GWI Presents

PDA Viruses - The New Frontier

Rocky Heckman

Table of Contents

Table Of Figures

1 Introduction

The world is going mobile. With that, the Personal Digital Assistant (PDA) or handheld is becoming part of our everyday lives and their use is growing [3]. These new gadgets, that all power-tie wearing business professionals are running their lives with, opens up a new world of opportunities for malicious hackers. The more people use PDAs for appointment tracking, storing personal information, saving meeting notes and critical decisions, and storing bank account details the more hackers want to see what's on them. Recently the first PDA targeted virus was found in the wild.

This new virus named Brador [2],[9], and [10], is the first to openly attack PDAs running Microsoft Windows CE. Windows CE is the core operating system under Pocket PC. The virus is delivered through email or downloaded from a web site much like common desktop viruses. The virus creates a svchost.exe file in the Windows autorun folder and opens up the PDA to the attacker on the next re-boot. Once the PDA has been compromised it emails the attacker the current IP address of the PDA. Once the attacker has the PDAs IP address, he connects back to the PDA and has complete unrestricted access to any information stored on it.

What makes this so serious other than the fact that all the sensitive information stored on the PDA now belongs to the attacker, is that there is little defense against it. PDA based operating systems are far less secure than their desktop and server counterparts. Anti-virus software is available for PDAs but there is no consistent way to keep it updated. PDA viruses are not all that common yet so AV companies don't have a tool or system for regularly updating the virus definitions for the PDA systems.

A further danger of the threat of viruses on PDAs goes beyond the PDA itself. These PDAs are normally synchronized with corporate LAN connected desktop machines. A creative virus writer could distribute his new virus through PDA synchronization. This new virus could be distributed to thousands of corporate LAN attached computers before activating itself. It completely bypasses the corporate gateway virus scanners. The PDA is possibly exposed to viruses and synchronized with corporate computers before the AV software on the local machine has been updated with the new virus signatures. Desktop AV signature updates traditionally lag behind corporate gateway updates due to the logistics involved and corporate policy dictating that the test machines then gateway machines get updated and checked for stability before distributing patches to the whole network.

This is the dawn of a new era in virus technology, and virus targets. The more critical information that is kept on PDAs, the more the bad guys will want to see what's on it.

2 The PDA Environment

This report will focus on Wi-Fi access and the Pocket PC operating system and how viruses will affect the PDA environment.

The PDA based operating systems that are in common use today are essentially scaled down versions of common Windows operating systems such as Windows CE / Pocket PC or custom ones built specifically for use on PDAs such as the Palm OS. There are Linux distributions that have been designed for PDA use such as Familiar which is based on the Debian distribution. The Linux based PDA Operating Systems (OSes) are in their infancy and not yet usable by the common public.

The fact that these OSes are scaled down for the small memory environment of the PDA means that essential security systems have been trimmed down considerably. In the PDA market usability is still the key driving factor. Until recently there was little threat to the PDA from viruses or malicious hackers. In fact in 2001 protection from PDA viruses was reported as "superfluous handled antivirus applications" in [1]. This is starting to change.

PDA's are becoming the office tool of the future and are even standard issue at some companies like Intel[4]. They are almost all Bluetooth and wireless LAN enabled. They are used as combination phone, Personal Information Manager, note takers, presentation managers, Global Positioning Systems and even cameras. Connected sales or corporate executives are relying on the PDA more and more as all their appointments, meeting notes, meeting presentations and personal information such as banking details are held on their PDAs.

The information is stored with minimal encryption, and few authentication security measures. They appear secure with their fingerprint scanners and passwords but these measures are easily bypassed. This report is not a discussion on how to break in to PDA's but suffice it to say that it is possible to connect to a modern PDA with a serial cable, use a terminal program to upload a new boot loader and instantly have access to the entire system bypassing the security features[1].

