



Interested in learning more about security?

SANS Institute

Security Consensus Operational Readiness Evaluation

This checklist is from the SCORE Checklist Project. Reposting is not permitted without express, written permission.

SCORE Security Checklist

Handheld devices audit checklist

Prepared by Eric Maiwald, Adam Robb, Jochen Bern, JB Bagby

References:

1. David Melnick, PDA Security: Incorporating Handhelds Into The Enterprise, McGraw-Hill, 2003
2. NIST, Special Publication 800-48, Wireless Network Security for 802.11, Bluetooth, and Handheld Devices. 2002
3. Palm Inc, Securing the Handheld Environment - An Enterprise Perspective.
4. Jansen et al, Assigning and Enforcing Security Policies on Handheld Devices, NIST 2002.
5. Handheld Security: A layered approach, Nelson Beach, June 2001
6. PDAs – A security primer, Susan Guerrero, May 2001
7. A whole new world for the 21st century, Darrin Lau, March 2001
8. PDAs and Policy, M Gregory St John, February 2001
9. PDA/Wireless Communications Pains, Scott Johnson, November 2000
10. Security in the palm of your handheld, John McCormick, March 2001, Techrepublic
11. Tips for keeping a leash on your PDAs data, Cameron Crouch, September 2001, PC World
12. Bolting down the secrets in your handheld, Dylan Tweney, June 2001, The Defogger
13. A virus in the palm of my hand, Allan Hollowell, September 2000
14. Security vulnerabilities in the Palm OS version 3.x, Laura Thomas, July 2001
15. A whole new world for the 21st Century, Darrin Lau, March 2001

Introduction:

The purpose of this paper is to update previous guidance on mitigating security measures for Personal Electronic Devices (PEDs), Personal Digital Assistants (PDAs), email and paging devices (such as Blackberry), and other hybrid handheld communication devices that have inherent vulnerabilities (for this paper all of these devices will be called PDAs). This paper provides a basic checklist in performing an audit of an environment in which PDAs are used. This checklist attempts to provide information on existing software that may be used to strengthen the security of the handheld devices.

Unfortunately, the PDA market is evolving quickly with the addition of new devices, peripherals, and services.

There are two basic classes of PDAs: those using the Palm Operating System (OS) (Palm Pilots, Handspring Visor, etc.); and those running Windows CE and Pocket PC (Compaq, HP Jornada, Casio, etc.). PDAs can have a wide variety of accessories, including modems, synchronization cables, wireless connections, and flash memory storage.

Both the Palm OS and Windows CE operating systems have software libraries with applications being developed and distributed throughout both the

commercial and freeware shareware channels. As with any software developed by non-trusted sources, however, there is the possibility that some programs may contain Trojan horse code, such as a code hidden within an application without the user's knowledge.

One problem with PDAs is their size, portability, and their ability to store large amounts of information. Add to this the breadth of communication options available and you have a device that introduces many security risks. Since the devices are relatively inexpensive, users buy their own devices or receive them as gifts. They may come into use in an organization regardless of whether the organization approves their use. As such, a company or government entity has no control over corporate data leaving the organization on the device. Therefore, prior to performing the audit, the auditor needs to ascertain the circumstances in which devices are used by the users and whether they are issued by the organization. How the devices are used and the type of information that is stored on the devices will directly impact the overall risk to the organization.

Vulnerabilities may exist when using PDAs attached to personal computers (PCs) or other network-connected AIS. The main risks associated with this usage are:

- A well-written Trojan horse program can be installed into a backdoor on host networks to permit hacker exploitation.
- A wireless PDA connection can be used to transmit and receive data to and from a PC without the knowledge or permission of the user.
- Antivirus products for handheld and mobile devices are not as well developed as PC antivirus software because the use of PDAs has only recently become routine.
- PDA operating systems do not limit malicious codes from modifying system files.
- A PDA uses infrared transport technology, which allows users to transmit data to other PDAs, thus circumventing information technology (IT) and physical security processes of such activity.
- PDAs are small and thus easy to steal or to lose. This may allow sensitive information to be disclosed to unauthorized individuals.

