Global Information Assurance Certification Paper

Susan Guerrero
Security Essentials
Version 1.2c

PDAs - A Security Primer

Chances are, if your are reading this, you either own a PDA or you have just been assigned the task of primary support person for your organization's handheld devices. The popularity and wide spread use of personal digital assistants by all segments of the business community has created a double-edged sword. Many companies have few if any security tools tips or best practices for governing the use of PDAs. Nor do most of the security awareness training programs developed in house or provided by third parties include guidelines, resources, or websites a questioning audience can go to reference pertinent material. While there are a wealth of games and information services available for the devices, the number of security focused applications is in its infancy. This primer is intended as a starting point for securing what may be your organization's weak link in your security chain.

A Basic Policy and a few Best Practices

If your user community is storing sensitive company information on their PDAs, it's a good idea to inform them of the company's expectations around their responsibility for securing the device and it's content. Will the company replace a lost PDS or will the employee be expected to replace it using their own funds? If the device will contain sensitive company information, does your company have minimum-security standards? Do you have a process for reporting lost PDAs? A method for having found PDAs returned to your company? If not, some of these suggestions should get you started on developing procedures of your own.

A broadly written security policy probably already covers the care and feeding of handheld devices. If your company has specific policies for hardware, see about having it modified to include 'handheld devices and content'. People tend to become more aware of their actions when they know they will be held accountable for them. In the event one of your road warriors looses their handheld a few simple practices could result in it's being returned. At a minimum, each device should include your company name, address and a contact phone number. These can be entered in the owner fields of the Preferences option on the Palm. Turning on the password lockout feature will display the information along with the password request when the unit is activated. As a backup tape a business card to the back of the device, or secure it within the carrying case in an easier viewable location. Some companies go as far as to include verbiage which guarantees return postage if the device is mailed back to the enclosed address. The key is to have a process, use it religiously, and make your people aware of their responsibility. These days, one of the most

common items in airport lost and founds are homeless PDAs. Don't let your company become a 'lost and found' contributor.

Backup and Insurance Options

Modify your awareness program to include tips on specific behavior recommendations for users of handhelds. One behavior to encourage is daily synchronization of the device. Daily synchronization serves two purposes. First, not only is a backup of the data being created, but should anything happen to the PDA, at most, you have lost only one day's worth of updates. Second, by establishing a routine, you are training your users to become aware of their devices, the importance of its data content, and the method they use to track the unit's whereabouts. May not sound like valuable advice, but infrequent users of PDAs are most likely not daily users. They often view the devices as high tech toys, fun to mess with, but not truly offering value to their daily business functions. This attitude translates into careless handling, both of the device itself and its content, higher breakage rates and limited use of on-board security features. This group of users will provide you with your greatest security challenges.

Start your people out right, by investing in a good carrying case for each PDA. There is now a wealth of cases on the market. While all are designed to protect the delicate display screen, some perform this function better than others do. Two that I've personally been able to checkout and can recommend are the Teleputer case by Levenger and the Titanium Slider by PalmGearHQ. Both are high-end models, listing for about $100.00 each, but they are the ultimate in protection. The Teleputer is leather with a full zipper closure, storage for an extra stylus, a place for note or business cards and an exterior pocket for your cell phone. PalmGearHQ's Titanium Slider is a full metal jacket designed to protect the Palm from just about any abuse short of a nuclear meltdown. No fancy features except for the ability of the face to slide into the back cover, creating easy access to the face. PalmGearHQ also offers many more cases at more reasonable rates. Stay away from the simple bi-fold types that have no closure or worse yet, use a snap or Velcro closer that puts pressure on the screen. Prices range from $10.00 to $30.00, but units carried in these cases tend to have a higher incident of screen cracks and scratches when stored in briefcases or purses.

