Global Information Assurance Certification Paper

Pocket PC – Secure or Unsecured?

INTRODUCTION

Handheld computers have been on the market for a couple of decades. One of the first attempts at a handheld computer was the Apple Newton which didn't take off commercially but had many features that today's Personal Digital Assistants (PDAs) use extensively. Many attempts at a commercially viable PDA have been attempted over the years but never really appealed to a mass market until the introduction of the Palm Pilot during the mid 90's. This device wrapped in a light weight shell offered small size and a lower price tag. Soon many business people were organizing their lives with this simple device. The primary functionality, that of a glorified personal planner, has not changed much since its introduction but many developers have created ingenious software and games to enable it to do so much more. It is built on a platform with a less than powerful processor and exceeds little more than 8 megabytes of memory.

Shortly after the Palm began to attract a mass audience, Microsoft introduced Windows CE and a lineup of hardware manufacturers to produce devices built on this platform. This initial attempt by Microsoft was never really able to get off the ground. Despite offering greater functionality and a more powerful handheld, people were not ready to do much more with a PDA than the Palm could do also. With a price tag that was 2 to 3 times more than the Palm PDA, these devices never really took off. But Microsoft was not done. In 1999 they retooled the CE OS by making it more stable and taking out features consumers did not like. They added other features such as MP3 players and eBook readers that consumers desired without giving up performance or size. The hardware manufacturers jumped back in line and soon Compaq and HP were spitting out handhelds that were more stable and better designed. These devices were more expensive than the Palm, but the added features were enough to convince consumers it was worth the extra price.

The Rise of Security Concerns

With the added functionality and the introduction of a Windows code base, corporations now found PDAs a useful device for increasing productivity. With this increased use in the corporate domain came new reasons to be concerned about security of the data stored on these devices.

The first reason that security professionals should be concerned with the security of these devices can be summed up by the hacker Radwork who, "believes that as smart devices come into general use, they will definitely be hit with various plagues" (Yahoo Finance).

Increased functionality and means of communicating also provides a platform to launch new attacks on technology. This is borne out through numerous historical examples such as the PC with its floppy drives and the Internet with its ubiquitous connections to millions of people around the world. The Microsoft code base that stresses functionality over security and stability is just another example. "As the functionality in handheld applications increases and as these machines become more

and more popular, the 'critical mass' required for wide-spread virus infections to take place also approaches with alarming speed. Handheld machines also continue to become more 'connected' with full featured Web browsers, email clients and also WAP [Wireless Application Protocol] support" (Yahoo News, 2). Much like the advent of Windows 95 to the desktop, PocketPC has done to the handheld.

The double whammy of widespread use and the added functionality of Microsoft operating systems is summed up in the following statement. "Think for a moment about the information that your handheld contains. Names, telephone numbers, email addresses, etc. This is all information that virus writers relish the thought of obtaining and using. Add to this the APIs that companies such as Microsoft have provided to allow applications to access and manipulate this information freely and you have the recipe for a digital disaster" (Yahoo News, 3).

As we begin to dive into more detail specifics of Pocket PC consider the fact that reports of viruses on handheld and mobile devices are already beginning to surface. "In fact, we've already had reports of the first worm that uses mobile phones as a mechanism for spreading – It's called VBS Timofonica" (Yahoo News, 4).

INHERENT PDA SECURITY FLAWS

It is not my intent to pick on PDAs and it is important to remember that "any system that involves memory and intelligence can be a target for a hacker" (Yahoo Finance). The Personal Digital Assistant, because of its purpose of providing on the go business people with all pertinent information in a small compact easy to use device, has inherent security vulnerabilities. These vulnerabilities stem from two major pieces of functionality that all PDAs have, small size (physical) and an always-on communications capability with infrared ports (logical).

Physical Access

"The Handheld PC's main strength is also a security weakness. It's small and goes with you wherever you go. It easily slips in and out of your pocket, and can just as easily be left behind" (Windows CE Webring). This statement sums up a major risk with using a PDA in that information stored on these can easily fall into the hands of a competitor or the hands of dishonest people who may decide to use the information against the individual or organization to which it belongs. This is why logical access controls, discussed later in the paper, is paramount to protecting the information stored on PDAs.

Logical Access

Most PDAs have always-on infrared ports, which can be accessed and used to transmit data and files. This presents yet another means for a competitor to gain access to your information, especially as more and more organizations begin to build

direct links between PDAs and corporate data centers and intranets.

As communication channels increase so to does the threat of viruses. Much like the floppy drive, networks and eventually the Internet lead to an exponential increase in virus activity among PCs the infrared port will provide the platform for virus increases among PDAs. "The popular beaming feature on Palms, which allows people to send and receive information via an infrared port, is one means of spreading viruses. And handheld computers are increasingly offering wireless internet access, which means that viruses may be even easier to spread" (Miles). An inkling of what the future may hold for virus activity among PDAs has already begun to filter through the press with a few reports of viruses among Palm's OS including Phage-936 and the Liberty Trojan Horse. Anti-virus software makers such as Norton and McAfee have also begun to create software for the Palm and CE platforms. "With such major player[s] in the PC security market now expanding into the handheld arena it's clear that the possibility of virus infections on a handheld is not as remote as was once thought" (Yahoo News).

POCKET PC SPECIFIC SECURITY AND FLAWS

As you can see PDAs are inherently vulnerable to attacks or loss of privacy but the newest entrant to the PDA market, Microsoft's Pocket PC (formerly Windows CE) brings extra vulnerabilities to the table. As I mentioned earlier in the introduction the Microsoft code base stresses functionality over security and stability and thus presents many back doors for attackers to perpetrate handheld devices. This message is reinforced in a recent Yahoo article, "The problem centers on software developers who continue to concentrate on building easy-use features into these devices instead of making sure that they are secure" (Yahoo Finance). This presents a cause for concern but other vulnerabilities are also notable.

A good example where functionality won out over security is in Pocket PC's auto finish feature that suggests words based on the characters entered on the emulated keyboard. Published reports tell of Win CE 2.1, the precursor to Pocket PC, showing the words which first characters match your password's first characters.

"Microsoft uses a trust model, relying on individual users to set their own limits. But many users are not informed about security issues and leave their MS programs set to the very trusting default" (Yahoo Finance). These trusting defaults are usually published early on hacker web sites and chat rooms while those using the devices are usually naive to the possible exploit and unsuspecting of any vulnerability.

One example of an option that must be enabled that could provide a level of security for Microsoft devices is the power-up password. "Pocket PC provides a power-up password, and a third-party network management system can be used to prevent someone from connecting to the corporate network unless the power on password is enabled on the device. Palm requires you to go to a setup screen and enable password protection" (Shier, 1). As an astute observer of the Microsoft OS notes in a

chat room, these passwords can be seen as 100% fool proof. "There is a major lack of security with these devices but using a power on password is certainly not going to help. If someone really wanted to get the data off the device they could do it by pulling the data directly off the embedded chips, or much simpler, eject the CF/PC Card/ MMC card and place it into another machine" (Howardhh).

The reader shouldn't get the impression that Microsoft devices are completely wide-open to would-be attackers. Several security features to protect browser-based communications through Pocket Internet Explorer are built in that should be mentioned. "Most importantly, the browser supports secure connections (SSL) that allow the user to send and receive private data" (Shier, 2). "It also supports the Private Communications Technology transaction protocols, 40- and 128-bit encryption and the Microsoft CryptoAPI 1.0" (Yasin, 1).

Despite these features some still feel that other operating systems offer superior means for protecting data. "Palm employs cryptography that may be better suited for smaller devices. Palm uses Elliptic Curve Cryptography technology from Certicom Corp. which provides higher levels of security at smaller key sizes than other public key systems" (Yasin, 2). This is however a mute point as Pocket PC devices have much faster processors and more memory which lends itself to the more robust cryptographic schemes such as SSL. Or is it a mute point? Jeff Zamora in the CEGadgets.com article "ActiveSync 2.x Allows Unauthorized Access to Your NT Password" published an easy crack of one of CE's features. Older versions of Win CE had the ability to store your Win 95/98/NT passwords to allow users to transfer information easily. The storage of this password is in a registry key that is encrypted using an XOR scheme based on Pegasus, code name of the first generation of Windows CE, spelled backwards. As a refresher XOR schemes are considered by many to be weak unless used with very large key sizes.

