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.

PDAs in the Corporate Environment

A Personal Digital Assistant (PDA) is a handheld device that combines computing, telephone/fax, and networking features. PDA size and portability makes them easy targets for thieves and they are easily misplaced or lost. As the use of PDAs in the workplace increases, companies are beginning to recognize the need to protect their most sensitive corporate data and business applications, which may be contained on the PDA in the event it is compromised, lost or stolen. PDA security, therefore, should be a serious concern f...

Copyright SANS Institute

Author Retains Full Rights

AD

By Dave Croxton
Version 1.2f

PDAs in the Corporate Environment

Overview

A Personal Digital Assistant (PDA) is a handheld device that combines computing, telephone/fax, and networking features. PDA size and portability makes them easy targets for thieves and they are easily misplaced or lost. As the use of PDAs in the workplace increases, companies are beginning to recognize the need to protect their most sensitive corporate data and business applications, which may be contained on the PDA in the event it is compromised, lost or stolen. PDA security, therefore, should be a serious concern for every individual and corporate handheld device user.

Although there are many different manufacturers of the PDA, most base their PDA on one of the two major Operating Systems ("OS"): Palm or the Windows CE ("Pocket PC"). Each company manufactures several models of the PDA and the capabilities of each model vary. The security concerns of the PDA remain no matter the manufacturer or model. Accordingly, this paper will be limited these two Operating Systems.

Palm OS

The use of the Palm OS has grown over time to become a widely accepted platform for the PDA. There are many manufacturers (i.e., Palm Pilot, Sony and Handspring Visor) who have adopted the Palm OS for their systems. Additionally, due to its popularity, our corporate environment has seen more of the Palm OS than the Pocket PC. Palm offers wireless Internet connectivity built into the Palm VII and, through the use of external wireless modems offered as add-ons for other models. Each of the other manufactures has similar models. Although some users purchased these wireless systems, most of our corporate users did not find the web clipping service to be a necessity for daily business.

MS Windows CE – Pocket PC OS

As the popularity of the PDA increases, many corporate professionals are turning to the Windows CE based Pocket PC. Major Manufacturers utilizing the Pocket PC OS are Compaq, Hewlett Packard and Casio. Often considered by many in the work force, as a tool, rather than a calendar and address book, users are turning to the application compatible Pocket PC based PDA. Microsoft Pocket Word/Excel/Outlook applications offer similar features and functionality to their desktop counterparts. Printing of Office documents can be accomplished by beaming (add-in product usually required) documents, spreadsheets and email directly to an Infrared (IR) equipped/enabled printer. No longer are you required to "plug-in" to transfer your data, receive your email or share your calendar, you can purchase an add-in product such as PrintPocketCE [(1)].

Portability Issues

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

As we begin to look at the portability issues related to desktop type applications, we realize that more information can be packed into these small devices and carried in a shirt/coat pocket, rather than a brief case. Much like a laptop in data storage capacities through the use of expansion slot memory cards, the increasing use of a PDA has given rise to new security issues. Some of those concerns include determining how policies and procedures should be written in order to address the data security. More importantly, once the policies and procedures are in place regarding such a portable device, consideration should be given to determine how those policies and procedures will be implemented and monitored.

Policies, Standards and Procedures

As outlined in the *Computer Security Handbook*, policies are broad statements of your company's management views of a specific topic. Standards are mandatory activities, actions, rules or regulations designed to provide the policies with the support, structure and specific direction they require to be meaningful and effective. Procedures spell out the specifics of how the policy and supportive standards will actually be implemented.

Senior management should agree with and approve the company's policy on the use of PDAs. As a security professional, you may be called upon to provide risk information related to the security of your company's data. Risk factors should consider the type of data that is to be secured and the threats actual or perceived against that data. Other issues would be the cost to the company if its sensitive data were deliberately or accidentally exposed, changed or deleted? The risk must be assessed and the proper, cost effective precautions taken to protect the data.

