Of special note is the increasing use of applications designed specifically to store passwords, account details and other authentication information which users often have trouble tracking. The conglomeration of this sort of information is a threat in itself and is often compounded by weak encryption protection (if there is any encryption at all). A PDA falling into hostile hands is open to unfettered brute-force attacks on encrypted information, usually with no secondary alerting or prevention mechanisms to slow down the attack.

Enterprise Applications
The deployment of enterprise applications on PDA devices is accelerating. Most existing applications of this sort are deployed using tactical "portal" type software, often known as mobile application servers. However support for PDA delivery of their applications is emerging from core application providers such as SAP, Oracle, PeopleSoft, IBM and Siebel.[3] Development tools and frameworks are rapidly evolving to support seamlessly PDAs as a delivery platform, particularly using Microsoft's Pocket PC platform and .Net framework.
Although these applications potentially offer access to an organisation's most sensitive information and processes, the security of enterprise applications is usually the best managed of all PDA applications. This stems directly from the more planned and less chaotic deployment of such applications by the IT department. That said, the threat from enterprise applications on PDAs is real. The threat vectors here include the security of cached information on the device, and the potential to circumvent authentication when accessing core systems. Enterprise applications as well as the use of thin-client technologies such as

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Windows Terminal Server and Citrix on PDAs are also a major driver of wireless access, with its associated security challenges.

The Nature of The Threat

The security challenge presented by PDAs has many aspects. The specific characteristics of the PDA which make it vulnerable to attack, or a vector for attack on other systems are examined below.

Portability Is A Threat

The very portability which makes the PDA so useful and attractive to its users threatens security. It increases the PDA's vulnerability to theft or loss and makes it a highly portable tool for circumventing security from within an organisation. Gartner tell us: "Approximately 250,000 handheld devices were left behind or lost in U.S. airports in 2001."[7] Most of those devices probably contained information useful in conducting a social engineering attack. Many of them will have contained information sensitive in its own right. Few of these losses are likely to have resulted in preventative security action, such as changing passwords or even cancelling credit cards.

Poor Native Security Mechanisms

Although most PDA devices have some form of power-on user authentication, these mechanisms are often weak. Weaknesses include:

- Poor encryption of passwords (notably using reversible encryption) leading to ready availability of password cracking programs (e.g. Palmcrypt[8]).
- Password mechanisms which can be circumvented altogether (e.g. synchronisation "overwrite" settings).
- A lack of mechanisms to prevent the use of trivial passwords.
- Encryption mechanisms which are not accessible to the end user.[9]

Where further security mechanisms are available, they are often so cumbersome to use that very few users persevere with them. Palm's "Private Record" mechanism typifies such available, yet poorly understood and difficult to use tools.

Unencrypted Storage

By default, information on PDA's is stored in unencrypted form (although proprietary file formats often mean information is not stored in clear-text). It is certainly fair to say that the overwhelming majority of information stored on PDAs is currently unencrypted.

Encrypted storage options and applications which can store their data in encrypted form are available as add-ons for most PDA platforms, but as these are an added cost only the most security-conscious users opt to use and pay for them.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Stored Credentials

User credentials are often stored in PDAs. These are rarely subject to any level of protection other than that of the PDA itself, which as we have already seen is often minimal. Thus, by gaining possession of a user's PDA, or the information therein, an attacker may immediately have access to other systems and networks.

In many cases, the attacker need not even make an attempt to extract and read the credentials. For example, credentials to access email accounts are often stored in, and passed from, the PDA in a completely transparent manner. The opportunities for social engineering and information warfare, and for the exposure of potentially sensitive information, presented by unfettered access to another's email account, even for a limited time, are a serious security threat. When coupled with the compounding effect of wireless networking, stored credentials of this type constitute a highly effective and difficult to detect attack vector.

PDA applications are often used to store username and password pairs and other secret information. Applications which offer some level of cryptographic protection for this information are available, although much of it is stored in unencrypted notes and documents. Even with encryption, the possibility of the entire device being stolen and allowing the attacker free reign to conduct brute force attacks is a serious risk.