REMEDIES

Despite the many pitfalls that can befall PDA users, the devices can be secured on many fronts. The first, most cost-effective way to secure your device is to keep it close to the vest. "Your handheld PC should be with you at all times, in a coat pocket, unless you're at home or sitting down at your desk in the office. Then you should put it in the same place. The trick is to not set it down in an unusual place, and to always put it back in your pocket when you're finished" (Windows CE Webring). Some firms are now making locks for PDAs. This would appear tough considering PDAs don't have a hole built into the casing for a lock like notebook computers do, but a great example of innovative design comes from Kensington's stylus-based PDA lock. This product is a six foot galvanized steel cable that anchors PDAs to an immovable object.

Another simple, fundamental step that can be taken to secure your PDA involves

setting corporate policies to protect PDAs and corporate information. "Company policies are a good idea, especially when it comes to connected '3rd party' devices" (Howardhh).

The onus is on corporate IT departments to select the technologies which will integrate PDAs into the organization without sacrificing security. Companies that fail to do so warns Stephanie Miles, "risk infection from employees who use their own handhelds and then sychronize them with corporate PCs." One means to this end is purchasing the appropriate hardware and software to standardize communications and synchronization. "Recommend specific products in order to discourage operating system proliferation. Select portal software for handhelds so that access to corporate information resources and intranets is coordinated and made secure" (Keen). Gartner analyst Ken Dulaney believes, "corporations must take responsibility for all the devices their employees use, including personal digital assitants, cell phones and PCs" (Miles).

Users should actively seek out training and corporations should encourage training on mobile devices to ensure users know the above vulnerabilities. "Even simple PDAs require training when they're used to access corporate data, sync to Microsoft Exchange and connect to the corporate Intranet" (Keen). This training should also include best practices for users to ensure against data loss and potential lost productivity. Examples would include synchronizing data between PDAs and corporate computers to ensure a back up copy is always up to date in the event of a necessary hard reboot. Training will more than likely need to be developed in house but as PDAs become even more prevalent some adult education facilities are beginning to offer classes on proper use of PDA technology.

Software is also increasingly available to provide extra protection of logical security in PDAs by providing classifications for data, extra encryption (as much as 128 bits) of passwords and monitors for malicious code being uploaded from PDAs to PCs. Other features that are available include disablement of transfer mechanisms after a certain number of invalid login attempts and destroys all RAM data. Some software have planted logic bombs that explode rendering the device useless when it falls into the hands of users with malicious intent. Some common examples of vendors developing software in this arena include PDABomb, PGP and McAfee. This software should be explored as possible extra protection against areas of concern for any organization hoping to increase their defenses.

A recent Yahoo article provides a great summary for protecting PDA devices on multiple fronts. "Raise those shields, keep the home firewalls burning, and make sure your intelligent devices are smart enough not to trust incoming external data" (Yahoo Finance).

WORKS CITED

Howardhh. http://www.pocketpcpassion.com/ubb/Forum6/HTML/000053.html. "Security

Warning?"

Keen, Peter G.W. "Embracing the PDA." *Computerworld*. 16 April 2001. Pg 36.

Miles, Stephanie. "First Palm virus raises questions about security." *CNET News.com*. http://news.cnet.com/news/0-1006-200-2839323.html?tag=rltdnws. 7/5/01.

Miles, Stephanie. "Trojan horse rears its head on Palms." *CNET News.com*. http://news.cnet.com/news/0-1006-200-2839323.html?tag=rltdnws. 7/5/01.

Shier, David. "Pocket PC: The Right Choice for the Enterprise." http://www.pocketpcmag.com/may00/enterprise.htm. 6/21/01.

Windows CE Webring. "Always put your H/PC back in your pocket." http://www.pocketpcmag.com/Jan/quick9.htm.

Yahoo Finance. "Are PDAs Next for Viruses?." http://www.palmsizepc.com/may2000-16-1.html. 6/21/01.

Yahoo News. "Is that a Virus in Your Pocket?" http://www.palmsizepc.com/july2000-27-1.html. 6/21/01.

Yasin, Rutrell. "Pocket PC Secured for E-Biz." *InternetWeek.* http://content.techweb.com/se/directlink.cgi?INW20000501S0034. 6/21/01.

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