Obviously, different policies and standards would apply to a company supplying the PDA to employees, as opposed to the PDA being purchased by an individual for use with company information. Front line managers seeking to increase productivity and revenues view the PDA as an efficient tool to communicate changes to staff meetings, client appointments and client sales opportunities. However, the computer support and information security departments view these security issues as huge challenges for which adequate support must be provided and, at the same time, privacy and security of sensitive data must be maintained. Deciding on which device to support and allow within your company is an ever-evolving process. Some companies allow any device but have strict Standards and guidelines on what they can be used for. Some companies do not allow them at all. Most companies face one of these decisions; buy and issue them, allow personally purchased devices to be used or to strictly ban their use within the company. Which decision your company makes about the use of PDAs needs to have effective Policies and Standards developed to address the issue.

Your Policies, Standards and Procedures should reflect the company's need to secure and protect sensitive data. Considerations should include the risk of exposure, and what poses that threat, loss, theft or simply the data being exposed to someone who doesn't have the need to know the information. Threats should be categorized by the likelihood of it happening, the severity of the threat and the consequences if it does happen. You should also consider what it would cost the company if the device were

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

lost or stolen and the data it contained was of a sensitive nature. The ability to synchronize email and documents to the PDA causes management to consider not only whether or not to allow it but how to control it, if PDAs are allowed in the company. Some company's have a 30 retention policy on email for pc storage but had to modify the policy, standards and procedures for PDA usage. This was because we could systematically remove email from the PC and servers but not the PDA. The modified policy, standards and procedures addressed the individual responsibility of each PDA user to ensure the company's 30 day retention policy was adhered to. Local scans of systems with attached PDA devices verify the standards and procedures are being followed.

Threats and Protection

Many of the aftermarket security programs researched regarding the Palm OS use 128-bit encryption algorithm, such as Top Secret [(2)]. Roughly speaking, 128-bit encryption is 309,485,009,821,345,068,724,781,056 times stronger than 40-bit encryption. Presently, 40-bit encryption is not considered "strong" security in the cryptographic community. However, even taking into account Moore's Law [(3),] which states that computing power doubles about every 18 months, 128-bit encryption represents a very strong method of encryption for the foreseeable future. Additionally, File Safe 2.2 [(4)] uses a 448-bit encryption key, the Blowfish algorithm, to encrypt your data. With Blowfish there are more possible keys to check than there are atoms in our galaxy. The approximate number of atoms in our galaxy = 2^{223} and the approximate possible keys using Blowfish = 2^{448}. Both applications and encryption s seem well suited to protect passwords, pin numbers, credit card numbers and other data on the device.

Information researched regarding the Windows CE/Pocket PC OS reveals that Pocket PCs have a similar choice of protective applications. A few of those applications, Sentry 2020/CE [(7)] which is also included in the Handango Security Suite – Pocket PC [(8)], and The Safe [(9)] utilize a 128-bit encryption algorithm used to secure data, lists of user passwords/account numbers, and different applications.

I have been successful (for demonstrations purposes only) in syncing my palm pilot using another users cradle connected to their pc and downloading their email to my handheld. This ability further supports the need to "lock" workstations when they are unattended. Similarly I was able to download data from another handheld device to my workstation using the "Sync" function. In both cases there was no password set for the device.

Unfortunately, a cursory search of web sites that offers security software also has links for programs or "cracks" that can be found for most of the freeware security applications. Examples of these are PCRACK 1.0 [(5)] and Sword I.D. [(6)] for the Palm OS Security Password.

Just a word of caution, you get what you pay for, don't scrimp on security. Passwords only prevent access to the data files they do not encrypt programs. You should consider testing several different encryption programs before making the decision on the one for your company. Some of them require huge amounts of memory

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

on the device and might limit the users ability store the data required.