It is almost impossible to attempt any audit of handhelds without a security policy item governing the use of the devices within the organization. If the organization has not implemented such a policy, this then should be the first step in reducing the overall security risk that these devices pose to the organization.

If the use of these devices is wide spread within the organization, it will be impossible to check and examine all of the devices. The auditor will need to determine which devices pose the biggest risk to the organization and begin there.

Checklist:

No	Control
1.	<p>Security Policy– Determine if the organization has a defined policy for the use of handheld devices. This policy should cover:</p> <ul style="list-style-type: none"> • Information that is to be placed on the device • Security configuration of the device including all software that is to be used to protect the information • Modes of operation, including whether wireless radio frequency and/or infrared transmission is permitted. • Whether the user is permitted System Administrator rights to the company or government entity base PC with which the device synchronizes.
2.	<p>Use Policy– Determine if the organization has included handheld devices in its acceptable use policy. This policy should cover:</p> <ul style="list-style-type: none"> • Prospective personally owned PDA users will sign an agreement defining permitted use policy. • A PDA may not be used to enter or store passwords, safe/door combinations, personal identification numbers, or classified, sensitive or proprietary information. • No upload/download via wireless or infrared, while connected to a desktop PC, particularly a networked PC. • Use infrared only for authorized data transfers. • PDAs will not be left unattended when attached to a computer. • PDAs will be secured with password protection when not in use. • Device should be used for work related activities • Device ownership is established (this will depend on the policy of the organization with regard to employee-owned devices) • Allowed network connectivity will be identified • Only approved software will be loaded on the device • The user must take responsible steps to prevent the loss or theft of the device • The user must regularly sync the device with its home PC or the network so that appropriate security files (such as virus signatures and policy files) may be updated
3.	<p>Awareness Training – Determine if the organization includes information about the security of handheld devices in its security awareness training. This training should cover:</p> <ul style="list-style-type: none"> • Physical security of the device • The handheld security policy • Information that may be stored on the device • The procedure to follow if a device is lost or stolen
4.	<p>Device Registration – The organization should maintain a registry of all devices in use. This registry should include:</p> <ul style="list-style-type: none"> • Serial number of the device

No	Control
	<ul style="list-style-type: none"> • Make and model of the device • Employee to whom the device has been issued <p>Each device that is owned by the organization should be marked as such with an asset tag or other permanent marking.</p>
5.	<p><u>Initial Checklist</u> – Prior to the device being issued to an employee, the organization should follow a checklist to make sure that the device is registered properly and that the employee has received a device that is properly configured. Items on the checklist should include:</p> <ul style="list-style-type: none"> • Device added to the registry • Employee has read and understood the Use Policy and the Security Policy associated with handheld devices • Employee has received awareness training regarding the security of the handheld • The device has been properly configured regarding security • All necessary security software has been loaded on the device
6.	<p><u>Employee Termination Procedure</u> – Determine if the return of handheld devices is included in the organization's employee termination procedures.</p>
7.	<p><u>Device Authentication</u> – Determine if the device authentication meets the organization's authentication policy. All devices should require authentication at power up and at regular intervals while active. The authentication mechanism should be one of the following:</p> <ul style="list-style-type: none"> • A strong password (preferably eight characters and a mixture of letters, numbers, and special characters) • A smart card in conjunction with a PIN or password • Biometrics (such as a fingerprint) in conjunction with a PIN or password <p>Note: authentication by handwriting is not recommended.</p> <p>Software to enhance device authentication is available from Bluefire Security, Credant, and PDA Defense</p>
8.	<p><u>Anti-Virus Software</u> – Determine if AV software is loaded on each handheld device. This software should be configured to examine files as they are opened. Updated signatures should be installed on the device every time the device syncs to its home PC or at regular intervals via a network connection.</p> <p>AV software for handheld devices is available from F-Secure, Trendmicro, and Symantec (Beta)</p>
9.	<p><u>Theft Protection</u> – Determine if sensitive information on the device is protected if the device is lost or stolen. In order to protect sensitive information that may be stored on the device, all information on the device should be permanently deleted if 8 consecutive failed login attempts are made.</p>

No	Control
	Software that can perform the information deletion is available from Bluefire Security, Credant, and PDA Defense. Note: Blackberry devices already have this functionality.
10.	<p>File Encryption – Determine if sensitive information on the device is encrypted with a strong, recognized algorithm such as AES or Triple DES. The key to the file encryption may be tied either to a certificate on a smart card or to the user’s authentication information.</p> <p>Note: As of the date of this paper, U.S. government use requiring encryption algorithms must meet National Institute of Standards and Technology (NIST) FIPS PUB 140-2.</p> <p>File encryption software is available from F-Secure, Bluefire Security, Credant, PDA Defense, Certicom, and Trust Digital.</p>
11.	<p>Device Firewall – Determine if the device is protected by a device firewall. The firewall should be configurable to the organization’s security policy and protect all network connections.</p> <p>Device firewall software is available from Checkpoint and Bluefire Security.</p>
12.	<p>Virtual Private Network Software – Determine if VPN software is used when the device connects to the organization over the Internet. The VPN software should use IPSec or SSL and be tied into a strong authentication mechanism.</p> <p>VPN software is available from Funk Software, NetMotion, Checkpoint, and Certicom.</p>
13.	<p>Device Integrity – Determine if the device has a mechanism to detect modifications to key system files or registry settings. The device should alarm if the key files or settings are modified and prevent damage from the device to spread into the organization.</p> <p>Integrity software is available from Bluefire Security.</p>
14.	<p>Device Management – Determine if there is a central management capability in the organization. Since these devices are not completely under the control of the organization and are by nature mobile, the organization should have a mechanism to manage the security policy of the device from a central location.</p>
15.	<p>Network Connections – Determine if all device network connections are either disabled or protected. The network connections to verify include:</p> <ul style="list-style-type: none"> • Bluetooth • Infrared • 802.11 • CDMA • GPRS
16.	<p>Desktop Syncing – Determine if a password is required in order to</p>

No	Control
	sync the hand held device to the desktop.
17.	Insurance - Ensure that all handhelds are insured against theft, loss or breakage.
18.	Expansion Slots – The use of peripheral hardware for handheld devices is not permitted unless pre-approved by the body within the organization responsible for establishing standards in this area.



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Tokyo 2010 Spring	Tokyo, Japan	Feb 15, 2010 - Feb 20, 2010	Live Event
SANS India 2010	Bangalore, India	Feb 22, 2010 - Feb 27, 2010	Live Event
SEC540 VoIP Security Debut, San Antonio	San Antonio, TX	Feb 22, 2010 - Feb 27, 2010	Live Event
RSA Conference 2010	San Francisco, CA	Feb 28, 2010 - Mar 01, 2010	Live Event
SANS 2010	Orlando, FL	Mar 06, 2010 - Mar 15, 2010	Live Event
SANS Wellington 2010	Wellington, New Zealand	Mar 15, 2010 - Mar 20, 2010	Live Event
SANS Dublin 2010	Dublin, Ireland	Mar 15, 2010 - Mar 20, 2010	Live Event
SANS 507 Norway 2010	Oslo, Norway	Mar 15, 2010 - Mar 20, 2010	Live Event
SANS at FOSE, GovSec and US Law 2010	Washington, DC	Mar 23, 2010 - Mar 25, 2010	Live Event
SANS UAE 2010	Dubai, United Arab Emirates	Mar 27, 2010 - May 06, 2010	Live Event
SANS Northern Virginia Bootcamp 2010	Reston, VA	Apr 06, 2010 - Apr 13, 2010	Live Event
SANS 503 Norway 2010	Oslo, Norway	Apr 12, 2010 - Apr 17, 2010	Live Event
The 2010 European Community Digital Forensics and Incident Response Summit	London, United Kingdom	Apr 14, 2010 - Apr 20, 2010	Live Event
SANS Geneva CISSP at HEG Spring 2010	Geneva, Switzerland	Apr 19, 2010 - Apr 24, 2010	Live Event
SANS Toronto 2010	Toronto, ON	May 05, 2010 - May 10, 2010	Live Event
SANS Security West 2010	San Diego, CA	May 07, 2010 - May 15, 2010	Live Event
SANS Phoenix 2010	OnlineAZ	Feb 14, 2010 - Feb 20, 2010	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced