Global Information Assurance Certification Paper

PDAs and Policy

M Gregory St John

The rapid concurrent development of PDAs (Personal Digital Assistants) and their wireless capabilities has created an urgent need within organizations to expand their IS policy to address the emerging risks presented by these devices.

Why Worry?

PDAs have rapidly evolved from their humble origins as digital address books and shopping list repositories to platforms with true operating systems and sophisticated communications features. As an alternative to the bulky, static and primitive appointment books lugged around by business and sales armies, PDAs offer all the obvious advantages in addition to expandability and connectivity. They have quickly become almost essential tools within most organizations. Their rapid assimilation into the mix of wireless devices serving personal needs adds to the blurring of partitions between work and personal information space. Consequently, security concerns take on new and complex dimensions. 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. Policy must be developed to address this wider and rapidly expanding sphere of exposure.

Where is it? – Everywhere!

The increased need for physical control of these devices should be apparent and should be specifically addressed by policy. This should include a statement about unsupervised access if they are publicly deployed throughout the organization. Palm ™ advertises their Ethernet Cradle with the caption "Access from anywhere in the enterprise". Product details expand on this by stating "The cradle is placed in lobbies, conference rooms, training centers, labs, cafeterias or other shared spaces where it offers a network access point…".[1] Risks associated with this capability can be limited by disabling it completely, strictly controlling access points, enhancing network security or issuing guidelines. The value of the information being protected and systems being accessed should be the driving considerations.

It must be in my briefcase.

When not used as a network connected device, PDAs are vulnerable both because of the information they contain and the means by which it is accessed. To a question on a bulletin board asking what use was made of a PDS, the answer was: "I am a nurse… I use it for personal organization & work. I keep ALL my personal data in one spot (passwords, immunization records, timelines,contacts, everything)". IS policy needs to address information classification for PDAs. Assessing the personal risk of keeping all your passwords on a PDA should not require more than a moment of consideration! In general, PDAs seem currently to lack adequate or easy to use security features. Operating system upgrades will eventually address this, but add-on applications such as TealLock™ are a viable interim solution. It also provides an additional layer of protection. As a basic security application, TealLock™ auto-locks the device after an interval of inactivity. It can then be unlocked by a sequence of keystrokes. Some guidelines for the use of this product might be as follows:

- Set everything of value to 'private'.
- Always hide private and attend to the need to re-hide after it has been changed.
- Use a long inconvenient password for the base security system, supplemented by an shorter, but more frequently changed one for the add-on security application.
- If ever left unattended, make sure private records are hidden or locked by the add-on application.
- Provide contact information at the login prompt so that if an honest person finds the device, it can be returned.

The downside of password security is associated with physical control of the device and the ability to reset passwords. The risk is lost availability, and possibly lost data, as illustrated by another BBS message: "Kids

---

put password and can't remember,what can i do???". The answer, for Palm™ devices at least, is to do a HotSync and hard reset of the resulting in the deletion of everything entered since the last HotSync. In summary, you might say that PDAs raise the bar on physical security and information access policy. Laptop policies and guidelines can be adapted to some extent, but greater portability and the tendency to continue using PDAs as personal organizers prompts the need for a more targeted and specific policy.

Palm Virus

By now, it's well known that several "proof of concept" type attacks have been successfully mounted against the PDA platform. These attacks, while not particularly damaging, were noteworthy in establishing the vulnerability of PDAs to such threats. International Data Corporation(IDC) estimates that worldwide deployment of handheld devices will reach 19 million by 2003[2]. Such rapid growth both in number of units, variety of features and value of a rapidly increasing volume of content adds to the appeal of these devices as targets for malicious attack. This problem is gaining attention and has led to the very recent introduction of PDA resident 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 as appropriate. Another layer of protection is clearly warranted as PDA use expands and they become increasingly exposed to a variety of threats.

Palm Surfing

Wireless capability arrived in a highly visible package with the Palm VII™. Having both HotSync and wireless in a single device presented a mobile challenge to IS policy. Since these devices pose threats similar to modem connected workstations, the most apparent risks typically fall under existing policy. An obvious response by some organizations was to absolutely prohibit the connecting of Palm VII™ to the network. But it's not that easy. Upgrade kits are now available to allow a variety of handheld devices to interface with modems or cells phones and establish wireless connectivity. It's apparent that policy must seek to address the appropriate use of these wireless devices since they will continue to proliferate in a variety of physical configurations.

The ability to download e-mail with attachments through a wireless connection is one clear exposure to be addressed by policies which permit wireless-capable PDAs to connect to the network. Virus scanning at the workstation interface is an applicable safeguard, but what about PDA's directly connected to the network? If PDA resident anti-virus software is not installed, or insufficient, Network security needs are highlighted as the first line of defense.

Other concerns are raised by the security of the wireless link itself. Does it meet your organization's standards for the electronic transmission of sensitive or restricted data? In some cases the answer may be 'yes'. In the case of Palm VII™ 's Web Clipping Proxy server, message confidentiality is provided by DESX data encryption combined with elliptic curve key management. [3] Server authentication is also implemented. For online transactions, vendor specifications indicate that client authentication can be built into those applications requiring it. Standards efforts are also ongoing, giving significant attention to security issues. 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 The next release of WAP "will contain additional measures to assure highly secure transactions, including end-to-end security and support for PKI."[4]. Despite these safeguards it must be kept in mind that all the communication and system security risks characteristic of the internet are present in these situations involving wireless to web connectivity.

Emerging Policy

Policies for PDAs will be under pressure to not impact the convenience and portability these devices provide. Often, the behavior of these device users will have already have been and constraints will be difficult to monitor or enforce. Some organizations are not willing to tolerate the risk inherent in wireless capable PDAs and have prohibited their use. Other elements of typical current policy might include:

- Configuration Management by Information Security or Technical Support personnel.
- Content dictated by information classification policies.

- Limitations on points of entry into the corporate network.
- Limitation by manufacturer or operating system.

The market driven introduction of products, features, more sophisticated operating systems and more elaborate wireless, IR and other points of entry will present the need for a sophisticated and finely tuned IS policy. At this point no clear patterns in policy have emerged, but the invasion is here and adaptability is key.

References:

1. Palm™ Ethernet Cradle URL: http://www.palm.com/products/enterprise/ethernet.html.
2. Trend Mico press release: Trend Mico offers Free Virus Protection for Wireless Devices URL: http://www.net-security.org/text/press/982203494,36531,.shtml.
3. Palm Computing Platform Copyright © 3Com Corporation.
4. WHAT IS WAP AND WAP FORUM? URL: http://www.wapforum.org/faqs/index.htm#faq05.
5. Brown, Bruce and Marge. Secure Your PDA , ZDNet HELP & HOW-TO URL: http://www8.zdnet.com/zdhelp/stories/main/0,5594,2403097-2,00.html.

Last Updated: May 29th, 2017

Upcoming Training

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 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 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 Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	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
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event