Malicious Code

Another consideration for both the Palm and Windows based PDA is malicious code. Viruses, which have been directed towards the Palm OS, are PalmOS.Liberty.A, PalmOS.Phage.A, and PalmOS.Vapor A. To date my research has found no known viruses aimed at the Pocket PC. However, it is only a matter of time before someone will take the first step… While viruses are always an issue to data security, the PDA presents an avenue to infect the corporate network with viruses during sync operations. Also the ability to "beam" data to infrared ports on desktops, laptops can easily bypass the anti-virus software if not properly configured to scan during beaming connections. As with all electronic file transfers your anti-virus software must be able to scan, detect and prevent infection to be effective. There are many vendors for anti-virus software (see references for a partial listing) and your company should have a standard anti-virus software package in use. A policy on its use and configuration will help to ensure that it is installed and current. Often anti-virus software if installed is found to be out of date or not enabled. Our company purchases an enterprise license of the anti-virus software and makes it available for those who work at home. We also provide a version for the hand held devices to users. This ensures that the anti-virus software is current and compatible with our enterprise hardware/software configurations.

Recommendations

What's the point? Realizing that there will always be a division between complete security and the leading edge of technology, there must be a compromise. When new products are seen as an enhancement to producing revenue or streamlining business functions, managers will embrace the products and encourage their workforce to use those products. Companies will continue to do business and technological advances will always present challenges that will either enhance security or force security practices, policies, standards and procedures to be reconsidered.

Based on the foregoing, you may want to consider the following as a starting point for protecting company and customer information/data and business applications:

- Ensure you have effective and enforceable policies that clearly define the individual user's responsibilities. They should also include the purpose, objective and scope of the policy. These policies should address data classification and storage, company standards that address software and hardware configurations including the PDA. Once in place, these policies should be reviewed and updated at least annually, or whenever new technology/software is introduced into the company.
- Users of handheld devices must be educated in the best practices to protect these devices from theft and loss. PDA users must be trained and enlightened to be aware of their surroundings when using the device. The user must be cognizant of the data that is stored on the PDA and feel at ease to report lost or stolen devices. He or she must also be able to

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

provide an inventory of the data that was contained on the device to company security personnel so that appropriate action may be taken to reduce/prevent further loss. This is especially true when traveling. Never assume that everyone is aware of every security concern.

- The use of security software to encrypt or prevent access to data stored on the PDA, such as those mentioned above should be used to help protect the data. Frequent purging of data, which is no longer needed on the PDA, is a practice that can help minimize exposure if a device is lost or stolen.
- PDA desktop interface software should be tested in a non-production environment to ensure compatibility with enterprise standard hardware/software configurations. Companies should have a policy in place that identifies those persons who can install software to its computer systems. Change control will also help maintain an inventory of the software and versions in use at your company.
- Anti-virus software should be configured to scan files during sync and beaming operations. If possible updates to the anti-virus software should be pushed to the desktop. This will ensure the software is kept up to date and a consistent version is used throughout the company.
- Define the consequences for breaches of Policies, Standards and Procedures. Identify disciplinary actions based on the nature of the offense and clearly identify management's intent to enforce the Policy.
- Define reporting procedures for employees to follow if they discover a breach in security and list points of contact for the different areas of your company.

These are simply a few key points to consider and should not be looked at as a complete list. Each company has to determine the risks it faces by utilizing Personal Digital Assistants within its work place. One thing that I have realized is that you can't keep them out of a large company. Your company should develop a strong policy based on Industry Best Practices and define user accountability for protection your information.

Summary

A clear understanding of the challenges posed by all mobile devices to your particular environment provides a basis for the development of sound security policies, standard and practices. Remember, to date, there is no silver bullet that will cure all the woes of security professionals. Adopting a "defense in depth" strategy will allow you to recognize security issues hopefully before they become security problems. Encryption programs, anti-virus software, effective password use, training and awareness are all components of an effective security posture. Our real challenge is to make security easy to use and almost transparent to the end users. If users have the opportunity to change settings in order to accomplish their needs most often they will change the setting without considering the security implications involved. Therefore each employee should be educated and aware of the policies that govern data security while

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

embracing those policies as sensible and easy to use. If we do our job thoroughly and correctly, security should be second nature to everyone, rather than a burden or an after thought. Ongoing company training at all levels, from the mailroom to the CEO, will ensure that the best security practices can be effective and enforceable. Without senior management support your policies, standards and procedures will be disregarded and often not implemented.

