Global Information Assurance Certification Paper

Daniel M. Lyon
Version 1.2f

THE DILEMMA OF PDA SECURITY: AN OVERVIEW

Personal Digital Assistants ("PDAs") are everywhere these days. There are many different manufacturers and styles of PDAs on the market. Typically they are some type of small, hand-held device that combines computing functions with telephone/fax and networking features. Even cellular phone companies have gotten into the act by combining hand-held computer technology with their existing products, which is one of the major reasons for the meteoric rise in the use of cellular phones. In fact, PDA technology is becoming so prevalent that industry analysts predict that by 2003, there will be more than one billion "smart devices" connected wirelessly, with more than half of that figure being web-enabled.[5] However, the primary attributes of the PDA (its portability, ease of use, and wireless capabilities) are also what turn them into the proverbial "two-edged sword". Its strengths are what make them so easily susceptible to being lost or misplaced, and also make them easy targets for thieves, hackers, and industrial pirates. Studies have shown that PDA devices have a 30% loss rate.

The ramifications of a breach of PDA security on PDA users, their clients, patients, and employers can be extremely detrimental. To put the security situation in perspective, as well as the difficulty involved in reactive measures, Tom Walsh of Enterprise Security says, "Robbers net about $85 per holdup and are caught 80% of the time. Information thefts average $800,000 in value and are caught 2% of the time."[13] That's why it is crucial to be proactive and install redundant levels of security at all of the PDAs vulnerable points, as described more fully later on in the paper. The following are potential situations confronting all of the possible "victims" of a PDA theft (even those who don't know they are):

Owner: The first "victim" to be affected by the loss or theft of a PDA is, of course, the owner. Apart from the obvious loss of a not exactly inexpensive device, the owner has also lost client phone numbers, business contacts, appointment reminders, and maybe even important electronic documents, to name a few.[12] That's just if the PDA is lost. What if the PDA is stolen? The owner may have his/her social security number, bank account numbers, online account passwords, etc. stored on his/her PDA. Imagine the damage that could be done with this valuable

information in the hands of a thief needing only a reasonable degree of technical skills. The theft scenario would be especially daunting to the PDA owner considering the woeful lack of pre-programmed security (see below).

Business/Employer: An ancillary "victim" of PDA security issues from loss, and particularly from theft, is the employer of the PDA owner. Company supplied PDAs and personal PDAs used for business purposes are ideal targets, as they are rich sources of company information. This information in the wrong hands could lead to theft of intellectual property, trade secrets, and other proprietary company information. As users keep more and more sensitive corporate data on them, PDAs represent one of the most significant holes in corporate security. Even when a PDA hasn't been lost or stolen, security issues still confront the employer of a PDA owner. With the speed and memory capacities of hand-held devices nowadays, Matt Hamblen says, "a disgruntled worker or corporate spy could quickly download data to a device with memory as big as 128MB."[5] Even absent of loss or theft, the employer may be vulnerable to PDA borne worms or viruses, which can penetrate the corporate network.

Patient/Client: Another collateral "victim" is the patient or client whose personal and/or confidential information may be stored on their doctor's, lawyer's, etc. hand-held device. This is no more clearly seen than in the healthcare industry. For example, "There are currently over 500 healthcare-specific applications for Personal Digital Assistants…[including] a growing number of applications, both commercial and internally developed, that allow a physician to store, view and interact with patient data on their PDA."[7], according to Liz Johnson and Susan Rivers. Much of this information is among the most sensitive personal information collected.[13] This not only opens up the patient to the same type dissemination of personal information that is applicable to the owner of the PDA (above), but it does so without the patient having any control or influence on the security measures adopted by the owner. The effects don't stop there. This breach of a patient's confidential information may subject the doctor to legal liability for breach of their physician-patient privilege. Furthermore, recent federal regulations could even further subject the doctor and his employer to fines and possible jail time (see Impact of HIPAA, below).

National Security: Finally, it is even possible that the loss or theft of a PDA could implicate national security. For example,

> Westinghouse Savannah River Co. in Aiken, S.C., makes weapons-grade plutonium and stores hazardous waste for the federal government, so the need to protect critical data from walking out the door is paramount, [IT manager, Charles Novak] says. Conceivably, a terrorist group could use the information to locate and steal secrets or deadly materials.[5]

Considering the events of September 11, 2001, and the type of enemy our country now faces, it is no longer possible to look at this scenario as an improbable hypothetical. It has become a distinct possibility; and thus, this kind of information must be secure at all times and at all costs.

Apart from the obvious security risks to the "victims" suggested above, in some industries, a PDA user might subject himself/herself and his/her employer to legal liability for failure to comply with new federal regulations mandating a specified level of security. For example, in the healthcare industry, PDAs are implicated in the promulgation of The Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

Impact of HIPAA: Due to the increased use of electronic patient information as a part of standardized transactions, including the use of PDAs, HIPAA directs the Department of Health and Human Services to develop high-level health information security and privacy standards.[6] The primary intent of the regulations is to ensure the secure transmission of confidential patient information by containing "a number of security and privacy regulations that will significantly affect the security requirements of hand-held devices."[6], says Liz Johnson and Susan Rivers.

> The objective of HIPAA is to:
>
> - Deploy national standards for electronic data interchange (EDI) across the industry;
> - Secure electronic individual health information;
> - Ensure uniform privacy related to access and disclosure of patient information; and,
> - Require documentation of organization-wide compliance with security and privacy regulations.[6]

HIPAA applies to any organization that transmits health information in electronic format, and sets out a time-line for implementation. For every articulated activity, HIPAA defines required parameters and implementation specifications in order to ensure privacy and compliance.[6] Failure to comply with the regulations will be enforced, and could lead to fines ranging from $100-$25,000 per violation for an unintentional violation.[6] Intentional violations could lead to a maximum jail term of ten years and fines up to $250,000 per offense.[6] It is only a matter of time before Congress decides to protect other industries that by their nature also deal with large amounts of personal, private, or confidential information.

The security issues and vulnerable points in the PDA system are several. Despite the tremendous popularity of these devices, the type of information typically carried on them, and the security implications outlined above, PDAs currently have very few security features built-in. Pre-programmed security usually consists of little more than password-based authentication. To exacerbate this lack of initial security, programs are publicly available that allow the user to bypass the default security system.[9]

Furthermore, as hand-held devices become more popular, virus writers and other hackers have begun to take advantage of the lack of built-in security. Unfortunately, the damage that can occur is not limited to the user's hand-held device. When a user syncs with a desktop, they can unwittingly transfer a virus or worm into a corporate network.[2] According to Dennis Fisher, "In the past six months, two Palm OS viruses-one more of an annoyance than anything else-have hit the handheld community."[2] Also from Dennis Fisher, "Experts say viruses and hacks written for Palm OS, which is open by design to encourage third-party application development, are just the beginning of security issues facing handheld users."[2]

As indicated, data security begins with basic password protection built in, which functions primarily to lock access to the unit and initially to hide records. A low-cost initial step would be to simply require that passwords be six to eight characters, include special characters, and be case sensitive. This can be enforced with strong IT policies/procedures in place. In addition, vendors are quickly capitalizing on this "new niche" in the hand-held market by providing enhanced password protection. These protections range from pressing a specific combination of buttons, biometrics (i.e. fingerprinting), using a stylus to

write a unique character on the screen, and tapping a unique ID on the ATM style keypad. For example, BioSentry and BioHub, which were recently unveiled by BioMetric solutions, are portable fingerprint readers and authentication devices.

Limiting access to the device using password protection is an excellent starting point, but may not go far enough for certain security sensitive applications. In addition to the password protections, it is prudent to add encryption to further increase the security of confidential information. A redundant level of protection by encrypting particular databases and applications is often necessary. One such product, MovianCrypt by Certicom, works on the Palm OS and uses the new Advanced Encryption Standard (AES) algorithm in order to encrypt each record in the Palm's database.[3] In addition, other PDA security products include:

- Security@Hand by F-Secure will include its FileCrypto software, with support for the Pocket PC and Symbian platforms as well as Palm OS. FileCrypto uses 128bit encryption and requires a password to decrypt files.[3]
- Symantec's AntiVirus for Palm OS software will scan all incoming files and applications for viruses and will download updated virus signatures to the handheld each time it is synched with the user's desktop.[2]
- PDA Defense (formerly PDABomb) is intended for Palm OS users who desire a higher-level of protection for the data residing on their PDAs than other applications currently provide. PDA Defense is an application that WILL delete all the data and applications residing on your PDA if unauthorized attempts are made to access your device (with the "bomb" enabled). You MUST set a password that you will not forget. If you do forget your password, you will have to rely on restoring your data and applications from your HotSync or backup.[9]
- Smart cards are another level of security that can be added by requiring users to physically have something, such as a smart card—a credit-card-size device that can contain identifying information and a decryption key. Smart cards can be used to authorize activation of a handheld computer. It is expected that this identification method will soon become a component of handheld authentication. Early products have already been released, such as the SmartClip sled for the Palm III and V series, from Sunderland Technologies.[9]

In conclusion, PDA security is for real. PDA security should be a serious matter for any owner. PDAs are as much of a security risk, if not more, than desktops. It is therefore incumbent upon all owners and employers, especially those that use their PDAs to store the type of information delineated above, to take it upon themselves to implement appropriate security and to articulate specific security policies.

REFERENCES:

1. *Enterprise-level Security for PDAs.* September 28, 2001. http://www.certicom.com/pdfs/datasheets/enterprise_solutions.pdf

2. Fisher, Dennis. *Grip on PDA security weakens.* eWeek. February 19, 2001. http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2686961,00.htm

3. Fisher, Dennis. *PDA security to get stronger.* eWeek. June 18, 2001. http://www.zdnet.com.au/newstech/news/story/0,2000025345,20233109-1,00.htm

4. Geralds, John and Gordon Kelly. *Biometric puts the finger on PDA Security.* Computer Reseller News. April 18, 2001. http://www.computing.co.uk/News/1125266

5. Hamblen, Matt. *Walking Disasters.* April 24, 2000. http://www.computerworld.com/storyba/0,4125,NAV47_STO46867,00.html

6. Johnson, Liz and Susan Rivers. *Feature – Implications of HIPAA on Hand Held Clinical Applications, Part 1.* http://www.pdamd.com/vertical/features/HIPAA1.xml

7. Johnson, Liz and Susan Rivers. *Feature – Implications of HIPAA on Hand Held Clinical Applications, Part 2.* http://www.pdamd.com/vertical/features/HIPAA2.xml

8. Johnson, Liz and Susan Rivers. *Feature – Implications of HIPAA on Hand Held Clinical Applications, Part 3.* http://www.pdamd.com/vertical/features/HIPAA3.xml

9. McDermott, Matthew. *PDA (Personal Digital Assistant) Security.* October 25, 2001.

http://its.med.yale.edu/security/PDA/

10. Scisco, Pete. *Split Decision.* HHC Weekly. January 5, 2001.
http://www.hhcmag.com/newsworthy/shownews.asp?article=95

11. Thibodeau, Patrick. *Information security will be key with Lawmakers.* September 14, 2001.
http://www.computerworld.com/itresources/rcstory/0,4167,STO63915_KEY73,00.html

12. Tweeney, Dylan. *Bolting Down the Secrets in Your Handheld.* June 14, 2001.
http://www.business2.com/articles/web/0,1653,12336,FF.html

13. Walsh, Tom. *Information Technology - HIPAA Security Issues & Procedures.*
http://accenet.org/HIPAA/Walsh%20Handout.pdf

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
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
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
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 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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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 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
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
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
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
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