Access to large amounts of private information is also extremely useful in identity theft, which is a rapidly growing problem, especially in the USA where 117,210 incidents were *reported* to the FTC in 2001.[10] An estimated 700,000 to 1,100,000 *total* incidents occurred in the same period.[11]

Malicious Software

Most organisations today are fully aware of the threat posed by viruses, trojans and other malicious software. Effective measures are widely deployed to prevent such software from reaching systems using well understood vectors such as email and floppy disks.

The PDA can also be a vector for attack from malicious software. PDA's commonly have 16-64MB of capacity to store information, including software and documents which might contain macros or other executable code, all of which are susceptible to viruses. Some of this storage may be even presented as a "virtual disk" allowing "drag and drop" file operations between the PDA and a desktop or laptop PC. Storage can also be augmented by expansion options which dramatically increase the capacity of the PDA. The popular CF format has recently reached capacities of 4GB[12] – more than many laptop and desktop computers in use today.

Viruses and other malicious software which attack the PDA itself are beginning to emerge and can be expected to proliferate as the PDA platform continues to become more compatible with, and connected to more common target systems. Cross-platform viruses which can infect both PDAs and other systems have been postulated by anti-virus vendors (although not yet seen "in the wild"). However, attacks on smart-phones using malicious scripts delivered over SMS have already occurred.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Social Engineering

A compromised or stolen PDA may contain a wealth of information useful in social engineering attacks or identity theft. In addition to the possibility of gaining access to user credentials (see above), PDAs often contain large amounts of other information, often of a personal nature, which can be used to assist in impersonating its owner or even other people. Information such as addresses, phone numbers, nicknames, pets' names, birthdays and children's names may appear innocuous at first, but can be used to great effect in establishing trust when assuming someone else's identity. These data may also contain the answers to questions used to verify identity when, for instance, requesting that a password be reset. This is especially true of public, web-based commercial services such as eBay and Amazon.com.

Malicious Use

The portability, versatility and connectivity of the PDA make it a tool for malicious users. Gartner comment: "The PDA's small size also makes it an ideal tool for corporate espionage, data theft and fraud, where files can be transferred to the devices from desktops and taken away quickly and unnoticed."[7]

The increasing capacity and speed of these PDAs mean that they can appear innocuous whilst being used to attack an organisation's security:

- As a storage device, PDAs increasingly have the capacity to transport vast amounts of information into and out of an organisation, bypassing security mechanisms such as locked-down PCs and Internet usage monitoring.
- Increasing "horsepower" makes the PDA a more and more feasible platform for limited password and encryption attacks. While probably underpowered for brute-force attacks, the PDA is still capable of dictionary attacks and attacks on known weaknesses in encryption algorithms.
- Wireless connectivity, portability and easy concealment make the PDA the perfect tool to attack wireless networks. The sight of "warchalkers" openly operating with a PDA in one hand and a stick of chalk in the other has become commonplace in such cities as London.

Wireless Threats

A full discussion of the threats from, and weaknesses within, wireless communications is beyond the scope of this document. It should be noted, however, that PDAs often make use of 802.11b ad-hoc mode wireless networking. This is a peer-to-peer implementation of the 802.11b standard for wireless LANs and allows devices to communicate without using a central access point. An insecure network can therefore be established with no control over, or visibility of, its security, and in fact with nobody else having any knowledge of its existence. Devices can enter and leave the network easily, as ad-hoc networks offer very limited control over authentication management.

Although any 802.11b-capable device can create or join an ad-hoc network, non-PDA devices usually operate in Infrastructure Mode. Infrastructure Mode allows

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

control over authentication and encryption via the central access point at the core of the wireless network.

Organisational Remedies To Secure PDAs

As with many aspects of security, the approach to securing PDAs within an organisation is multi-faceted, and part of a greater management challenge. Senior Management must provide policy which determines the use support, management, and security acceptable for PDA devices within the organisation. The IT department must determine guidelines for their use and deployment and provide supporting infrastructure for their management and for the management of their security.

