GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Security Risks and Solutions offered for PDAs

By: Lindsay M. Genter

GSEC Practical Assignment Version 1.2b

Personal digital assistants or PDAs are becoming a necessity in corporate environments. PDAs in many instances are replacing traditional computer functions. PDA users can do simple tasks including daily organization, contact lists and simple messaging, as well as, more PC-centric tasks such as browsing the web and checking e-mail. Through PDA technology, users have the ability to browse the web, distribute files and documents, send and receive e-mail and review office suite documents. However as PDAs become more prominent throughout the corporate world, risks and security problems accompany their wide spread popularity. "Virus writers and other hackers have begun to focus some of their attention on the PDA because it is a nonsecured target." [1]

"In many cases PDAs are exactly the same as non-wireless devices. The fact that it is wireless does not necessarily put it in a class by itself. What starts making wireless more interesting from a security perspective stems from human behavior associated with the wireless device. Encryption that is used in almost every wireless device provides reasonable levels of security therefore the risks fall into human behavior issues." [2]

The two key security risk areas for any hand-held computers are Accessibility, which is broken into password and physical security and Integrity, which is broken into data and backup security, and virus security. In order to take the necessary precautions to avoid the risks on your PDA, two main security risks and solutions/guidelines offered for PDA owners are listed below.

Accessibility Risks

Password Security:

Many users do not recognize that the information stored on their PDA is open to compromise by unauthorized users therefore they do not treat data stored on their handhelds with the same care as they do their desktop. The password feature on a PDA is your first line of defense. If the user has made available his/her password function he/she is opening the data to the world. A power-on password should be required to access your PDA, similar to a PC password. Password protection is a valuable part of protecting the safety of your PDA.

- Login IDs, passwords, internal network configurations, addresses and system names must never be transmitted in e-mail messages.
- Keep passwords confidential. Never write your password on a piece of paper.
- Choose passwords that are not common, but ones that you will remember without having to write them down.

© SANS Institute 2000 - 2005 Author retains full rights.

- Avoid common password schemes such as location, PC brand, family member names or birth dates, license plate numbers, etc.
- Don't leave your wireless device unattended with it configured to remember your logon credentials and do not have its startup password feature enabled.

Physical Security:

Losing your PDA can be devastating, not just because of the hassle and expense of replacing the hardware but because of the lost data. It is each individual's responsibility to protect and secure this equipment B and more importantly, client sensitive data. Security of the PDAs is of the utmost importance. Many times, the cost of replacing lost data is greater than the cost of the PDA itself. When using a PDA, please keep the following tips in mind.

- Store your PDA in a locked credenza or drawer after hours and on weekends or take your PDA home with you, even if your equipment is locked down it is still at risk when visible and unattended.
- Don't check your PDA with your luggage at the airport and stay with it when you go through airport security. Always keep your equipment in sight in airport terminals and hotel lobbies.
- Never leave equipment visible in your parked vehicle.
- Never leave PDA exposed to extreme temperatures (below 50 or above 95 degrees). [3 4 5]

<u>Integrity</u>

Data and Backup Security:

- Only data from the most recent backup can be restored.
- Synchronize regularly to protect against permanent data loss.
- Backup your data regularly to guard against permanent data loss.
- Keep electronic and hard copies of client data secured at all times.
- Encrypt data while transmitting. [3 6]

Viruses:

"Once a virus resides on a handheld, the real problems begin. When a user sync their PDA with their desktops, they can easily transfer a virus or worm into a corporate network, which could cause significant damage. In addition, existing desktop anti-virus products are not designed to look for or block Palm OS-based viruses or worms." [1] Virus protection will be handled at the server level.

Solutions offered to Protect PDAs and Audit Devices are Available

Security issues with PDAs have become incredibly common throughout the corporate world. As mentioned above, it is important to be aware of the Accessibility and Integrity risks that could develop because the appropriate PDA precautions were not taken. There are types of defense that can be implemented to your PDA in order protect the information against possible virus

© SANS Institute 2000 - 2005 Author retains full rights.

writers and other hackers. The main solutions that I am going to address are Anti-virus products, Firewalls, data encryption, and PDA Defense. In addition, an audit tool is available called Wireless Security Auditor (WSA), which can automatically audit the wireless network.

Solutions

Anti-virus Products

"One such product, PC-cillin for Wireless, released by Trend Micro is advertised to protect all popular PDA operating systems (Palm OS, Windows CE and EPOC). As such products become generally available, their efficacy should be evaluated and incorporated into written policy. Network Associates (McAfee Division) and Computer Associates have released downloadable software for the Palm to prevent it from bringing viruses to your PC. If PDA resident anti-virus software is not installed or is insufficient, Network security needs are highlighted as the first line of defense." [8]

Firewalls

"A firewall is a software that screens or blocks certain types of sites, documents or files and can be partnered with other security measures. "Firewalls are the "traffic cops" of network security. All messages in and out must pass through them. They allow only certain types of messages to be sent to the other side." [6] "An example of another security measure is a virtual private network (VPN). The VPN serves as a tunnel from a source to its destination, encrypting information at the source that can only be decrypted at the target destination. Firewall vendors like Checkpoint are developing firewalls on a chip that can be placed in these devices for network level protection." [10]

Data Encryption

"A "wireless" transmission travels over the standard "wired" Internet network, as well as, a "wireless" network. Your transmission passes through a network gateway that converts the transmissions between wireless and wired. When traveling over the standard "wired" portion of the Internet network, your transaction is secured using 128-bit Secure Sockets Layer (SSL) encryption. This level of security is available for Netscape Navigator, Microsoft Internet Explorer, and America Online browsers free of charge. When using a PDA, the "wireless" portion of the transmission is encrypted over the wireless network using Elliptic Curve Cryptography (ECC)." [6]

PDA Defense

"PDA Defense, which was formally known as PDA Bomb, has features including encryption, lockout and a "bomb" that erases data after a pre-set number of "break-in" attempts. There are

© SANS Institute 2000 - 2005 Author retains full rights.

four versions of the PDA Defense that can be used depending on the purpose of your PDA. They are: standard (for personal use), professional (for business use), enterprise (for enterprise/business/administration use), and government (with functionality for military or government use)." [8] "The PDA Defense automatically and securely locks the PDA device. PDA Defense also provides powerful, customized, and flexible encryption of personal data. Data transfer mechanisms such as HotSync and IrDa are disabled, so that there is no way to retrieve any information without the correct password. The user can even select the option to set off the "bomb" after a certain number of incorrect password attempts. The "bomb" permanently and completely erases all data applications from the device. The data can then be stored when the device is synced with a backup maintained on the owner's computer (which is the main reason for continually backing-up your PDA). The PDA Defense is one of the first choices for PDA users and companies because of its reliability and responsible price." [13]

Audit Tool

Wireless Security Auditor

"Wireless Security Auditor (WSA) automatically audits a wireless network for proper security configuration, which helps network administrators close any vulnerabilities before the hackers attempt to break in. WSA is intended for the more general audience of network installers and administrators, who want a way to easily and quickly verify the security configuration of their networks without having to understand any of the details of the protocols. WSA is not a packet dump/analyzer It does the entire necessary packet monitoring and analysis, and provides the user with just the answer to the important management questions. The WSA has a variety of beneficial components such as:

- Tracks beacon packets to find all access points.
- Determines SSID and AP name.
- Tracks probe packets, and the probe response.
- Tracks data packets.
- Determines: link encryption method.
- Tracks authentication packets.
- Determines authentication method.
- Tracks clients.
- Determines firmware version by fingerprinting the access point's detailed behavior." [14]

Developing Policies for PDAs

Most of the PDAs used today have been purchased by individual employees. However the question now arises as to whether or not companies should issue PDAs much like they issue laptops as standard equipment. The main problem with the controversy over company issued PDAs vs employee purchased PDAs is who is the owner of the company and/or client information, the company or the employee? Most network executive's say it does not matter whether or not the PDA is purchased by the company or the individual employee the information

© SANS Institute 2000 - 2005 Author retains full rights.

on the PDA still belongs to the company. Due to the fact that PDAs are extremely common whether purchased by an individual employee or provided for by a company, it is important to either develop a policy that employees can reference on a need to know basis or to address the emerging risks presented by the PDA devices by expanding their IS policy. "To the degree that more powerful PDAs mirror the features of the desktop environment, organizations can adapt existing policy. But new vulnerabilities arise due to the high portability of these devices, rapidly emerging wireless capabilities and the need for fast, convenient access to their collections of personally useful information. A policy must be developed to address this wider and rapidly expanding sphere of exposure. The policy must take into account whether the electronic transmission of sensitive or restricted data meet your organization's standards or not." [11] There are six key items that should be considered when developing policies for a PDA, they are:

- "Supported Applications: With consumer-oriented handhelds come a plethora of applications not usually supported within the IS organization. While IS may want to support some common ones, other simply put too great a burden on support staff due to their "consumer" nature.
- Data Security: Policies must be in place to safeguard data on personally owned machines. Data ownership can become a gray area and must be clearly articulated. Sometimes purchasing the devices for employees may be the best course of action to ensure ownership. All data maintained on mobile devices should be backed up to corporate resources.
- File Formats: Many consumer mobile devices have proprietary file formats. Any device supported must have a well-understood translation facility to move data to the standard formats employed on the desktop.
- Procurement Relationships: The IS organization should encourage mobile device purchases from vendors with which there is an existing relationship.
- Third-party Service Relationships: In many cases, consumer mobile devices are "throwaways," that is, the cost of repair is often more than the price of new equipment. You have to decide whether service contracts are worth it or not.
- Does it meet your organization's standards for the electronic transmission of sensitive or restricted data?" [5]

"Wireless Application Protocol(WAP) is an international industry effort that has established standards for wireless communications. As part of the WAP specifications, WTLS implements options for authentication and encryption. It is optimized for use in the mobile environment. The next release of WAP will contain additional measures to assure highly secure transactions, including end-to-end security and support for PKI." [11]

© SANS Institute 2000 - 2005 Author retains full rights.

Conclusion

There is an obvious value in equipping users with PDAs but at the same time there are obvious risks involved. Since PDAs are becoming more and more common throughout the corporate world, it is important to remember that appropriate precautions should be taken before placing confidential personal or business/client information on your individual PDA. The technological world is constantly changing and part of our responsibility is to take the correct safety measures and to use the references available to us to secure and protect our personal information.

List of References

[1] Fisher Dennis. "Grip on PDA security Weakness" 19 February 2001. URL: http://techupdate.zdnet.com/techupdate/stroies/main/0,14179,2686961,00.html

[2] Knight, Julian. "What are the security issues involved with the use of handheld Web devices?" URL: http://www.itsecurity.com/asktecs/jun401.htm

[3] Crouch, Cameron. "Tech tips: Keep your PDA data safe." 12 February 2001. URL: http://www.cnn.com/2001/TECH/ptech/02/12/PDA.security.idg/index.html

[4] Reuters. "PDAs increasingly vulnerable to hackers" 16 August 2001. URL: http://news.cnet.com/news/0-1006-202-6894699.html

[5] Gaudin, Sharon. "The PDA Predicament" 20 April 2000. URL: http://www.nwfusion.com/reviews/2000/0320pda.html

[6] Fleet. " HomeLink Security and Privacy." URL: http://welcome.fleet.com/homelink/security.asp

[8] Trend Micro Press Release. "Trend Micro offers free Virus Protection for Wireless Devices." URL: http://www.net-security.org/text/press/982203494,36531,.shtml

[10] Dodd, Carla. "In Depth: Information Technology." 27 July 2001. URL: http://stlouis.bcentral.com/stloois/stories/2001/07/30/focus2.html

[9] PDA Defense. " Defend your Information." 31 January 2001. URL: http://www.pdadefense.com/newsVersion1.asp

[10] IBM. "Wireless Security Auditor." URL: http://researchweb.watson.ibm.com/gsal/wsa

[11] St John, M Gregory. "PDAs and Policy." 3 February 2001. URL:

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.sans.org/infosecFAQ/PDAs/PDA_policy.htm

© SANS Institute 2000 - 2005, Author retains full rights.

Last Updated: April 27th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
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
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 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 Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	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
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS