GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?

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

By: Nelson Beach
        Paper Version 1

Handheld Security: A Layered Approach

Palm Pilot handhelds, and similar devices, have started to make great strides into our business environments. Some organizations even insist on their employees owning and using one of these handheld devices as part of their daily work. These devices are basically just small computers using an operating system (OS) designed by Palm Software. This operating system is similar to the Microsoft Windows OS in look and feel, but does have a multitude of differences in its operation. The small size of a Palm Pilot makes it ideal for keeping information close at hand while you are on the road but it also makes it ideal for thieves to get their hands on. While the laptop may have started the portability of information, there are times when a laptop just won't do, such as during a sales meeting, when only a few notes need to be taken, or when you need to stay mobile all the time. To fill this gap, Palm and a few other companies like Handspring and Sony have introduced other handheld devices. Palms offer a variety of programs such as databases, spreadsheets, and word processors, as well as user-designed programs to fit just about any need you might have. These applications allow a user to carry practically any information with them where ever they go. Sometimes this information can be of a personal nature. When the handheld is being used for company business, it can contain sensitive information such as that covered by the Privacy Act of 1974, or proprietary information.

The very nature of a Palm computer allows a user to carry information with them. It can even facilitate access to information from a distance through a wireless connection, via cell phone connection or a modem. The thought of having this information rifled through by some data thief should be enough to force anyone to secure their handheld device. For example employee records might be kept on a manager's handheld. Information such as this is covered by the Privacy Act of 1974, and the loss of such information could have great repercussions for both the manager and the organization the manager works for. It is inevitable that accidents will happen and someone's handheld device will be lost, stolen, or hacked. For whatever the reason or cause, the data on the handheld device needs to be protected beyond just making sure the handheld device is not lost.

As with any form of security, more then one layer should be implemented. To rely on a single parameter or object for any security is to invite disaster. To avoid this end a multi-layered approach should be implemented with each layer having its own security controls and being separate from every other layer. For the purposes of our handheld security we are going to use a four-layer approach:
1. Responsibility;
2. Physical;
   - Theft
   - Return
3. Initial Access; and
4. Information Access.

Security at the *Responsibility* layer is enforced even before we allow our manager to take his handheld out of the box. This layer refers to outlining exactly what our manager's responsibilities are with the new handheld and details appropriate behavior with the handheld. The second layer is the *Physical* layer. This layer is in itself twofold. First the handheld needs to be protected from theft and secondly, should the handheld be stolen, a method to secure its safe return needs to be in place. The third layer, *Initial Access*, is provided when the user first signs onto or powers up the handheld device. The fourth layer, *Information Access*, is enforced when a user accesses the information itself, regardless of where that information resides, such as databases or memos.

To illustrate our four layered security model implemented in an actual work place environment, let us follow a security professional preparing to send a mobile manager out on the road with his/her new handheld. Each layer will be examined and implemented with existing products, both freeware and commercial-off-the-shelf (COTS).

Let us assume that the worst situation can occur; or, as they say, "Hope for the best, but plan for the worst". Let us assume that we have a handheld device with Privacy Act information that is being used by our mobile manager. The information on the handheld device is used to track his/her employee's time worked based on an employee number, which just happens to be the employee's Social Security Number (SSN).

Responsibility Layer
First of all, security starts long before our happy-go-lucky manager take off for his/her trip. To implement our first layer of security, *Responsibilities*, he/she should have signed a Rules of Behavior (ROB) document before they received the handheld device (A sample Rules of Behavior document is listed at the end of this paper). This document states exactly what the handheld device can be used for and what type of information can be stored on it. The ROB should also outline the disciplinary actions that will be taken should the handheld device be used improperly, or the information on it be compromised in any way. It should also provide for some type of auditing of the handheld device, since the device is not for the manager's personal use. The device belongs to the company and the company is ultimately responsible for that happens to the handheld and the information contained within it. A signed ROB will also protect the company should something happen and the information becomes compromised. A properly constructed ROB is nothing more than a document of trust that the company bestows onto the manager. The ROB provides that no surprises occur in the event of a security breach. A ROB can save a security professional's job and keep the company safe from legal action should the incident have severe consequences. Now lets assume that our manager is a little forgetful, for instance we all remember that laptop he/she left on the tram at the airport. Our manager has a poor track record so as good security professionals we need to take a few extra steps to protect the handheld device and the data.

Physical Layer
Now that we have the ROB signed, we can look into securing the handheld device by protecting the our other three layers. There are a few different methods of meeting the requirements of our

second security layer, the *Physical* layer. The first is to ensure that the handheld is transported in a place that our manager will not likely forget about, such as a large leather folder, his/her daytimer, etc. The size of the handheld device, being about the size of an average calculator, makes it easy to lose or misplace while at a dinner or meeting. By placing the handheld in a large container, or attaching it to a larger device, our manager is less likely to misplace it. It is just easier to see a large object over a smaller one. We have to assume at some point that the handheld device will be stolen or lost despite out best efforts. This is a tricky subject to deal with. If the device is stolen nothing short of a freak set of circumstances will get the device back. If the device is lost it will be very difficult to recover as well. We might get lucky and someone will turn the device in to a lost-and-Found and we can try to track it down that way. To make this easier we decide to attach the companies name, address, and phone number to the back of the device. With luck, someone will contact us and we can make arrangements to have the device retrieved. A company called IDstrip.com (www.idstrip.com) makes this a little easier for you by acting as a go between.   They provide a strip that identifies the machine to them.   Should someone find the device they can contact IDstrip.com, they will compare the ID number on the device to their database and contact the owner. This way, we as the owner don't need to put our company's identifying information on the device. We have to assume that the device, once lost, will probably be lost forever. The best hope we really have is to recover the information on it. This can only be done in one way: that is to forget about the device, get a new one, and sync it up with our manager's desktop. Hopefully they did a sync just before he/she left, as our ROB states they should. If not, wish them well in their next job.

Initial Access Layer
Before the handheld was lost, we need to have taken some action to help secure the initial sign-on. This is done in the *Initial Access* layer. The simplest way of securing the device at this layer is to require a basic password that is already built into the handheld's software. To do this we will ensure that there is a sign-on password for the handheld device. The password scheme should be the same as any password used in your organization.   The software allows a sufficiently large field to enter a password that would meet any organizations requirements. If you make this password too simple, it will be easily guessed; if too difficult your manager won't be able to remember it. He/she will then most likely write down the password on a slip of paper and tuck it conveniently into the handheld's holder where he/she can find it easily, and thus aid in the compromise of his/her own device. In order to assign a sign-on password all you need to do is go to the System option on the handheld. Then select the Password icon. A screen will come up that allows you to assign the password. Just type the password in and you're ready to go.

Using the operating system's password will only protect so far. As security professionals, we know that there are a variety of password crackers on the Internet, like Sword V1.0 which can be found at www.palmgear.com, or pcrack v1.0 found at www.freewarepalm.com. All we have to do is get the cracker, hook it up to our handheld device's desktop software and we can crack it. To provide a greater security posture for this layer, and our manager's handheld, we need to go a little further.   While the software password will stop the average thief just trying to access the handheld device, it won't stop someone more knowledgeable and determined to get to the information contained on the device. As an added feature to our software's sign-on password we

have decided to incorporate a biometric hand writing recognition software package. This way even if the password is guessed, it will still be needed to be entered onto the device in a specific hand-written script to be effective. After looking at a few products, we decide on "Sign On" from Communication Intelligent Corporation at www.cic.com. This product has the advantage of not requiring yet another password for our world-weary manager to remember, but that the manager knows how to write. The disadvantage is that there are, most likely, papers with the handheld device that have the manager's signature on them. A decent forger could just trace the signature into the graffiti box and gain access. To mitigate this, we insist that the manager use a password instead of just the signature of their name. This is also stated in our ROB so the manager should be well aware of the fact that a new password is required. This forces our manager to remember a new password, but the effort is worth it. This way, if thieves wanted to hack the handheld device, they would have to know both the password and to be able to write it into the device in the handwriting of the manager. This method might not be perfect, but it is better then using a password along, and is about the best available for the handheld device. This software is fairly robust as well. Trying to brute force the password would be nearly impossible because the hash for the sign-on is triple-DES encrypted; it would be nearly impossible to hack the code, even if the specific password file could be accessed. If the thought of using a biometric for a handheld doesn't appeal to you, or is not consistent with your organizational security methodology, you can employ any of the basic password protection programs available on the market. A good example of one is OnlyMe from Tranzoa, which can be found at www.tranzoa.com. This password product replaces the operating system's password with its own. Its nothing fancy, but it is effective. The encryption scheme used by OnlyMe is more robust then that provided by the handheld's native software.

(**Note**: Another of the advantages of passwords on the handheld device is that it doesn't need to be changed with the frequency normally seen on a standard network. The reason for this is that the handheld device can not be attacked time and time again over a period of time. If someone is trying to hack into the handheld, it will be a one-time deal, and the password they are trying to hack will be the password for the first time the hack is attempted. This doesn't make it any more difficult to hack. It just makes it easier for our mobile manager because he/she doesn't have to worry about changing the password every 30 or 60 days.)

We'll assume that someone can crack the password, and since we are paranoid we'll assume that someone will be able to duplicate the handwriting and forge the sign-on. More than likely our manager has changed the password to a sports team or a child's name by now anyways. So the only protection is the hand writing control, but if someone has stolen the Palm device, they have probable also gotten some documents that were stored in the same case.

Information Access Layer
The last layer to our security model is *Information Access*. This layer discusses the controls given to specific information contained on the handheld device. Since we assume that the sign-on password can be compromised, we decide to apply a few passwords on some of the more important databases, memos, or files that need extra protection. The basic password provided in the handhelds native software is not a strong one and we know that there are password crackers

that can get to those passwords without much difficulty. We have already mentioned a few of the crackers that can do this earlier in this paper.