We have simply scratched the surface, dealing only with high-level issues of the different operating systems of the two major palm type hand held devices. There are many other devices such as the Blackberry, two-way pagers and cellular phones with a built in PDA, and handheld PCs, all that can pose threats to data security. Most of the handheld devices have the capability to connect to the Internet with either an internal wireless modem or through add-on cards. These connections are usually configured by the manufacturer to allow a wide range of connections and do not necessarily address security. When I contacted one supplier, I was told, "Security is the responsibility of the individual end users organization because it may restrict the device from performing as advertised". Yes security is a concern of the wireless world, implementing it remains the issue of the companies using the devices. Wireless connections to LAN/WANS are also issues that need to be considered if your company allows such access. There are too many accessories to even begin to list and each of them is a potential security risk. As the software for PDAs continues to become more compatible with our desktops, we should consider their use as an extension of the desktop. Accordingly our policies and standards should reflect these peripherals. Our only hope is to stay abreast of the changes in technology that affects the company enterprise network and build policies and apply industry best practices to defend against the threat of data loss or compromise.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References:

Computer Security Handbook Third Edition – Authur E. Hutt, Seymour Bosworth, Douglas B. Hoyt. Wiley Press – Part 1; section 2 - Policies, Standards and Procedures.

Applied Cryptography Second Edition – Bruce Schneier – Wiley Press – Section 14-3

PC Tech Guide - Mobile Computing – PDAs
http://www.pctechguide.com/25mob3.htm

SANS Institute Resources – Model Security Policies
http://www.sans.org/newlook/resources/policies/policies.htm

Information Security Policy World
http://www.information-security-policies-and-standards.com/

Federal Computer Week - Pentagon scrutinizes handheld security
BY GEORGE I. SEFFERS 31 JULY 2000
http://www.fcw.com/fcw/articles/2000/0731/news-pda-07-31-00.asp

Vendor applications mentioned:

(1) PrintPocketCE - "http://www.fieldsoftware.com/PrintPocketCE.htm"
(2) Top Secret - "www.clicklite.com"
(3) Moore's Law - "http://www.intel.com/museum/25znniv/hof/moore.htm"
(4) File Safe 2.2 - "http://www.pointinception.com/product/?id=2"
(5) PCRACK 1.0 - "http://www.jkware.com/palm/palm.html#PC"
(6) Sword I.D. - "http://www.palmix.itil.com/newpalmix/products/sword_home.htm".
(7) Sentry 2020/CE - "http://www.softwinter.com/sentry_ce.html"
(8) Handango Security Suite – Pocket PC - "http://www.handango.com/PlatformProductDetail.jsp?siteId=1&platformId=2&productType=2&productId=14394&sectionId=0&catalog=30"
(9) The Safe - http://www.sbm.nu/englisch/windowsce/thesafe/docu/readme.htm

Anti-Virus companies providing PDA software (not all inclusive):

Computer Associates Inoculate*IT* – for Palm OS
http://www3.ca.com/Solutions/Product.asp?ID=171
McAfee – for Palm and Windows CE/Pocket PC
http://www.mcafeeb2b.com/products/virusscan-wireless/default.asp
F-Secure – for Palm and Windows CE/Pocket PC
http://palmtops.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.f-secure.com%2Fpalm%2F
Symantec – for Palm OS
http://www.symantec.com/sav/
Trend Micro – PC-cillin - for Palm and Windows CE/Pocket PC OS
http://www.antivirus.com/free_tools/wireless/

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: October 2nd, 2013

Upcoming SANS Training

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

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced