Personal Digital Assistants are convenient, but is your data safe?

Lindsey Street

East Carolina University

11/29/2005

Abstract

This paper looks at protecting PDA data from the consumer perspective by comparing five different third party security software packages for PDA's. After analyzing those, it looks at what the original operating system on the PDA does for security. Last, the paper looks at the business perspective of the PDA, and different theories on the famous convenience versus security question.

Is data on your Personal Digital Assistant safe?

As a consumer I was attracted to the personal digital assistant (PDA) because of its ability to travel with me at all times. But with that ability I was worried about the data I kept on my PDA, I then went on a hunt to find the best way to protect the data I put on my PDA. While looking for programs to protect my data, I discovered many different ways I could accomplish this. Today I will give an outline of my research on crypto-Sign, PDASecure, Pointsec, CREDANT Mobile Guardian and SafeGuard PDA. Then I will discuss the security already built into different operating systems on the market. Next I will show information I found on how IT departments feel about the new PDA craze and finally I will present several examples of how PDA's were used in real world applications and how they were secured in each instance.

Crypto-Sign is mostly used as a method of securing wireless transactions, but the same biometrics that ensure these transactions can also ensure encrypted files are only opened by the intended recipient or original owner of the file. Crypto-Signs biggest advantage is that it combines the benefits of a password with those of electronic signature verification to utilize the benefits of each (Crypto-sign, 2003). Crypto-Sign uses the biometrics of a persons signature to both record the final signature and any pauses or hard impressions that person makes with the pen as they write their signature. This makes your signature hard to duplicate even if that person has a copy of your signature (Crypto-sign, 2003). This signature can be used to verify the author of an e-mail or important document to allow a digital signature to be applied to an e-mail. This ensures the original author of an e-mail to the recipient. This can also be applied to encrypting and decrypting files. A person could put their signature as a password to open a certain file, for example one that contained all of their passwords, and only their signature could open that encrypted file.

"PDASecure uses encryption algorithms and password protection to protect all the vulnerabilities associated with a PDA." According to *Ferrill* (2002) who recently reviewed this product. PDASecure requires users to enter there password every time the PDA goes idle. Idle time for a PDA depends on what the users sets it to, this should be set to a short time for maximum security. While it might seem annoying to have to enter your password every time you want to take notes at a meeting, this is one of the features that makes PDASecure so secure. In addition to the password, PDASecure also supports up to a 128 bit encryption, which implemented to the "most secure level could take 90 seconds to decrypt an address book" *Ferrill* states. This will cause most users not to implement this to its most secure settings. PDASecure also allows the user to set the device up to lock after a certain number of incorrect password attempts and erase all data on the device (Ferrill, 2002). One more feature worth mentioning for this method is the users ability to set specific policies that dictate things such as, password length, time of day usage and application lockouts (Ferrill, 2002).

Pointsec makes data encryption, user authentication, and access control easy enough that anyone could use their PDA securely and not even realize it (Pointsec, 2003). The encryption provided by Pointsec is a 128-bit AES algorithm (Pointsec, 2003) that makes the encryption of all the data on the PDA transparent to the user (Garvey, 2005). Not only is all data stored on the internal flash of your PDA encrypted, but also all any data that you save on removable media, such as Secure Digital (SD) cards or compact Flash (CF) cards is encrypted as well. The Pointsec software also allows for user account lockouts if an incorrect password is entered more times then the central management allows on their equipment (Pointsec, 2003). The advantages of Pointsec are, when you forget your password, instead of having all of your data erased, you can call the help desk and they can reset your password for you. Additionally Pointsec has a new approach to passwords called PicturePIN. PicturePIN allows users to create a story in their heads from a selection of nine pictures, then every time their PDA locks itself, they just type in the four pictures that make up the story they have in their head. This makes passwords easier and more fun to remember.

CREDANT Mobile Guardian Shield (CMG Shield) is an encryption program that allows users to maintain there usual schedule, while the program encrypts everything behind the scenes and on the fly. CMG Shield is rule based, which means that only essential information is encrypted, this gets rid of all the problems associated with encrypting the whole disk (Next, 2005). The IT staff will be the judge of what essential information is and what is not (Next, 2005). CMG Shield offers a standard windows login screen for users when they turn the PDA on. Once the user is logged in, the encryption keys for that user are unlocked, and any data that user attempts to access they will be able to see if their keys unlock that data (Next, 2005). The single point of user identification makes this program easy and hassle free to use, but might also leave it more open to someone taking a PDA while it is logged on to the right user, and having total access to all of their information.

SafeGuard PDA uses strong encryption that the user can choose to implement in many different ways. The conventional password option is available, as well as a symbol PIN or the user can choose a biometric signature recognition password (SafeGuard, 2004). The use of all of these options makes this method appealing to many who like choices and don't want to be tied down to one authentication method. The encryption runs in the background and all data and applications on the PDA are encrypted. This enables the user to encrypt and decrypt files on the fly, so the users daily routine is never disrupted. The central management of a safeGuard PDA system sets policies as far as passwords and types of encryption on different files (SafeGuard, 2004). SafeGuard PDA also protects against unauthorized deinstallation of itself and automatically re-starts with all its old settings if a hard reset is done to the PDA (SafeGuard, 2004).

With the five methods I have presented here, any organization, or individual looking to protect the information on there PDA should be able to do it. As we have seen above, the encryption ranges in how it is implemented, from encrypting everything to encrypting just certain applications to encrypting just certain files. These options are what users should look at as they try to determine the best method for them. The biggest difference I saw between the five methods was how the password is actually input into the device. There were biometric options as well as picture stories, and regular old passwords of numbers or letters. When a user or business is looking at implementing PDA's into their network they should always deploy a security method like one of the five I have already discussed. Look at **Table 1** below for a review of the five methods.

Table 1

Comparison of the five methods reviewed

	Crypto-sign	PDASecure	Pointsec	CREDANT Mobile Guardian Shield	SafeGuard PDA
Does it allow central management	No	Yes	Yes	Yes	Yes
Is the encryption transparent to the user?	No	No	Yes	Yes	Yes
Does this require the user to change many of their daily habits?	yes	Yes	No	No	No
Are biometric needed for this method?	yes	No	No	No	Yes
Is all the data stored encrypted?	No	Yes	Yes	No	Yes
Do you have to call the help desk to reset your password?	No	No	Yes	No	No
Do you have to be on-line to reset your password?	No	No	No	No	No
Does the device lock the user out after a certain number of incorrect password guesses?	Possible option	Yes	Yes	Possible option	Yes
Can you set policies for your PDA's features and applications?	No	Yes	No	Yes	Yes

What does the operating system included do for security?

Third party security methods are available on the market because there is a demand for higher security of data. With that said, what are the manufacturers of operating systems doing to ensure their PDA's are secure without the use of third party software? While shopping for a PDA I looked at PDA's with three different operating systems (OS). All of the Palm PDA's come with the Palm OS 5. While most other PDA's come with a form of the windows OS. The two Windows OS's are Pocket PC 2002, and the newly released Windows Mobile 5.

The Palm OS is thought to be more user friendly if you are not familiar with a windows operating system already. Palm is also thought to make the most secure OS, however they accomplish this by including third party software with their products when they are shipped (LaRochelle, 2002). Palm does think about security in its OS by incorporating a 128 bit encryption as a standard feature (LaRochelle, 2002), but ships it with a third party software to ensure the security of their system.

The Windows OS that has been on the market for a while, it is appealing to many because it has the same look and feel as the regular windows OS many PDA consumers have on their desktops and laptops at home. Pocket PC 2002, offers many of the features of the regular Windows 2000 OS, this includes the strong password standard it started in the computer market in addition to its regular four digit password to unlock the device (LaRochelle, 2002). This is similar to the Palm OS, however Pocket PC 2002 is not shipped from the factory with any third party security software. The user must buy the third party software themselves if they wish to secure their PDA beyond the standard password.

That leads us to the latest a greatest OS, which is Windows Mobile 5, which was supposed to fix many of the problems with Pocket PC 2002. Most of the problems had to do with battery life, memory and applications, but security was also a big concern. The new Windows Mobile 5 includes many new security features such as, the ability to use SSL to encrypt all outlook features, the use of digital certificates, password lengths and timeout dates can also be set now as well (Greer, 2005). IT staffs are also given much more access to monitoring and setting security policies for this new operating system. Administrators can also push down policies and administrative requirements to all the PDA's on their network, by using their windows 2003 sever consoles, that many businesses already have in use (Greer, 2005).