Next, don't rely on daily HotSyncing of the unit as the only backup utility. Traveling road warriors may not be syncing their units daily. Instead, invest in a backup software application designed specifically for the Palm. Three currently available are BackUpBuddy, BackupPro, and JackBack. All are available from PalmGearHQ. BackUpBuddy is the priciest of the three, listing at $29.95. It works in conjunction with the HotSync function to backup all applications and data on the unit. A subsequent HotSync accomplishes system restores. The

application features include a high level of customization, a cool status display and the ability to backup FlashRom applications. For what it's worth, BackUpBuddy is advertised as the only Palm Platinum Certified backup utility. BackupPro is listed for $9.95 and is executed on-board via an icon identified as zzbackup. Functionality includes selection of databases and programs to backup and the ability to execute a restore on the unit itself. The backup is stored in Flash memory. JackBack, currently offered at a discount of $9.95 until June, 2001 also maintains the backup on-board. It features a compressed incremental backup designed to reduce space and energy requirements to a minimum. Restored occur on-board. This application is the only one advertised to execute on multiple platforms. Check the specs for current compatibility.

If all else fails, there are companies who will insure your PDA against theft, loss, or breakage. Two such companies are eTagit and PalmsLostorStolen. Keep in mind, many homeowners' insurance policies also cover handhelds, but there are drawbacks. First, the deductible may be more than the device is worth, and second, you many not know if the device is covered until a claim if filed. E-tagit's premise is simple. Registration is on-line, the annual fee is $5.95, and you can 10 label up to ten small items you are prone to loose. You can even offer a reward for return of the items. When lost, the label directs the finder to call e-tagit, who in turn has FedEx contact, the finder for shipment of the item back to you. Cool Beans! The extra incentive here is your reward offer (optional), and e-tagit 'finders keepers' periodic raffles. PalmsLostorStolen's program, titled 'The Signal', is actually insurance for handhelds. Policy prices range from $3.99 to $9.99 per month, based on the original cost of the unit rather than any content. Signal's deductible is $35.00 and the service includes a copy of BackUpBuddy. As is the case with all insurance, you don't realize its value until you need it.

Password and Encryption Software

A good toolbox should include a few applications for securing the device and it's contents. The utilities described below along with more current offerings can be found at the websites listed at the end of this paper under Recommended Sites. Below are a few of the more commonly used applications with a description of their features and current prices.

- ***PDABOMB*** - $20.00 Enhances password protection by disabling all forms of data transfer, including infrared and HotSync ports until the password is supplied.

- ***OnlyMe*** - $10.00. Locks Pam when it's turned off. Password is required to access data. Does not affect previous state when turned off, so you don't have to drill back down to where you left off after power off.

- ***TealLock*** - $17.00 Allows for personal settings. Includes shortcut-stroke activation, custom locking for screen, text and images; optional automatic locking. Ability to hide private records from view.

- ***JotLock*** - $12.00. Handwriting recognition password protection.

- ***MemoSafe -*** $7.00 Replaces memo applications with encrypted ones.

- ***MaxSecret -*** $20.00 A PGP encryption applications

- ***JAWZSDataGator -*** $40.00 & $50.00. Application dependent data encryption. Lower price is standard offering; higher price is professional version.

WAP and F-Secure

Currently WAP and F-Secure are the respective organization and company leading the way in handheld security. While many others are developing applications and tools for handheld support, these two are focused on creating a secure environment for the future development of PDAs. Each has a website, which can be checked for current developments. The Wireless Application Protocol forum, WAP forum, formed in 1997 by four founding companies, is today comprised of over 500 members. Members represent the most powerful telecom, IT and software companies from around the world. This consortium's primary goal is to develop and promote a world standard protocol for use by wireless and telephony companies. The primary hardware target for WAP is a wireless device such as mobile phones, pagers, two-way radios and such. But the communication protocol and the application environment under development can be built on both PalmOS and Windows CE operating systems. The key to the WAP security model is the ability of WTLS, the Wireless Transport Layer Security, to interact with SSL, the Secure Sockets Layer through the WAP gateway. WTLS was formulated to specifically support super-secure transactions for environments with power and memory limitations. Coinciding with WTLS design with the trend of increasing power and memory in handheld devices. The convergence of the two is opening the door to development of WAP protocol in the area of HTML, HTTP and TCP. As the interoperability between different handheld devices develops two things are certain. One will be and increase in the number of attacks against handhelds as well as more cross-platform attacks. We'll also see a resulting expansion in the number of security oriented applications which will be design to create an integrated security front for these devices.