PDA Policy

> "With the increasing penetration into the enterprise of personal digital assistants (PDAs), companies must establish firm guidelines for the appropriate utilization of devices, especially regarding business-sensitive data. Ownership, appropriate use, synchronization, and support limits must be defined."[1]

This quote from Meta Group in 2002 demonstrates that the importance of properly managing PDAs is gaining greater acceptance within the industry as a whole. As organisations begin to purchase PDAs in quantity, deploy enterprise applications to PDAs, and build wireless networks to support them, the necessity of including PDAs within proper management and support structures cannot be ignored.

From a security point of view, this presents a window of opportunity to ensure that appropriate consideration is given to the security implications of PDAs while policy is being formulated.

Purchasing Control and Standardisation

Legitimising PDAs within the organisation provides the opportunity to standardise procedures for their purchase / reimbursement and for gaining permission to connect them in the first place. It also provides the vehicle to enforce "standard build" tactics to gain at least partial control over what applications and hardware are allowed. These have implications for many aspects of PDA management, but especially security as the installation of systems management and security management software can be enforced at this point.

Standardisation also may include replacing many instances of desktop-based synchronisation software with network-based alternatives, which allow centralised management of settings controlling such parameters as password strength and email attachments.

Support Mechanisms

Formalising support for PDAs increases their visibility to the IT department, and exposes the costs of supporting them by replacing "shadow support" with more measurable support systems. These costs can be used to justify the deployment

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

of systems management and security management solutions. Increased visibility also allows the IT department to be alerted to applications and practices with potential security ramifications.

Development and Application Guidelines
Guidelines governing acceptable security standards to which applications installed on PDAs must comply, and to which developers building applications for deployment on PDAs must adhere, can be used to provide control over encryption and persistence of information. Authentication standards for applications should also be managed closely, particularly where distributed application architectures are used – digital signatures should be provided for application components.

Technical Remedies And Tools To Secure PDAs

A variety of technical measures are available to help manage the security of PDAs. These are categorised and discussed below. Some products have features from more than one category. A chart of some common tools and the categories they fall into is appended to this document.

Authentication and Access Tools
These tools are used to provide stronger user authentication (i.e. power-on login) and increase the granularity of security within the PDA and between different users.
Common features:

- Centralised administration of password (or other authentication mechanism) rules.
- Countermeasures against common attacks which circumvent PDA password security.
- Support for multiple users with individually controlled access levels.
- The ability to lock the PDA or wipe its contents after repeated, unsuccessful attempts to access it.
- One-way hash algorithms to ensure secure storage of passwords.

Biometrics
The Biometric Consortium defines biometrics thus: "Biometrics are automated methods of recognizing a person based on a physiological or behavioural characteristic. Among the features measured are; face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice."[13]
Biometric devices are rapidly gaining acceptance as an authentication mechanism to establish a user's identity. Recently we have even seen biometric iris scanners being used at major airports to establish the identity of frequent travellers.
Biometric identification is beginning to be used with PDAs to control access. Solutions are available to establish a user's identity based on signature

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

recognition, voice recognition and, increasingly, fingerprint recognition. Until recently, fingerprint recognition was available only as an aftermarket addition, but the first PDAs with inbuilt fingerprint scanners are beginning to reach market.

Encryption Tools and Applications

These provide the ability for the user to encrypt specific information or to encrypt the entire contents of the PDA. Contrary to common understanding, the encryption libraries supplied by Microsoft on the Pocket PC platform, and by Palm on the new PalmOS 5 platform are not directly available to the end user, so additional software is needed.[9] Common features of PDA encryption tools include:

- Selectable encryption algorithms and strengths
- Selectable key lengths
- Control over persistence of encryption keys
- File-by-file or wholesale encryption
- Transparent, on-the-fly encryption/decryption

Antivirus Tools

Antivirus vendors have been quick to extend their product lines to include protection for PDAs. At least two viruses and one trojan which target PDAs (specifically the Palm platform) have been found "in the wild".[14]

There are four common transmission methods by which a virus (or other malicious software) could infect a PDA:

- Through infected e-mail when using a PDA over a wired or wireless Internet connection
- When syncing with an infected PC
- Via an infected file transferred from another PDA via infrared (IR)
- By downloading infected files from the Internet

Although software is now available from all most antivirus vendors to protect PDAs against infection, not all anti-virus software protects against all these vectors. No single solution protects against viruses on all PDA platforms. Software which examines files being transferred during a synchronization or virtual disk access can also protect against viruses which attack other platforms being transferred via a PDA.

Integrated Security Tools and Policy Tools

PDA security suites which conglomerate many different technical remedies to parts of the PDA security challenge are beginning to appear on the market. These are often early versions and are sometimes created by acquisition of various modules and components. As a result, the level of integration within these suites is sometimes not to the same standard we expect from similar products in other fields. That said, integrated PDA security suites are maturing rapidly and market leaders are emerging.

Integrated security suites include such features as:

- Centralised enforcement of policies and configuration
- "Push" updates to multiple devices.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Incident alerting and logging
- Tools for installation across large numbers of PDAs

Systems Management Software
Major systems management vendors are moving quickly to include PDAs in the scope of their products. Most vendors now include at least some functionality to manage PDAs when they connect to enterprise networks, although cross-platform (PDA platform) support is patchy and functionality is not as comprehensive as with support for other devices such as desktop PCs. Rapid progress is being made in this area with vendors now beginning to offer more fully integrated PDA support.
One of the challenges facing centralised management of PDAs is the varied and often unreliable nature of the ways in which they connect to the organisation's network. With devices using a mixture of cradle, infra-red and differing wireless networks, reliably establishing a connection of sufficient speed and duration to effect software updates, for instance, can be difficult.
However, functions such as configuration management, remote software installation and network backup for PDAs are becoming commonplace among systems management products.
Note that these products do not enhance the level of security protection technology available on PDAs, but they can ensure that the protection which is available is used to best effect.

VPN Software
In order to counteract the well-documented weaknesses of many forms of wireless communication (and especially 802.11b networks), many VPN vendors are releasing client software to allow wireless PDA communications to be secured using encrypted VPNs.
By encrypting wireless traffic in proven VPN technology, the risk from some of the vulnerabilities in wireless networks can be mitigated. In particular, weaknesses in encryption, authorisation and authentication mechanisms are bolstered by the use of VPNs.[15]

The PDA as a Security Tool

In considering the security profile of the PDA, its potential advantages as a security tool cannot be ignored. If PDAs can be properly secured and managed there is considerable scope to make them part of the organisation's overall security strategy.
Unsecured documents stored on a PDA are a risk to security. However, when properly protected, documents stored on PDAs are a much better option than the most common form solution for document portability – paper. PDA storage, protected using strong authentication, strong encryption, and other measures such as "logic bombs" to guard against repeated access attempts, can provide very portable transport and viewing for documents.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

If users are already carrying PDAs, they make an excellent platform to deploy software versions of two-factor authentication systems. PDAs can be used to rapidly increase acceptance and penetration of such strong authentication mechanisms because users are not required to carry a new device, and because the interface they use to generate access keys is familiar to them. At the same time, the cost to deploy is far lower than using hardware authenticators. Software versions of leading products in this field are already available in PDA-compatible versions, such as RSA's SecurID For Pocket PC.[16]

Similarly, PDAs equipped with biometric authentication mechanisms can also be used to increase user authentication standards elsewhere in the organisation. PDAs also provide a method for securing and storing encryption keys and certificates. There is no better way of ensuring the identity of a public key's owner than being given the key in person.

As PDAs increase in capacity, they are increasingly viable as a highly portable platform for common security tools, such as port scanners and host fingerprinting tools. Some authors of these tools are already producing PDA versions, especially for the Pocket PC. A large range of tools specifically aimed at wireless networks is already available.[17]

Future Trends

As the PDA evolves it is becoming more capable, more connected and more difficult to distinguish from other devices. The convergence of the PDA and the mobile telephone is already well advanced and shows no sign of slowing. This convergence is broadening, as the functions of other devices are included in PDAs. The lines between the PDA, telephone, MP3 player, USB disk, GPS receiver, remote control and even car keys are blurring as vendors strive to create the "Personal Information Appliance". We are even seeing the emergence of wearable computers.

This suggests that increasingly, we will be carrying (or wearing) and using computerised devices of ever growing power, and flexibility. Their use will be multifaceted, affecting our personal and professional lives, providing entertainment and information, communication and storage. The difference between organisations' IT environments and their users' personal tools will become increasingly semantic. Security measures, both technical and organisational, will need to be adaptable to both environments and flexible enough to address many different flavours of device and many different functions.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

The threat profile of PDAs is growing, driven by their increasing capability and connectivity as well as their accelerating proliferation and convergence with other devices.

As PDAs increase in capability, the nature of their use and ownership within organisations is changing. Once, these devices were limited to maintaining calendars and contact lists, now they provide a highly functional and versatile platform which can even be used to deploy enterprise applications.

The security threat posed by PDAs mirrors their growing usefulness. PDA's are becoming highly connectable and capable devices. Their in-built security mechanisms remain inherently weak and their very portability and the nature of their use provide additional security challenges.

Organisations are recognising the security implications of PDAs and are increasingly aware of the different threats posed by these devices.[18] The current focus on wireless network security and the increased general awareness of security in the wake of the events of September 11, 2001, is providing organisational impetus to address these implications.

Organisations today must face the challenge presented by PDAs and address the management and security problems they pose. Organisations can no longer turn a blind eye to the proliferation of PDAs nor to the need to properly manage and secure them.

Effective management of PDA security must begin with policies and processes. The organisation's commitment to managing the PDAs within its environment must be clear and unequivocal.

With proper organisational mandate (and budget), a variety of technical tools are available to assist the IT department in managing and securing PDAs. It is unlikely (at this stage) that a single vendor can provide all the tools necessary to properly secure an organisations' PDAs – a combination of tactical solutions will be needed to augment broader offerings from systems management vendors.

Properly recognised and secured, the PDA can be an integral part of an organisation's security framework, providing user-friendly ways of securely transporting documents and a vehicle to increase acceptance and deployment of security tools.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

[1] Gold, Jack. "Enterprise PDA Policy: Part 2". Meta Group Delta 1078 (13 January, 2002)

[2] "Getting A Handle On Handhelds". Novell ZENworks Cool Solutions. 27 February, 2003. URL: http://www.novell.com/coolsolutions/zenworks/features/a_handhelds_part1_zw.html

[3] Gold, Jack. "PDA TCO: How Much?". Meta Group Delta 1165 (20 August, 2002)

[4] Gold, Jack. "Enterprise PDA Policy: Part 1". Meta Group Delta 1077 (13 January, 2002)

[5] "AvantGo M-Business Server Web Edition Datasheet". AvantGo Inc. 13 May, 2002 URL: http://avantgo.com/products/pdfs/mbus_server_web_datasheet.pdf

[6] Mossberg, Walther S. "Office Documents Look Better On Palms Than on Pocket PCs". The Wall Street Journal. 6 February 2003. URL: http://ptech.wsj.com/archive/ptech-20030206.html

[7] Wiggins, D; Simpson, R; McHugh, D. "What Does Trustworthy Computing Mean For Pocket PC?". Gartner Inc. Research Note (27 August, 2002).

[8] "PalmOS Password Retrieval and Decoding (A092600-1)". @stake Inc. 26 September 2000. URL: http://www.atstake.com/research/advisories/2000/a092600-1.txt

[9] Richardson, Robert. "Slipping Through Your Fingers". Computer Security Institute ALERT November & December, 2002.

[10] "Figures and Trends On Identity Theft, January 2001 Through December 2001". Federal Trade Commission (August 7, 2001).

[11] "Facts and Statistics". Identity Theft Resource Center. May 2002. URL: http://www.idtheftcenter.org/html/facts_and_statistics.htm

[12] "SanDisk Introduces Four Gigabyte CompactFlash Card, World's Highest Capacity CF Flash Memory Card". SanDisk Corporation, March 13, 2003 URL: http://www.sandisk.com/pressrelease/031303_cf4GB.htm

[13] "An Introduction To Biometrics". The Biometric Consortium. URL: http://www.biometrics.org/html/introduction.html

[14] Cardoza, Patricia. "Block PDA Viruses" ZDNet. April 25, 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2862764,00.html

[15] "Wireless LANs, Risks and Defenses". Airdefense Inc. August 2002. URL (via form): http://www.airdefense.net/whitepapers/rd_request2.php4

[16] "SecurID For Pocket PC". RSA Security Inc. 2003. URL: http://www.rsasecurity.com/products/securid/techspecs/pocketpc.html

[17] "Wireless LAN Analyzers: The Ultimate Hacking Tools?". NetworkMagazine.com. March 5, 2003. URL: http://www.networkmagazine.com/article/NMG20030305S0001

[18] Hudson, Sally; Burden, Kevin; Raschke, Thomas. "Corporate Concerns for PDA Security". IDC Bulletin #26657. (March 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix A
Selected PDA Security Tools

Product Name	Manufacturer	Authentication and Accesws	Biometrics	Encryption	Antivuris	Integrated Tools	Systems Management	VPN	PalmOS	Pocket PC	Other PDA O/S
Restrictor	ISComplete www.iscomplete.org	●							●		
SafeguardPDA	Utimaco www.utimaco.com	●		●		●				●	
Sentry 2020	Softwinter www.softwinter.com			●						●	
PDA Defense	PDA Defense www.pdadefense.com	●		●		●			●	●	●
PDA Secure	Trust Digital www.trustdigital.com	●		●		●			●	●	●
PDA Lok	PDA Lok www.pdalok.com		●						●	●	
PDA Secure VPN	Trust Digital www.trustdigital.com					●		●	●	●	●
VPN1 – SecureClient	Checkpoint www.checkpoint.com							●		●	
Trusted Mobility	Trust Digital www.trustdigital.com	●		●		●		●	●	●	●
TealLock	Teal Software www.tealpoint.com	●		●		●			●		
iPAQ h5455	Hewlett-Packard www.hp.com		●							●	
VirusScan Wireless	McAfee (NAI) www.mcaffee.com				●				●	●	●
ZENworks For Handhelds	Novell Inc. www.novell.com	●				●	●		●	●	●
eTrust Antivirus	Computer Associates www.ca.com				●				●	●	
Unicenter TNG	Computer Associates www.ca.com				●		●		●	●	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 28th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

FOR578 Cyber Threat Intelligence	**Tysons Corner, VAUS**	**Aug 31, 2015 - Sep 04, 2015**	**Live Event**
SANS Milan 2015	**Milan, IT**	**Sep 07, 2015 - Sep 12, 2015**	**Live Event**
SANS Crystal City 2015	**Crystal City, VAUS**	**Sep 08, 2015 - Sep 13, 2015**	**Live Event**
SANS Network Security 2015	**Las Vegas, NVUS**	**Sep 12, 2015 - Sep 21, 2015**	**Live Event**
SANS Seoul 2015	**Seoul, KR**	**Sep 14, 2015 - Sep 19, 2015**	**Live Event**
SANS Baltimore 2015	**Baltimore, MDUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
Data Breach Investigation Summit & Training	**Dallas, TXUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Perth 2015	**Perth, AU**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Tallinn 2015	**Tallinn, EE**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS ICS Amsterdam 2015	**Amsterdam, NL**	**Sep 22, 2015 - Sep 28, 2015**	**Live Event**
SANS Bangalore 2015	**Bangalore, IN**	**Sep 28, 2015 - Oct 17, 2015**	**Live Event**
SANS DFIR Prague 2015	**Prague, CZ**	**Oct 05, 2015 - Oct 17, 2015**	**Live Event**
SANS Seattle 2015	**Seattle, WAUS**	**Oct 05, 2015 - Oct 10, 2015**	**Live Event**
SOS: SANS October Singapore 2015	**Singapore, SG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
GridSecCon 2015	**Philadelphia, PAUS**	**Oct 13, 2015 - Oct 13, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS Chicago 2015	**OnlineILUS**	**Aug 30, 2015 - Sep 04, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**