Mobile Personal Digital Assistants

By Christopher Beggs
Master of Science in Information Security
Lewis University

February 2008

Table of Contents

Introduction

Today's business climate demands working around the clock and even around the world. This has placed a greater emphasis than ever on mobile Personal Digital Assistants (PDAs). It is said that, by 2012, 50% of traveling workers will leave their notebooks at home in favor of other devices. [1] The ability to get your email and respond wirelessly are just the beginning of the opportunities companies are looking at to extend the reach of their workforce, provide true collaboration, and ensure real-time data flow away from the confines of the office.

A number of organizations are beginning to leverage the power of smart phones, PDAs and convergence devices. These devices, along with appropriately designed software solutions, help increase revenues and profits, and improve operational efficiencies. As previously referenced, many traveling workers are now opting to leave the heavier, bulkier notebook at home in favor of a smaller, more easily handled device such as a smart phone or PDA. Smart phones, PDAs and other smaller convergence devices also allow quick access to information needed for the traveling worker, making their time more efficient on quick, smaller tasks such as checking email or getting contact information. Businesses realize the true collaboration potential of these devices compared to notebooks. While notebooks still have their role with traveling workers, it would take significantly longer to boot up a notebook, get to the desktop, find an internet connection, login to the network, download new email and other necessary files, and so on. With a wireless PDA, the information is nearly always readily available by a click of a button and, if enforced, a password to access the device.

Recently, the rise in mobile PDA use has made a number of companies, as well as government organizations, create standards in documentation for mobile devices. Suzanne Kiraly of the Canadian Standards Association states:

"Mobile devices are gaining popularity across a wide range of vertical markets in North America and are increasingly seen as a convenient way to access and share information." "As the first known standard development organization to offer standards and related products in an

interactive mobile device format, CSA is leading the way in promoting new, innovative technologies with advanced features and capabilities that deliver the best, most efficient products and services to our clients, members, and end users." [2]

As organizations continue the trend of increasing their mobile PDAs (Figure 1), many organizations need to take a moment to analyze the implications these devices have if no security strategy is implemented.

Mobile PDAs require similar approach to security as with other mobile devices such as notebooks. This ensures all policies and approaches align with the overall goals and security procedures, while managing the mobile PDAs with a consistent applied set of rules based on access rather than the device. With mobile PDAs, these devices are generally tied to an individual, which is generally a little different from other company-issued equipment.

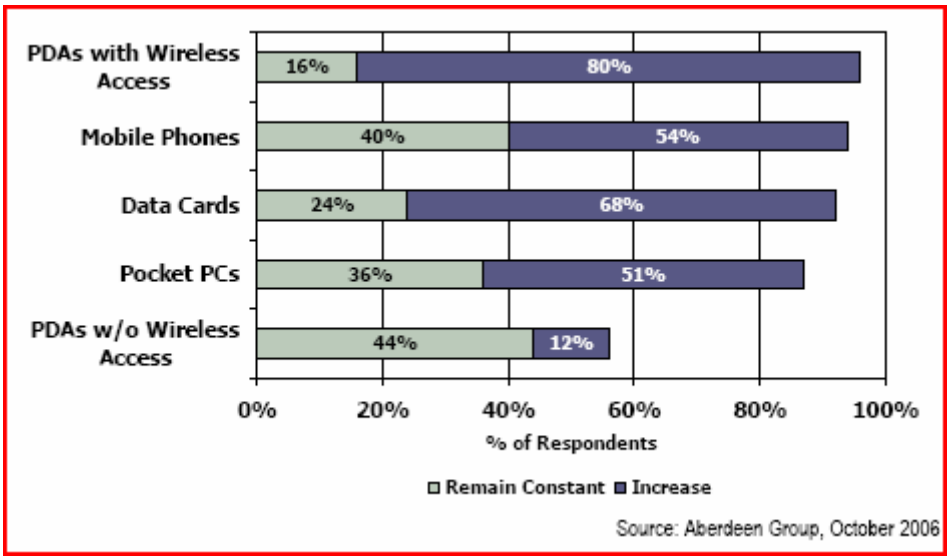


Figure 1. Increase in PDAs with Wireless Access [3]

Because of the slight difference between a notebook and a mobile PDA, the rules for how a user access on a mobile PDA are defined on an individual basis. This is dependent on how the

network environment is setup for the use of mobile PDAs. Depending on the environment and how much detail its security policies is dependent on the organization. No matter how this is done, there are always risks involved with the mobile PDA itself.

Risks

Mobile PDAs are increasing rapidly in both capacity and coming down in pricing. Because of this, the mobile PDA is more prone to loss and/or theft because of the ease of portability. Still a number of organizations are adopting the mobile PDA to support wireless e-mail and other services.

Mobile PDAs can carry a significant amount of information in the applications on the device, calendar appointments, email and even contact lists. Any organization can be at a risk of losing their intellectual property and/or other critical corporate data should the mobile PDA get into the hands of a malicious individual. The impact of such a loss can be a breach in a regulation or a loss in consumer confidence.

Many mobile PDAs reside outside of corporate firewalls but have access to corporate networks and databases. Because of this, users who lose their mobile PDA to theft allow malicious users, whose intent is to harm, an easy way to bypass perimeter defenses and introduce malware or steal intellectual property. This, of course, may be the extreme, but can be a high risk to some organizations.

Just as the loss of a notebook is much greater than replacing the notebook, the same is for mobile PDAs [4]. With the high probability of losing a device, there is greater emphasis on ways to secure the data if ever lost. This can be done by encrypting the data on the mobile PDA or by taking a more secure approach such as remotely wiping the device of all data.

A number of challenges are associated with managing and securing mobile PDAs. According to David Friedlander, Analyst at Forrester, there are many challenges which explain the level of concern with mobile PDAs. Here are just a few:

- **Personal Devices Outside of IT Control:** Users often bring in their own PDAs without IT oversight. Employees often connect the device to their machine using desktop synchronization tools. If the company is unwilling to set and enforce standards, the costs and risks associated with the mobile PDA population could increase.
- **Connection over Unsecured Networks:** Devices are often outside the enterprise's network and may connect over unsecured networks.
- **Device Complexity**: As mobile devices develop greater features, they become more complex. These device complexities can create more vulnerabilities.
- **Sensitive Information Control:** It is easy to load sensitive information on PDAs. Even with policies regarding mobile device usage, employees have significant control over what data and files are carried on mobile devices.
- **Control versus Convenience:** Some users try to get around the system by circumventing policies or even the technology in the name of convenience. [5]

Since it is impractical for companies to prohibit the use of mobile PDAs, a good approach is a controlled strategy consistent with the overall corporate security procedures. The first approach is to create a security policy. Executive support is key when creating a policy around the use of mobile PDAs. This policy should be consistent across all mobile and telecommuting devices as well. At a minimum, a policy should contain the use of strong passwords, authentication and encryption. Other security measures on the device such as antivirus, encryption of the storage cards, strong authentication and virtual private networks are also important.

A *USA Today* discusses the case of an Ernst & Young consultant who lost the names, address and credit card information on a large number of Hotel.com customers [6]. Here, if a minimum policy was in effect for the encryption on the mobile device, there might not have been a problem. Is there a need to have this information on a mobile device? Certainly, a case can be made to have this information readily available so as to help build a relationship with customers or potential customers. No matter what the benefit the user may see, training needs to be part of the process an organization follows to be aware of and mitigate possible risks associated with the loss or theft of such a device.

Training sometimes is one of the most overlooked in an organization. If employees view the security policy as a barrier to productivity, having the employees understand the risks would be helpful. No security control is 100%, so regular communications to employees is essential to cultivate awareness. In the Hotel.com case mentioned previously, even though it was an Ernst & Young consultant, giving a short training tutorial to the consultant of the risks may have helped. Others may have never even permitted an outside device to touch its network because of the risk of providing unwarranted access to information.

Finally, the use of technology to assist in enforcing policies can help. Technology should not be the first step when attempting to implement a policy, but it certainly will may be used to advantage at later stages of implementing the policy. Technology should be used to automate a manual process or at least to make it more efficient.

Policy and Procedures

Security for mobile PDAs must be based on overall risks to the enterprise rather than on a perceived need for security. Policies should be clear and understandable. Policies should also be enforceable.

As mentioned earlier, consistency should be in all security policies. Policies are written to support the mission, vision and strategic planning of an organization [7]. An ample security policy should include input from not only management, but from those specifically using PDAs to ensure the policy provides all the necessary protection while still providing functionality and not hampering the convenience of the users.

As an example, a policy should exist for locking the mobile PDA. Just like other mobile devices such as notebooks, mobile PDAs should also have a password or some means of password protection to access the data. This policy should set clear expectations of what is required. Once a policy has been established, a procedure should be implemented. An example of such a policy can be as broad as the following:

Password Use and Protection Policy EXAMPLE

I. Intent

The intent of this policy is to establish the requirements for the use and management of passwords.

II. Scope

This policy applies to all accounts that provide access to information assets or systems.

This policy applies to all locations, all business units, all users and enterprises who are entrusted with information access.

III. Responsibility

The implementation of this policy is the responsibility of all users.

IV. Enforcement

Failure to comply with this policy may result in corrective action according to the Corrective Action Policy.

V. Exceptions

For exceptions to this policy please refer to the Enterprise Information Security Exception Policy.

VI. Policy

1. Passwords must *never* be shared or divulged.

2. Passwords will not be stored electronically unless they are encrypted and password protected, nor written down unless they are locked and accessible only to the owner.

3. Compliance with this policy is will either be automated either via policy technology where possible, or a report will be emailed to the CISO regarding password changes for compliance.

4. Passwords must not be easily compromised or guessed. For example password will not contain a user name or other name, or personal information that is easily obtained (e.g. address, phone number, social security/government ID number, license plate number, pet's name etc…)

5. Passwords must be changed at least every ninety (90) days or whenever the there is reason to believe they have been compromised.

6. Passwords will not be displayed when entered.

7. User accounts will be disabled after 3 consecutive invalid login attempts in a thirty (30) minute time period. The user account is then to be locked for a period of 30 minutes. After this period, the bad password count is reset to zero and the user can attempt to log on. (The System Administrator can reset the password count at any time.)

8. Automatic lockout on all devices will be set for activation after no more than fifteen (15) minutes inactivity.

9. Users must completely log off and/or lock their device prior to leaving their computer unattended (i.e., going to lunch or attending a meeting). Users must completely log-off or shutdown before going home, leaving for the day, vacation, etc unless they are running a job on their computer.

10. User passwords will not be included in any automatic logon script, macro or terminal function keys, etc. (i.e., passwords must be manually entered at logon time).

11. If a password and credentials must be included in a job submittal stream, the job should be restricted to authorized users.

12. The credentials for a new user will require the password be changed at initial login.

13. Passwords must be encrypted when transmitted.

14. Passwords must be a minimum of seven alpha numeric characters in length, and include a minimum of one alpha (Upper and Lower Case) and one numeric character.

15. Accounts that have been inactive for thirty (30) days will be disabled. Accounts that have been inactive for ninety (90) days will be removed from the system entirely.

16. Users must not reuse a password that is the same as any of their prior four passwords they have submitted.

17. Vendor supplied default password will always be changed before a system is attached to the network.

VII. References

- Enterprise Information Security Charter

VIII. Maintenance

For any questions concerning the interpretation or application of this policy please contact the CISO.

Procedures are usually developed to describe the methods for implementing policy. A procedure is the "how to" of a policy. For every policy, typically a procedure is associated with it. Procedures can also be used as a training guide to users to help understand how he/she can lock their PDA. Some procedures could also assist in the steps needed to assist the end user.

On the next page is an example of a procedure on how to reset a password. This procedure is for the IT Helpdesk or person in charge of password resets.

Password Reset Procedure EXAMPLE

Purpose

The purpose of this procedure is to document the steps taken when a user requests a password reset.

Procedure

1. The user contacts the IT department and requests a password reset.
2. The IT department verifies the users identity by any one of the following activities:
   - 2.1 Calling the user back at their registered office phone, mobile phone, or home phone according to records
   - 2.2 Request and receive an email from the user's account
   - 2.3 If the first two options are not possible, email approval by an IT manager is acceptable.
3. The user's password is reset by an authorized IT associate.
4. The user's new password is delivered verbally to the user.

References

- Password Protection Policy

Maintenance

For any questions concerning the interpretation or application of this procedure, please contact your IT Security Representative.

Training

One key mentioned earlier was training and awareness for users who use mobile PDAs. When designing an effective training program, it is important to be sure all training products and services meet the four critical success factors: design, development, implementation, and monitoring and updating [8].

Depending on the organization, training can be done in several different ways. With Mobile PDAs, the training does not have to be different. It can be included in the overall Security and Awareness program, or could be simply providing the user with the necessary documentation. One example used is creating customized training material. On the next few pages is an example of a training document that could be used to assist users.

LOCKING YOUR WINDOWS MOBILE PDA

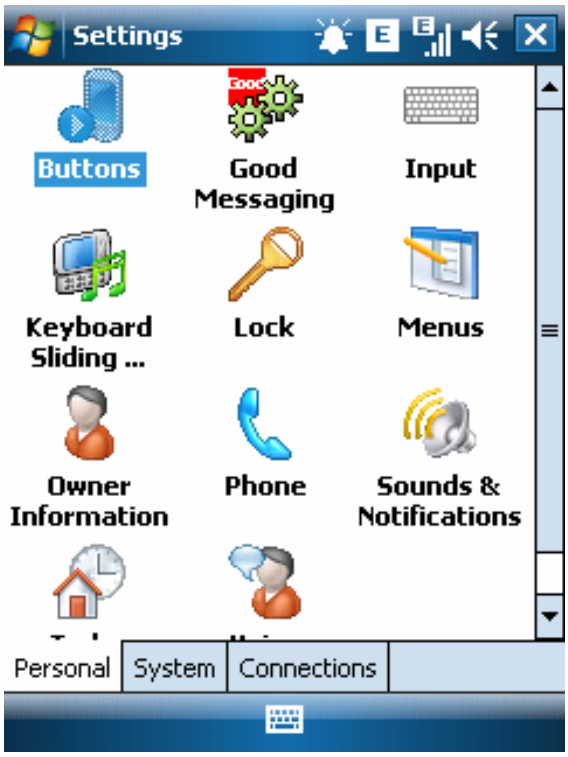
This document is to assist users with locking their Windows Mobile v6.0 Mobile PDA. For additional assistance, please contact your normal means of technical Support.

From your Today Screen:

- Click the *Start* button
- Click the *Settings* menu item

From your new screen, select the *Personal* tab.

Next, find the *Lock* icon.



The lock icon may be slightly different than the image above. This is due to the different hardware device and not the Windows Mobile v6.0 operating system.

Also note that you may need to scroll, depending on the size and number of icons in this section.

In this next window, please be sure to check the box next to *Prompt if device unused for* and use the drop down to 5 minutes or lower. We recommend 1 minute.

Inside the password box, enter a password you, and only you, can remember. These are case sensitive. We recommend using the onscreen keyboard while entering your password and confirming the password.

When complete, click *Ok* in the upper right corner. You have now successfully setup your PDA to lock itself after the set time.

As mentioned before, there are a number of different training methods an organization can take. The example above is just one example of a select policy used at an organization. Other methods can include professional training offsite or even onsite. Training such as these can get expensive but it all depends on how an organization wants to relay its message.

No matter what approach an organization takes to help train their users, getting the message out on the risks of using a Mobile PDA should be the goal. This is not to deter users from using such devices, but to spark awareness of the potential threats.

Technologies

The use of mobile devices, especially PDAs, can be managed with additional technology. One sort of technology is used to assist with enforcing the policies discussed earlier. The other is the actual mobile PDA itself. What many have not considered is the fact the different carrier technology used can also assist in mitigation risks.

Wireless Carriers

There are a large number of wireless carriers around the globe and the United States. No matter what the wireless carrier is, there are two technologies being used: GSM (Global System for mobiles) and CDMA (Code Division Multiple Access). While many people may prefer one wireless carrier over another, many do not look at how one technology can be used as a way to mitigate risk.

While there are a number of different model cell phones, smart phones, and PDAs out on the market, the one specific model to focus on is common between a number of wireless carriers and works with both wireless technologies used: GSM and CDMA. This is the Treo unit by Palm. Many of the mobile devices will have the carrier logo somewhere on the device. To most, this does not mean anything but the service one is using most of the time. However, these labels can give a thief and good indication of what wireless technology the phone is using.

For example, of the main four carriers in the US, there are 2 carriers on the GSM network, AT&T and T-Mobile. These phones have a slightly higher risk level than the other 2 carriers,

Sprint and Verizon. In figure 2, the GSM phone shows a slot for a SIM (Subscriber Identity Module) card, which is required for the phone to operate.

Figure 2. GSM Phone showing SIM Card

The SIM card is a small memory chip which is programmed with the phone number, carrier information, and other information of the user. The phone can then identify which wireless network to connect to. Because of this small card, some deviant person can simply replace this card with their own card and have control of the device in moments. Most carriers lock their phones to their service which helps alleviate some risk. However, if the user is from the same carrier, they are able to use their SIM card to get access to the phone in the same amount of time.

The largest risk on the GSM side is when people purchase "unlocked" GSM phones or PDAs. If this is the case, any GSM SIM card will work in the device. However, this is as easy to do with a CDMA wireless PDA.

CDMA devices do not use an easily accessible SIM card. In figure 3, the similar Treo unit as shown in Figure 2, shows no SIM card slot.

Figure 3. CDMA Treo showing no SIM Card Slot

In comparing the two similar Treo units side by side, Figure 4 shows the slight difference of a CDMA (top) and GSM (bottom) unit. The top unit does not contain a spot for a SIM card, while the bottom unit contains a spot for a SIM card.

Figure 4. CDMA and GSM Units

No matter what carrier a user chooses or a corporation chooses for their employees, users should be aware of the whereabouts of even these devices and be aware of the risks these devices can have at an enterprise level. One thing users should have automatically set up on a mobile PDA is to setup the locking feature on the PDA itself.

Locking a mobile PDA

As mentioned, no matter what carrier is used, any mobile device should be locked to keep others out. Each PDA operating system - Palm OS, Windows Mobile OS, etc. - have the ability to setup a locking feature on the unit. Depending on which mobile PDA a user has, will determine where to find the lock button. On some units, you will find a key guard option. This is not the same as the lock for the PDA. The key guard option does just that, guard the keys. The purpose of the key guard is to keep the PDA from accidently be turned on if dropped in a bag, pushed into a pocket, etc. The key guard will keep the phone locked until an additional key is pushed. On the other hand, the lock button is used with a simple password which requires a user to enter

in a code or PIN to access the device. While locking the device in a manual way does not have a control over this and is left up to the user to do, some programs on the market have the ability to push this control out to each PDA on its network.

Depending on the software implemented on the server to control access of mobile PDAs to information on the network, you may have to follow different control policies. There are a few software vendors out there from the Blackberry Enterprise to Good Mobile Messaging software. Microsoft has also updated its Exchange Server software, the software used in some companies to handle email messages, to allow mobile PDAs to pick up email directly. Novell has Handheld Management in its ZENworks application to help with the management of mobile PDAs. Each of the mentioned software has the ability to push a lock feature to the mobile PDA connecting to its network.

Server side technologies are not just there to push a simple lock policy request, but can also do more to mitigate the risks of any mobile device that connects to its network. This software technology allows for the data, when traveling between the server and the mobile PDA or other convergence device to have this data encrypted and sent.

Server Technologies

Each corporation is different in what messaging server is used down to what specific configuration. This also goes for the policies used to mitigate risks. For corporations that want to allow users to connect to its network to get messages, calendar information, etc, besides having policies established, using a piece of server technology can assist in enforcing most policies. Having a piece of server technology in place does not take the place of having necessary policies. Technology should be used to assist with a manual process.

While each product has its own look and feel to its management screens, most have the ability to manage mobile PDAs and other mobile devices on its network. Some of the server technologies allow the control of the hardware components including cameras, Bluetooth and IR Ports. With many newer PDAs with memory cards for extra storage, policies can be setup to disable even the

use of any memory card inserted. However, because there are more beneficial uses to having a memory card slot used, a better approach is to encrypt the data.

Encrypting the information on a memory card has almost become a standard procedure when corporations issue mobile PDAs. No matter how a mobile PDA connects to the corporation's network, information on the PDA should be encrypted. Here, additional software on the PDA could be used. However, in this example of using server side technologies, using a product such as Blackberry Enterprise of Good Mobile Messaging allows an administrator to enforce encryption to a mobile PDA. Both products have the ability to encrypt data. On the Blackberry side, it is stated as the following from their website:

> **Blackberry**
> Advanced Security Features — BlackBerry Enterprise Server delivers end-to-end Advanced Encryption Standard (AES) or Triple Data Encryption Standard (Triple DES) encryption that helps ensure the confidentiality and integrity of wirelessly transmitted information from behind the firewall to wireless devices in the field. With support for more than 100 over-the-air wireless IT policies and commands that enable IT administrators to wirelessly enforce security settings, BlackBerry Enterprise Server meets even the most stringent IT requirements. [9]

On the Good Mobile Messaging server, a similar statement on encryption of data is mentioned:

> **Good Mobile Messaging**
> Good Mobile Messaging provides enterprise-class, end-to-end security that protects your enterprise firewall, over-the-air (OTA) transmissions and the Smartphone itself. IT can even remotely control hardware components including cameras, Bluetooth and IR ports, SD cards, and more. Key security capabilities include:
> - No firewall re-configuration required
> - AES, FIPS certified encryption
> - Robust password policies
> - Remote erase of all data on the device [10]

Again, no matter what technology at the server side is used to assist in mitigating risks, something at a minimum should be used to help assist a corporation in enforcing its security policies in place.

Conclusion

Mobile PDAs make life easier for those who use them. At the same time, maintaining and administering these devices has caused some headaches for some administrators. No matter where a company may be at in deploying their PDAs, it is always best to make sure there are security policies developed to address these devices. These policies would also need to be addressed with users. By doing this, users can understand the risks associated with using mobile PDAs as well as why the policies were created. Since many users feel their internal Information Technology groups are only around to make their life more difficult, getting the users to be aware of these risks is important.

Once users are aware, when more controls are put in place to mitigate new risks, most users will now have an understanding. With mobile PDAs being very new to many companies, not all risks have presented themselves. Each day, something new is found whether it is a programming error, or some unique way of doing something could cause an exploit to appear.

No technology is foolproof. Technology is there to help us with enforcing policies put in place. Rarely should technology be put in place before having a policy. With Mobile PDAs, many corporations have acknowledged that something needs to be done to protect the data and have incorporated technology to assist. In the end, some sort of policy to be enforced is what is needed most. Training for the end users should also be made available and incorporated into the deployment process. No matter what, mobile PDAs, smart phones and other convergence devices are here to stay and must be secured.

References

[1] 10 Trends that will transform IT in the next five years. Retrieved February 5, 2008, from TechRepublic Website: http://www.techrepublic.com

[2] Canadian Standards Association to Offer PDA-Friendly Standards. Retrieved February 19, 2008 Website: http://www.ohsonline.com

[3] Enterprise Mobile Adoption. Retrieved August 30, 2007, from NetworkWorld Website: http://www.networkworld.com/whitepapers/abstract.jsp?id=116047

[4] John Surmacz, "Talk Back: Should We Store Sensitive Information on Portable Devices", *CSO Online*, 30 March 2005

[5] Managing and Securing Mobile Devices. Retrieved November 12, 2007 from CSO Online Website: http://www.csoonline.com/analyst/report2794.html

[6] Why would sensitive data ever need to be on portable computers? Retrieved November 20, 2007, from USA Today Website: http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-07-09-stolen-laptop-data_x.htm?csp=34

[7] Whitman, Michael E., H.J. Mattord (2003). *Principles of Information Security.* Boston, Massachusetts: Course Technology

[8] Technology Administration US Department of Commerce. (2003). *Building an Information Technology Security Awareness and Training Program* (NIST Special Publication 800-50) Washington, DC: US Government Printing Office

[9] BlackBerry Enterprise Server. Retrieved November 1, 2007, from BlackBerry Website: http://www.blackberry.com

[10] Good Mobile Messaging. Retrieved November 1, 2007, from Good Mobile Messaging Website: http://www.good.com