F-Secure, a leader in providing security for mobile, distributed enterprises announced in March of 2001 its second-generation anti-virus software product for the PalmOS. Known as F-Secure Anti-Virus for the PalmOS, F-Secure's website of March 7, states 'The product offers on-device protection with continuous,

automatic update service and technical support. It supports all PalmOS devices with OS 2.0 or later.' The product is designed to run locally on the handheld device and will automatically scan and detect all known malware. Automatic updates are pushed to the client's PC, allowing for synchronization during HotSync. The update process is transparent to the client. The $25.00 price includes the first year's update service. Corporate account prices, while not listed are offered. The key to F-Secure's approach is the push to the client's PC. Due to the nature of handheld devices, most threats from malicious code occur as a result of a HotSync with an infected desktop. F-Secure's process of pushing updates to the host PC ensure the handheld owner will always have the most current version of the product running on the device. It is this process which F-Secure believes will eliminate the previously identified weak link in handheld security. Prior to the release of F-Secure's product, wireless handhelds were only as secure as their last HotSync. This created a situation where the host desktop, protected by its on-board anti-virus software, could do nothing to protect the wireless handheld from receiving transmissions. Expect more development in the area of addressing wireless attacks.

Known Handheld Malware

Since mid year 2000, there have been four documented attacks in the world of handhelds. A fifth, which occurred in March of 2001 was directed at cell phones and did not affect handhelds although the potential existed. The point is the number is growing. Phage first appeared sometime in September of 2000. Considered to be the first real virus aimed a the Palm operating system, this baby was designed to affect a variety of PDA devices manufactured by Palm, Handspring, IBM, TRG, and Symbol Technologies. IT is spread when infected files are shared either through beaming or HotSync. The virus causes the screen of the handheld to fill with a dark gray box and then terminates any application, which is running. Some reports indicate all applications are deleted, leaving on the database files. Other reports state that it replicates to all other applications on the device without deleting applications. It isn't clear whether there are two variations of the same virus or if it is able to perform multiple actions. Liberty or Liberty Crack is a Trojan horse, which is much more destructive. Reports indicate it deletes all applications. Vapor, another Trojan, is reported to change file attributes to hidden. Your files are still there, but appear to have vaporized before your eyes. Finally, there is Santa, which is actually an Easter egg. That's security code for hidden functionality. Santa affected the datebook, and is believe to have been created by the original programmer of the datebook. The symptom, which is benign to device operation, is the display of the date December 25, 2030. F-Secure's anti-virus section of their website provides more detail on each of these programs along with instructions for removing them from your handheld. Some articles have also indicated infected devices can be restored via the HotSync manager by setting all HotSync conduits to 'Desktop overwrites Handheld. The problem with this approach is any applications you

have installed will have to be reinstalled. The morals of this section, get and use a good anti-virus program.

Recommended Security Sites (listed in alphabetical order):

www.Avantgo.com (mostly games, but some security articles)

www.dseifert.com/adminpass

www.handango.com

www.levenger.com

www.palmgearhq.com

www.plamslostorstolen.com

www.returnme.com

www.wapforum.com

www.F-Secure.com

Citations:

Crouch, Cameron. 'Tech tips: Keep your PDA data safe." February 12, 2001. URL: www.cnn.com/2001/TECH/ptech/02/12/PDA.security.idg (April 20, 2001).

DeJuses, Edmund X. "Airborne Viruses." Information Security. April 2001 (2001): 84-88.

Field, Benjamin J. "Wireless Security Overview." April 25, 2000. URL: www.securityportal.com/research/wireless/wirelessgeneral20000421.html (April 20, 2001).

Uimonen, Terho. "New Palm Virus Detected." September 22, 2000. URL: www.cnn.com/2000/TECH/computing/09/22/palm.virus.idg (April 22, 2001).

Halonen, Arto. "F-Secure Offers Full On-Device Anti-Virus Protection for Palms." March 7, 2001. URL: www.datafellows.com/news/2001/news_2001030700.html (April 20, 2001).

Last Updated: May 29th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event