Most modern PDAs are Wireless LAN (WLAN) enabled, or can easily be expanded to use WLANs. This allows them to connect to the Internet to access online mail, corporate networks and the latest stock prices from popular web sites. Several modern coffee shop chains have installed WLAN access points to provide customers access to the Internet from whatever device they have while they enjoy their Skinny Decaf Hazelnut Latte's. With a connected world, the PDA has been opened up to the prying eyes of anyone within radio distance.

The security mechanisms are included in the OS to secure the WLAN. There are also freely downloadable tools (see section 6 PDA Protection Products) available to install anti-virus software and firewalls on a PDA. The general public just is not aware of them yet. The mindset in dealing with the PDA is that they are small devices that fit in a pocket. They aren't plugged in to a network cable therefore hackers can't possibly get in. It's not a "PC" so it doesn't have viruses. People are slowly learning this is not the case.

Most of the security mechanisms in place for PDA's are single facing facades. Most people don't think of their PDA with the same security precepts in mind as they do their desktop computer. They don't bother setting up strong passwords because it's too much hassle to enter them. They forget to scan emails for viruses, and install firewalls on their PDA. Do to these factors it is easier to get in the backdoor of a PDA. The Brador virus demonstrates this.

2.1 The PDA Operating Systems

PDA operating systems have only recently become the nice 'Windows like' experience they are today. Essentially they are scaled down versions of desktop equivalents. They have been trimmed down to fit into the small memory space available on the PDA. Normally the first things to go when these OSes are scaled down are the robust security features.

[1] Based on the experience and research of the author using an HP iPAQ h5550 running Pocket PC 2003.

A PDA has to be usable and offer a lot of functionality to the user in order to make it in the market. They are normally sold with an OS that is an all-in-one system much like Pocket PC. In order to pack all the features of spreadsheets, word processors, internet browsing, email, scheduling, and the plethora of time tracking and expense report tools out there, sacrifices must be made.

The security mechanisms that are left in the system have been neutered to the point of being single line of defense. They stop people from accessing the touch-screen if they do not authenticate themselves correctly. PDA's do not have an equivalent of the 'secure attention sequence' (CTRL-ALT-DEL), which controls logging on and off a computer. The 'suspend' functionality is as close as it gets. Even then, the system comes with a default of not asking for a password on waking. This is not necessarily the case with the Palm OS and the newer Blackberry.

This allows an attacker to be able to get into the system simply by getting a Trojan behind the login screen. If that can be accomplished, there are no further barriers to the system. There is no concept of file level security in the PDA. There is no multi-user concept which would allow folder or user directory security that comes with most desktop OSes by default. The WLAN connections are in promiscuous mode and unsecured by default. This is to allow them to sniff out and log in to WLAN access points as the user roams around the city. The Bluetooth communications by comparison normally asks permission when someone tried to access the PDA. The default installation of Pocket PC wireless network communication does not.

In a lot of the modern PDA OSes the WLAN communications security mechanisms are as strong as most wired ones. They employ WEP, WPA, and even 802.1X and some are poised for the upcoming 802.1i. However, if a virus is slipped through the email, or these measures are not in place, the PDA is still vulnerable.

A benefit that the PDA has is natural 'security by obscurity'. The microprocessors that run these devices are very different than standard x86 Intel or AMD architectures. The MIPS and ARM (StrongARM) processors will not run standard x86 based programs out-of-the-box. Therefore they are not susceptible to common viruses that are targeted at desktop systems. Common stack-smashing buffer overruns, format string attacks and other common hacking measures are as of yet unheard of on these processors. While these attacks are not common to PDAs yet, it is probably only a matter of time before they are exploited as well. The smaller instruction set of the ARM processors [12] may make the applications designed for them easier to reverse engineer and find bugs in.

One of the major drawbacks to the OS as installed on handhelds is that all the addresses of every function, class, object and driver are easily obtainable. The way that handheld OSes work is by loading the Read Only Memory (ROM) section with the OS code. The entire OS is loaded into fixed memory locations that are identical on all products from the same manufacturer. For example the loaded ROM for all HP iPAQ h5550 handhelds will be the same. When an OS is loaded onto a PDA each instruction is mapped into memory addresses in ROM. This can be observed by using a terminal program to upload an OS into the PDA ROM[2].