The new Windows Mobile 5 OS sounds like the best choice, however experience in the realm of technology has taught many of us that the newest just means they haven't had as much time to work out all the bugs. Not many PDA's on the market now are shipping with the Windows Mobile 5, because it is still too new and too little is known about it. So for now most people looking at security as their main feature when they purchase a PDA should look at the Palm OS. However if you are adventurous or just like to have the newest, Windows Mobile 5 looks like a promising operating system.

What do businesses think?

As early as 1997 (Miah, 1997) business were talking about all the great things that mobile pc's, such as PDA's could be used for. So what do businesses think about PDA's now? Is the convenience of a PDA worth the security risks, if one should be stolen, or more often than that, misplaced. Should businesses give employees PDA's to use, or should employees have to buy their own if they really want to use such a device? I have read several articles and I have generally found these to be the questions most business are trying to answer.

According to Tom Goodman, Vice President of operations at Bluefire Security Technologies, "Some experts believe that the best way to protect your confidential information is not to put it on your PDA." (2003, p. 58) He goes on to say that current

PDA's lack the built in security to make IT departments feel good about encouraging upper management to add PDA's to their networks (Goodman, 2003). Later he explains why it is hard to build security into PDA operation systems. He says "[because] The handheld operating system is considerably smaller than that of a laptop, it is even more difficult for manufacturers to build in adequate security while maintaining computing power." (Goodman, 2003, p. 58) But with all the tools available today for securing sensitive data, such as personal firewalls, encryption of data stored on the device, and enforced passwords PDA's are still good tools for working professionals (Goodman, 2003) and they seem to be popular among the workforce today.

In fact they are so popular they have even been compared to the PC explosion. According to Bob LaRochelle, Vice President of product development at Axolotl, "The growth of handheld technology is reminiscent of the explosion of PC technology and its rapid adoption in the 1980's and 1990's." (2002, 68) He read from a Aberdeen Group report that the personal digital assistant market will be a $6.6 billion market by 2005 with approximately 39 million units shipped (LaRochelle, 2002). He goes on to talk about the security risk that PDA's present, but that organizations are going to have to set up policies to deal with PDA's (LaRochelle, 2002) before people start buying their own and bringing them to work.

According to Margaret Grayson, President and CEO of V-ONE Corp., People are already starting to bring their personal PDA's to work with them, creating a much bigger security risk then if the IT staff had handed out a standard PDA (Grayson, 2001). She states that because all the PDA's are different and use different security and can handle different programs, they now have a hard time making sure that information on all PDA's is secure (Grayson, 2001). Her organization thought about banning all PDA's from the network and only allowing people to use them as an address book, but they were afraid they would cut down on productivity now that so many people are used to using them everyday (Grayson, 2001). Her organization is currently looking for a compromise between user convenience and security.

An article I found suggests web applications as a compromise between security and convenience for the user (Essmayr, 2003). Weippl and Essmayr say that web services will allow most important data to stay on the secure servers at the businesses home base, but still allow users on PDA's access to the information they have become accustom to having at their finger tips (Essmayr, 2003). Through my search for business information on security and the PDA. I found that I always thought about regular 9 – 5 businesses using PDA's and I was missing a huge part of the market by not looking at health care. In the health care field doctors don't sit at a desk, instead they move around form patient to patient, thus making the PDA a very useful tool for doctors, nurses and other hospital personal to have. But with HIPPA being enacted, hospitals are one of the places that security is not only a concern but a requirement (LaRochelle, 2002).

The use of PDA's in hospitals

I have found two hospital examples I thought exemplify how useful PDA's can be in a health care setting. The first example describes one physician's account of his day with the PDA, as opposed to writing everything down on paper. The second example is using the PDA for transmitting patient x-rays and radiology scans to the doctor. I think these examples will show how useful a PDA can be in a variety of jobs in the hospital. But still remembering that security is a must in a healthcare setting.

The Canadian Journal of Anesthesia published this study in 2003. A doctor who usually talks with his patients and then walks outside to write on the chart his orders and thoughts, was now going to try using a PDA. This means instead of listening to the patient and then having to remember all that information, now he would write down everything the patient was saying as they said it, and this increased accuracy of symptoms from the patient's mouth to the doctor's notes. The study found that while this was more accurate, it also took approximately 53 seconds longer than the usual exam a doctor would do. However the chart review, assessment and documentation was 74 seconds shorter than with the usual pen and paper method (VanDenKerkof, 2003). The studies eventual findings concluded that the PDA is a reliable tool that meets data management requirements, and that the effort to secure these new devices on the network should become a top priority to hospitals to increase patient care (VanDenKerkof, 2003).

The second example was published in the Journal of Telemedicine and Telecare in 2000. This example was using a "PDA as a teleradiology terminal for reporting emergency computerized tomography scans." This study looked at how long it took to get the scan transmitted via wireless, as opposed to if it had been done, printed and taken by hand to the doctor who needed it. The study found that in 24 % of the cases the neurologist gained essential information that helped then treat the patient correctly. In 62% of the cases the neurologist received beneficial information (Reponen, 2000). The Authors of this study concluded that the PDA is a great device for helping in medical situations, not just in a hospital, but speculate that one day PDA's transmission of scans like this could save people from coming to the hospital at all if they live in a remote area with the capability to take the scan, but no doctor there to fully understand how to read it

(Reponen, 2000).

References

Crypto-sign – A White Paper. (2003). 1-8, Retrieved October 17, 2005, from http://www.crypto-sign.com

Essmayr, W., & Weippl, E. (2003). Personal trusted Devices for Web Services: Revisiting Multilevel Security. *Mobile Networks and Applications*, 8, 151 – 157, Retrieved November 16, 2005, from IEEE Xplore.

Ferrill, P. (2002). Protecting your PDA assets. *Network World*, 19(19), 52, Retrieved November 16, 2005, from ProQuest research Library.

Garvey, M. (2005). Tighter Security for PDA's. *InformationWeek*, 1(1054), 49, Retrieved November 16, 2005, from ProQuest Research Library.

Goodman, T. (2003). Lack of built-in security shouldn't inhibit PDA use. *Health Management Technology*, 24(11), 58, Retrieved November 16, 2005, from ProQuest Research Library.

Grayson, M. (2001). End the PDA security dilemma. *Communications News*, 38(2), 38-39, Retrieved November 16, 2005, from ProQuest Research Library.

Greer, T. (2005). Improve your device security. Retrieved November 16, 2005, from http://www.microsoft.com/windowsmobile/articles/msfp.mspx

LaRochelle, B. (2002). PDA's and the emerging security crisis. *Health Management Technology*, 23(10), 68-69, Retrieved November 16, 2005, from ProQuest Research Library.

Miah, T., & Bashir, O. (1997). Mobile Workers: access to information on the move. *Computing & Control Engineering Journal*, 8(5), 215 – 223, Retrieved November 16, 2005, from http://scitation.aip.org/vsearch/servlet/VerityServlet

The Next Generation: Encryption and control for Windows Notebooks, Tablets, Desktops and External Storage Devices. (2005), *CREDANT Technologies Security Solutions White Paper*, 1-15, Retrieved October 17, 2005, from http://www.bitpipe.com/detail/RES/1127826681_687.html?src=FEATURE_TERM

Pointsec for Pocket PC. (2003). Retrieved October 17, 2005, from http://www.pointsec.com/products/products_pocketpc.asp

Reponen, J., Ilkko, E., Jyrkinen, L., Tervonen, O., Ninimaki, J., & karhula, V. (2000). Initial experience with a wireless personal digital assistant as a teleradiology terminal for reporting emergency computerized tomography scans. *Journal of Telemedicine and Telecare*, 6(1), 45-49. Retrieved November 16, 2005, from IEEE Xplore.

SafeGuard PDA Enterprise Edition. (2004). Retrieved October 17, 2005, from http://www.ultimaco.com/content_products/sg_pda.html

VanDenkerkhof, E., Goldstein, D., Lane, J., Rimmer, M., & Van Dijk, J. (2003). Using a personal digital assistant enhances gathering of patient data on an acute pain management service: a pilot study. *Canadian Journal of Anesthesia*, 50, 368-375. Retrieved November 16, 2005, from http://www.cja-jca.org/cgi/content/full/50/4/368?view=long&pmid=12670814