Global Information Assurance Certification Paper

PDAs: The New Vulnerability That's No Longer Over the Horizon

Timothy D. Westland

15 September 2000

The use of personal data assistant (PDA) devices is exploding. "Palm expects to double sales of its handhelds this year."[1] Every week my information assurance office receives a new request for another PDA to be purchased and approved for use. So far we are not allowing them to connect to our LAN because they are a "new, largely unprotected domain where viruses could spread."[2] But it's only a matter of time until this becomes the norm. Many hours of discussion have been expended on the new threats and vulnerabilities this presents to our network. Most of those discussions occurred even before the PalmOS/LibertyCrack trojan appeared on 28 August 2000.[3] The reason I feel this is a growing concern was emphasized when Palm Inc's. CEO recently was provided an audience with military officials at the Air Force Information Technology Conference in Montgomery, Alabama. His pitch was "Simply Palm, simply Air Force."[4] The devices are already becoming standard in sections of the Navy and Palm Inc., "is targeting the military as its latest growth market."[5] Once the military gets used to having access to these very useful devices we in the military information assurance world will be told to find a way to secure them without hampering their usefulness too much. The question then is how do we do just that.

There have always been two extremes in the security world. The opposite ends of the security

[1] Salkever, Alex. "The Next Target for Viruses: Mobile Devices." 5 September 2000. URL: http://www.businessweek.com/bwdaily/dnflash/sep2000/nf2000095_571.htm (7 September 2000)
[2] Shankland, Stephen. "McAfee takes crack at antivirus software for handhelds." 21 August 2000. URL: http://news.cnet.com/news/0-1006-200-2577916.html?tag=st.ne.ni.rnbot.rn.ni (7 September 2000)
[3] McAfee.com. "Virus Profile-Liberty Crack." Virus Information Library. 28 August 2000. URL: http://vil.mcafee.com/dispVirus.asp?virus_k=98801 (7 September 2000)
[4] Quoted by Verton, Dan and Seffers, George. "Palm makes a pitch to the military." 11 September 2000. URL: http://www.fcw.com/print.asp (7 September 2000)
[5] Verton and Seffers.

spectrum are complete unhindered access (read: little or no security in place) and such tight security that even legitimate users are restricted to the point of frustration with use of the system. All of the security disciplines walk this tenuous tightrope of determining the proper mix of security vs. access. Over the years we have become experts at determining the proper mix for standard information technology installations and will eventually get there with PDAs. The problem is that PDAs are very new, uncharted territory when compared with the average desktop computer and PDA technology is changing rapidly.

Right now the memory and processing power in a PDA is limited and thus its ability to run software designed to detect malicious software is also limited.[6] But, we have now had the landmark occurrence of the first malicious software on a palm top. If the malicious code trend on PDAs follows the trend malicious code followed on desktops a floodgate of malicious software is headed our way very soon. PDAs are approximately at the same position now, as PCs were when the prime mode of transferring malicious code on a PC was via a floppy disk taken from one computer to the next via the "sneaker net." However, a PDA is still vulnerable "to virus transmissions when it exchanges information directly with the internet or with another handheld."[7]

Furthermore, palm tops are gaining processing power every day and the push is to have wireless Internet connectivity.[8] This makes them much more useful, attractive and beneficial to the user but also opens up a whole new arena of vulnerabilities. PDA popularity is partly due to the ability to beam applications and contact information via the infrared port.[9] This makes PDAs

---

[6] Shankland.
[7] Shankland.
[8] Salkever.
[9] Miles, Stephanie. "Trojan horse rears its head on Palms." 28 August 2000. URL: http://news.cnet.com/news/0-1006-200-2635223.html (7 September 2000)

the most mobile, hard to track backdoors into the LAN around the firewall that we have. It is not unrealistic to imagine a user connecting via PDA to the Internet and unknowingly downloading malicious code, that may or may not affect his PDA, then synching that PDA with a desktop inside the firewall and infecting the entire organization.

Another consideration must be that as the memory capability and processing power of PDAs increases so will the complexity and ability of the operating systems. Equally the complexity, damage potentiality, and variety or range of malicious software capable of affecting or being transmitted by PDAs increases. The bottom line is PDA transmitted or affecting code will surely become more and more destructive and disruptive.

What's the answer?

Certainly good policy is an absolute requirement! The debate over what verbiage a policy must contain is ongoing. In a military environment with areas where classified information is routinely processed consideration must be given as to where PDAs will be allowed to be brought. We must also stipulate what procedures or measures will be instituted to ensure PDAs are not brought into an area where they are prohibited. We must determine what unclassified information will be allowed to be processed and stored on PDAs. Some of the information categories requiring decisions are For Official Use Only, sensitive but unclassified, and information covered under the Privacy Act of 1974. Again, answers to the hard questions on the enforcement of storage and processing rules must be answered. What malicious code protection software will be used and how will it be employed? How will that protective software be kept current? Who will ensure up-to-date protection measures are applied? All of these issues must afford the protection required and still fit into the workplace culture.

Another consideration is that multilayer security not only becomes recommended but mandatory. Without it we really have no security at all. The major virus protection product manufacturers have already produced virus protection software to check for known viruses being transferred between the PDA and the desktop.[10] Of course this only works if we know of every instance where a PDA is in use and have a way of enforcing the use of the protection software as stated in the preceding paragraph. The troublesome portion of dealing with this new technology from a security specialist's point of view is the wireless connection capability and growing interface options creating unknown or uncontrolled backdoors into the LAN and the enforcement of whatever policy is enacted. As more and more PDAs are linked via networks, "it opens up the potential for viruses and worms to spread, disguised not just as e-mail attachments, but also in voice messages, MP3 files, video games, interactive maps and other seemingly harmless communications."[11] The threat is exploding right along with the new PDA technology.

The attraction of a PDA is its ability to provide desktop-like functions on the move without the bulk of a laptop. Inherently this means greater amounts of data storage and processing power will be developed quickly. The first Trojan horse for Palm Pilots had the potential to destroy all programs contained on the Palm Pilot.[12] Not exactly benign code. Before the important notes and priceless data an official has just entered into a PDA during an important meeting can be downloaded into a PC would not be the time to discover the next piece of malicious code.

[10] Shankland.
[11] Fortt, Jon. "Viruses threaten to evolve beyond PCs." 1 September 2000. URL: http://www.mercurycenter.com/premium/front/docs/palmvirus01.htm (7 September 2000)
[12] Creed, Adam. "First Palm Pilot Trojan Found in The Wild." 29 Aug 2000. URL: http://www.nbnn.com/pubNews/00/154341.html (7 September 2000)

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event