With this in mind, we decide that we need to take things a bit further to protect the data. We decide to encrypt a few of the databases and files that contain our Privacy Act information. There are a few products on the market that allow us to do this, like PalmSafe from Portable Projects at www.portableprojects.com or jaws Memo from jaws Technologies at www.jawstech.com. Either of these products will allow the user to encrypt specific files or databases. Some research should be done before any solution is implemented using this type of protection since the nature of the information being protected and the guidelines from your organization should drive this more than anything else. Our manager in question needs to have a fairly robust encryption scheme. With this in mind we decide on the jaws Technologies product. This will afford us a password up to 512 characters long and uses a 4096-bit encryption algorithm. With the Privacy Act information on the handheld, this should be fine.

Now we've locked down the Palm device with a means of transportation, a ROB, sign-on password, database/memo passwords, and encryption for the more sensitive information. There is still a few areas that need to be addressed. One is the unauthorized beaming of information from one handheld device to another. This can occur more often then many people realize. There are two ways that this can happen: first someone maybe trying to send malicious code to the handheld device; second an organization may have set up a device to automatically beam information onto the handheld device in order to help them disseminate information. This method is one way to spread virus code through handheld devices. This can occur when our manager is using his handheld but not paying attention or he/she is falling asleep and has left the device on. It is simple for an individual near our manager to initiate a beaming. The entire process would only take a few seconds and our inattentive manager would be none the wiser. (Just as a side note, this would be one of the items listed in the ROB.) To prevent unauthorized beaming all you have to do is go into the Systems option, then select the Preference icon. The last selection on this page allows the user to toggle back and forth between "Beam Receive On" and "Beam Receive Off". We are going to set the toggle to "Beam Receive Off". With all these procedures complete, including the sign-on biometric password, the ROB, the database encryption, and the prevention of unauthorized beaming, our manager is ready to use his/her handheld device, and we are feeling better that we have done all we could to secure the device.

The last area for our *Information Access* layer deals with viruses. The issue of viruses has grown quite a bit in the last few years. At first we didn't need to worry about viruses but as email programs were developed for the handhelds the introduction of virus became inevitable. Our manager uses the handheld version of Microsoft's Outlook so he/she can keep track of their mail while on the road. Since email is the easiest and most predominant method of introducing a virus into a computer device we need to place some anti-virus software onto the handheld. After looking at the products available on the market we decide on F-Secure Anti Virus for the Palm made by F-Secure located at www.fsecure.com. This product runs on the handheld device and scans emails as well as files that are loaded into it. Updates to the virus software need to be performed on a regular basis to be effective. The frequency should be listed in the ROB so that no mistake can be made.

Well, we've done about all we can for our mobile manager. We've applied our four-layered handheld security model to the managers handheld device. We've described the proper physical precautions. We've ensured that the manager has signed a Rules of Behavior stating what is and is not acceptable behavior with the handheld device. We've put a boimetric for the initial sign-on and added encryption software for the more important file and databases as well as added anti-virus protection. So with our fingers crossed we hand over the handheld device knowing that we have done all we can.

Sample Handheld Rules of Behavior:

Note: *This is a sample set of Rules of Behavior for a Handheld device. They are not to be considered all encompassing or intended to be used without modifications. All Rules of Behavior need to be tailored to your organizations specific needs and requirements.*

The signer of this document agrees to adhere to all the conditions set forth in this document. Violations of any of the conditions listed here may result in disciplinary or legal action depending on the severity of the violation. If the hand held device is lost/stolen it will be the responsibility of the user to replace the device.

- The handheld device will be used for official work use only.
- The handheld device will not be used for personal use.
- The handheld device will be used for company purposes only.
- The handheld device will not contain any information that is of a personal nature.
- All information, residing on the handheld, that contain sensitive or Privacy Act information will be encrypted.
- Wireless connection will be limited to accessing emails only. No other wireless transaction will be used on the handheld device.
- Handheld device passwords will comply with organizational standards.
- Only approved software will be loaded onto any handheld device.
- Handheld devices will be synced with the desktop software on a daily basis.
- All virus software for the handheld should be updated with the same frequency as the organizations desktop virus.

Bibliography:

1. Securing the handheld environment - An Enterprise Perspective: www.palm.com
2. Palm Security: http://palmtops.about.com/gadgets/paltops/library/weekly/aa06042000b.htm
3. Passwords don't protect Palm data: http://news.cnet.com/news/0-1006-201-5005917-0.html
4. The Educator's Palm: http://educationpalm.org/palm12/security/security.html
5. Communication Intelligent Corporation: www.cic.com.
6. Portable Projects: www.portableprojects.com.
7. FreewarePalm: www.freewarepalm.com/utilities/utilities_security.shtml
8. F-Secure: http://www.fsecure.com/wireless/palm/
9. IDstrip: www.idstrip.com
10. Palmgear: www.palmgear.com
11. Tranzoa Inc.: www.tranzoa.com
12. Jawstech: www.jawstech.com
13. Person use