There is a structure that is available from usermode called KDataStruct which contains a pointer to a list of module structures according to [7]. This provides the

[2] As observed by the author during research into Linux based OSes for the PDA and restoring Pocket PC 2003 using this technique.

ability to locate any structure the virus might need to perform its work. The ARM ISA generates position independent code and methods to support it so knowing the exact address of a file or function isn't required before the virus executes. In desktop systems, libraries are loaded dynamically at runtime and may be loaded at different addresses each time. This makes writing viral code to hook function calls, or change memory addressed much more difficult because it has to guess to calculate the current address of the vulnerable program or the function it requires to perform its work.

The Windows CE based Pocket PC operating system still uses the Windows Portable Executable (WinPE) file format for executables. The compiled instructions are different to that of a desktop WinPE file, the file format and basic headers are the roughly the same. This gives a virus writer with knowledge of the Windows PE format an advantage when knowing where to inject their viral code and how to do it. It is quite possible that existing Windows PE infection algorithms can be modified and compiled for ARM/MIPS processors with minimal effort. Fortunately there has not been a lot of activity in this area.

This was the case until the Brador virus surfaced and opened up a new avenue for attacking handheld devices. As the handheld operating systems begin to share libraries and software architectures with desktop machines, they too will become susceptible to viruses that target OS level mechanisms. Executable files on the PDAs are quite different to desktop ones at the low level but still share many of the same file formats such as WinPE format mentioned above. The low level processor instructions are different as well. So direct low level attacks are still relatively unknown territory.

The files themselves are still written with C++ or .NET languages. Being able to replace them with common C++ or .NET based malicious versions is still possible.

2.2 The Current Defensive State

The current defenses of the PDA are limited to touch-screen lockouts, and the various wireless security protocols mentioned previously. There are virus scanners available for the PDA OSes but they are still in their infancy. They have problems when it comes to updating the virus definitions on a regular basis. Thankfully, there are not very many viruses to have definitions for yet.

There are a several PDA security products on the market. The majority of them have to do with screen lockouts and encrypting the data on the PDA. What people should be considering though are PDA Antivirus Scanners, PDA firewalls and intrusion detection systems.

PDA Antivirus (AV) scanners are not all that uncommon. Symantec, F-Secure and Airscanner all make good AV scanners for the Pocket PC. These scanners can be updated from a host sync PC or through the wireless networking in the PDA.

There are several firewall products for PDAs as well. Companies like Airscanner and Bluefire provide firewalls for Pocket PC devices. These are quite robust application and protocol/port level firewalls that can prevent unwanted browsing of your PDA. A note of caution on the Airscanner Mobile Firewall. There are three 'zones' that can be set for the firewall, 'Trust All', 'Cautious', and 'Trust No One'. While 'Cautious' appears to be a level between 'Trust All' and 'Trust No One', the default settings are to allow all protocols and ports.

The ‘Trust All’ setting allows everything and there are no choices available to turn of specific services. The ‘Cautious’ settings gives the user the choice to turn off certain services (i.e. SSH In/Out/TCP(22)), but they are all enabled by default which doesn’t provide any better security than the ‘Trust All’ setting. It is advisable that if the Cautious setting is used that the user specifically disables all but the needed services and protocol/port combinations.

When these products are combined with wireless security in the form of WEP or WPA, 802.1x, and soon 802.1i a PDA can be quite secure and safe from wandering marauders. However all of these protection measures have to be turned on. The PDA OSes are still in an ‘open by default’ state unlike current PC OSes which have learned to be locked down by default.

3 Analysis

3.1 PDA Virus Found in the Wild

3.1.1 Introduction to Brador

The Brador virus was the first Trojan found in the wild that specifically targeted Pocket PC. When the 5632 byte Trojan was discovered it was dubbed Backdoor.Brador.A by Symantec [9] and Backdoor.WinCE.Brador.a by Kaspersky [10] Labs. Because of its small footprint, it is easily downloadable onto a PDA. 5.6K files are not a big deal on modern PDAs.

The Kaspersky article [10] had this to say from one of Kaspersky’s researchers:

> *"We were certain that a viable malicious program for PDAs would appear soon after the first proof of concept viruses emerged for mobile phones and Windows Mobile", commented Eugene Kaspersky, Head of Anti-Virus Research at Kaspersky Labs, "WinCE.Brador.a is a full-scale malicious program ready to go: unlike proof of concept malware, Brador has a complete set of destructive functions typical for backdoors."* [10]

3.1.2 Origins of the Technology

The Brador virus is actually based on some proof of concept (POC) work done by Ratter of the hacking group 29a called WinCE4.Dust [5],[7]. This was the first virus to actually infect executables designed for the ARM processor. While the virus was not destructive it did prove that ARM executables could be infected.

Ratter summarised the items he had to overcome to modify a virus to run on the WinCE / Pocket PC system as opposed to the traditional Win32 (Windows 95+) systems [7].

- Absence of image headers at the start of loaded image on WinCE
- No awareness of the current directory on WinCE
- The need to call Create FileForMapping on WinCE
- WinCE is Unicode only
- Absence of DIV instruction in ARM ISA
- Automatic generation of position-independent code with armasm

Considering the dramatic differences between the two platforms, this list is not very long. Now that the ground work for making this change has occurred, the way is open for new PDA viruses to start surfacing.

The Dust virus was written much like any other virus [7]. It was written in assembler for the Pocket PC OS. It used the trimmed down instruction set of the ARM processor [12] and some traditional virus techniques modified for the ARM / Pocket PC environment. Compiled with utilities freely available over the Internet, it is the pattern for future viruses targeted at the Pocket PC market.

According to [5] the Dust virus checks to be sure that the file is writeable. If it is not it may indicate that the particular file may be in use at the time the virus acts. It then checks various portions of the Windows PE file format to ensure that the file is actually an executable file. It then checks for previous infection by looking at the offset 0x11C for the word ATAR which is placed there when the file is infected.

Once these tests are passed the 1,536 byte payload code is appended to the file. Then the virus changed the PE header point to the virus code located at the end of the file so this code is executed when the file is executed. Finally it writes the ATAR tag at offset 0x11C. After the virus has infected all the executable files in the root folder it calculates the correct starting address for the file the virus is executing from. It then redirects the program execution to this location which allows the infected program to operate normally from that point.

The WinCE4.Dust virus is even polite enough to ask the user's permission to infect the .exe files in the root directory of the handheld device. It also restricts itself to only those files in the root folder. This is more by mistake than design as mentioned by Ratter in [7]. The Dust virus only infects files in the root folder due to the lack of current directory awareness in Pocket PC as mentioned above. So it just heads straight for the root and infects all files there. It didn't need to be destructive to make a significant point.

3.1.3 The Malicious Changes

The Brador virus is not nearly as considerate. According to [9], and [10], once Brador runs, it creates a svchost.exe file in the Windows autorun (Startup) folder on ARM compatible PDAs. When the PDA re-starts that copy of the svchost.exe is loaded and the Trojan is active. Brador emails the attacker the current IP address of the PDA. Finally it opens port 2989 and awaits further commands. The attacker can then make a connection to the PDA where the Trojan is waiting to answer. Once the attacker connects to the PDA through the Trojan, he has complete access to the files on the PDA. This even extends to the ability to upload other files or tools to the PDA.

Uploading other tools to the PDA could include more vicious viruses or tools which would allow the attacker to hijack the data on the PDA and extort money from the user. This would be the case if the attacker uploaded a crypto-virus [11] which encrypts data on a target system using public key cryptography. The attacker then forces the victim to hand over that data in return for a key to decrypt it. This gives the attacker access to any sensitive information they can get to.

3.1.4 The Impact

Because of the limited antivirus support, at the time the Brador virus was discovered in the wild, the recommendation from Symantec for removing it was to delete the infected file. In the case of Brador this is not a major problem because it creates a file that is not installed by default and has no dependencies.

If the virus was to infect primary OS files, and the AV software was not able clean the file the effect would be much worse. Previously a problem like this would require a complete restore of the PDA. Most users synchronize their data but don't often perform full PDA backups. In this case an unrepairable infection of a primary OS file would require a re-install of the OS on the PDA in order to recover a good file.

Reinstalling the Pocket PC operating system is not a trivial task. The nature of the PDA architecture makes changing the OS in the ROM a potentially fatal operation for the PDA. If the OS or more specifically the boot loader is corrupted on install, the PDA will be in an unbootable state. This state is often referred to as 'bricked' because of its nice brick-like usefulness at that point. The only way to repair it from a bricked state is to return it to the manufacturer for a reinstall of the boot loader and OS. If the PDA is not under warranty, this can be a costly process to the user.

Fortunately, PDA viruses are not as adaptable as desktop based ones. The very nature of the PDA makes applications that run on one environment not likely to run on another. For example viruses written to run on ARM processors won't work on a MIPS processor. A virus written to run on Pocket PC won't work on Palm OS, Familiar, or any other PDA based OS that it wasn't specifically written for. The more the industry standardizes on handheld device operating systems and APIs, the less of a comfort this will be.

The other side of the coin is that the closer PDA operating systems get to desktop operating systems, the more likely we are to see cross-platform viruses appear. At this point in time it is feasible that a virus targeting the .NET Framework would work on both desktops and PDAs. The .NET Framework is similar to the Java Runtime in that code written to take advantage of it can be run on any platform that supports it.

Fortunately there are several security measures in place that can mitigate this such as Code Access Security and Strong Naming of assemblies [16]. These security measures have to be used to be effective. Often Code Access Security is overlooked because most applications run in an environment where Active Directory or some other authentication mechanism is used.

This becomes the authentication mechanism of choice. In a PDA based application, this is often not the case. The only authentication available is the local password. Code Access Security is based on the various 'trusted zones' such as Internet, Intranet and Local. Enforcing this restriction in .NET based PDA applications can prevent critical files from being attacked by viral code from the Internet.

Any file that is downloaded to the local PDA and executed is still considered in the 'local trusted zone'. This means that the protection falls back to whatever the user is allowed to do. In most cases, the one and only registered user on a PDA is the PDA Admin and has unrestricted access to the PDA. There is no defence against a user with Admin access on any OS on any platform. Applications running under their control can do anything.

3.2 How Viruses Get In

The Brador virus was spread by email. It is presumed that the coder of Brador was Russian as it was sent in an email with Russian text [10]. Once a user executes the attached file, the PDA is infected. This is a familiar situation to desktop users. Viruses have been spread through email for a long time.

The most common inroad for viruses on PDAs is the same as the one for desktops. Email and downloaded files are the delivery mechanism of choice. Often users are tricked into opening attachments in emails or downloading infected files. PDA applications are very popular downloads now.

Without adequate anti-virus and firewall protection on the PDA a virus can get to the machine. Once a file has infected the PDA, it can easily spread to other PDAs that may share a common data store or shared file area on the synchronized network. The PDA needs to be treated with the same care as any desktop system when it comes to defending against malicious code.

3.3 How to Prevent Infections

The same rules apply to PDAs as to desktops.

- Install firewall and virus scanning systems on the PDA
- Do not run attachments that are not from trusted sources
- Do not run downloaded files that are not from trusted sources
- Do not run any downloaded file without scanning it for viruses
- Keep the virus definitions up to date
- Keep patches up to date
- Back up the data and the OS ROM on the PDA regularly

With AV and firewall software becoming more readily available for PDAs there is little reason not to have it. Airscanner's AV software and firewall are free for personal use. They install easily and do a good job of protecting the PDA.

Some of the more common desktop anti-virus scanners are picking up PDA viruses now as well. Symantec and Kaspersky labs have specific entries for the Brador virus [9], [10] and are actively watching the PDA market now.

4 Recommendations

4.1 Hardening PDAs

The PDA OSes need to make room for the security features of their desktop equivalents. PDAs need to be treated with the same concern as laptops. One of the very first things that should be done on a PDA is to enable the password protection and use a complex password.

Laura Taylor in [13] lists several things in addition to strong passwords that can be done to prevent a PDA from being an open book. In several cases the open-by-default nature of the wireless LAN on PDAs has exposed data to un-authenticated users. This is a good reason to make sure that the passwords on the PDA are as enabled and as secure and complex as any desktop password. It's also a good idea to not make it the same as the desktop password. While password entry on a PDA is cumbersome, it's sure easier than re-installing the OS or facing the potential impact of financial loss or identity theft.

Use data encryption if the data is of any importance. As stated in [13] how important is the data really? How important are client names and phone numbers? How important is a personal schedule that lists meetings with potential clients and details of closing deals? How important are the meeting notes that list sales figures, and upcoming development plans? This kind of data could make or break a company. It should be treated with the same security concerns as data on the corporate LAN.

If sensitive data or highly classified data is stored on the PDA, install bit wiping software [13]. This is the ultimate in data protection at this time. If an incorrect password is entered too many times, or the PDA has not been synchronized with the secure Corporate LAN recently enough, the data will be completely wiped in case the

PDA has been lost or stolen. While this is not for everyone, if the data is critical and the PDA is lost, this kind of tool may be essential to protect sensitive data.

PDAs by their nature are in an ‘always on’ state. If the wireless LAN is enabled, the PDA is constantly broadcasting and searching for networks to connect to. In some cases the wireless LAN is on even when the PDA is suspended. This is an invitation to malicious hackers. Make sure that the wireless access is disabled when not in use. There are electronic shielding PDA bags made by a company called. MobileCloak that can help prevent signal leakage.

PDAs should use the security features of the network systems on the device whenever possible. If the network being connected to supports 802.11X, it should be enabled. WEP, while crackable, should still be used as it is far better than no protection at all.

Install firewall software on the PDA. There are many free ones and they are very easy to install and use. A firewall that operates on both incoming and outgoing connections will stop viruses like Brador from being able to complete their tasks. It would prevent it from opening port 2989 and listening for the attacker to connect.

There is a list of some of these tools in Section 4 PDA Protection Products. With tools readily available now from leading vendors and specialist tools from places like Airscanner, there is no reason not to put anti-virus scanners on PDAs. While there are not many PDA viruses now, there will be in the near future.

As PDA viruses get more sophisticated and more prevalent, it will be just as important to keep the PDA AV virus definitions up to date. They should be updated every time the PDA is connected to the Internet, or synchronized with a desktop machine.

PDA antivirus has come a long way but there is still room for improvement. The most difficult hurdle for protecting PDAs from viruses is the virus definition updates. It is easy to schedule an Internet connected desktop computer to poll for virus updates on a regular basis. PDAs are not always connected to the Internet and can not do this. When they do connect they need to check for new definitions. If the definitions are updated from a synchronized PC, there could be other problems. The AV software needs to check for AV definitions before allowing the PDA to synchronize with the PC in order to prevent the PDA from infecting the host computer before it can check itself for viruses. This kind of protection is not in place yet.

There are also several security tools on the market to help fill the gap left by the built in OS security measures. There are firewalls, encryption tools, and network tracking tools. It is wise to protect sensitive data with the encryption tools available. Any data that is on the PDA that would benefit an attacker should be encrypted. PDA data can have high levels of encryption now with added memory and processor speeds.

What goes onto a PDA should also be considered. If the data is not there, it is not in danger. RIMRoad produced an article [17] that listed 10 things not to put on unprotected PDAs being used by employees

1. Network passwords
2. Customer Data
3. Press Releases
4. Credit Card & Account Numbers
5. Financial Data

6. E-Mail
7. Intranet Access
8. Price Lists
9. Employee Information
10. Medical (HIPPA) Information

A good rule of thumb is to not put data on a PDA that could be damaging if it got into the wrong hands. Sometimes this is not feasible due to the nature of what PDAs are used for. In these cases employing security measures are even more critical.

For large organizations, policies need to be established on the acceptable use and management of PDAs. This policy should cover:

- Password enablement and complexity
- What can and can not be stored on the PDA
- AV packages and updating schedules
- Firewall packages and settings
- Encryption levels and usage
- Network enablement and usage
- Synchronization rules
- Mandatory security check-ups

As the tools mature, the threat will be mitigated to some extent. The environment will become much like the desktop environment is today. Until then, a certain level of vigilance is required by connected mobile PDA users.

The following is a list that Laura Taylor produced of security measures to consider for PDAs in one of her articles on PDA Security [14].

- Install a firewall on the handheld that has its rules configured to allow only authorized IP addresses to make connections to the device.
- Disable all HotSync and ActiveSync features when not in use.
- Ensure that password lock-out software is enabled to restrict the number of password guesses.
- Do not store PDA passwords on desktop PCs.
- Install a reputable anti-virus product on your device to prevent propagation of malicious code (viruses, Trojans, and worms).
- Strong third-party authentication (e.g. two-factor authentication) software should be installed to protect them from brute force attacks and password sniffing.
- Any PDAs or smartphones that transmit classified information should have their connections to third-party systems and networks protected by VPNs.
- Handhelds that contain sensitive or classified information should have their data encrypted with keys that are at least 80 bits long.
- Make sure your mobile device is upgraded with the latest security patches.
- Do not use un-trusted Wi-Fi access points (such as those at coffee shops) since they may not have all their security features properly configured.

Some people may consider these ‘common sense’ measures. Obviously there is still a need to remind people of them. The risk of identity theft or exposing critical corporate data is too great.

To further secure the PDA it is possible to eliminate unnecessary features from it that may prove to be security vulnerabilities. For example, Pocket PC comes with MSN

Messenger in the default installation. This is probably not necessary for corporate use and can be removed. Applications like this can create network exposure that is an unnecessary risk.

As with any corporate desktop computer, the applications that get installed on a PDA should be governed by corporate policies if the PDA is used in a corporate environment or used to hold sensitive corporate data. In the personal sector this obviously doesn't apply. Personal users are no less at risk that corporate users are and should take the same level of care with their personal data.

Any applications installed on a PDA should be treated with the same diligence as an application installed on a desktop computer.

- They should only be installed if there is a strong case for doing so
- They should not be installed from unknown or unreliable sources
- They should be scanned for viruses before being installed
- PDA stability should be checked after installing the applications
- Data and the PDA OS should be backed up before installing them

Most users synchronize their PDA with their desktop machine via USB or Serial cable. This is a fast reliable way to synchronize with the PC so there is no need for network or Bluetooth based synchronization. Disabling these potential synchronization problem areas would not reduce the PDAs usability and will eliminate the vulnerabilities such as extra open ports on the PDA which are used for network synchronization.

If roaming users need access to the corporate LAN, ensure that proper VPN mechanisms are in place. These policies and more are enforceable through group policies downloaded to the PDA. The Windows CE environment can support an appropriate selection of group policy settings.

5 Conclusion

It was only a matter of time and interest before viruses started making the rounds of PDA users. There is always someone out there who wants to know what tidbits of interesting data people are carrying in their pockets. It may be as simple as curiosity that drives malicious hackers to try to get that information. It may be that someone is trying to get important corporate data for more nefarious uses.

According to [10] the author of Brador is already putting the source up for sale to the highest bidder. PDAs are considerably easier targets than secure or isolated corporate LANs. There is enough information on them to expose corporate data, and personal information. This information could be used for industrial espionage, or identity theft.

Whatever the reason, the time has arrived that PDA viruses are a real threat. They have graduated from proof of concept to malicious reality. With the introduction of WLANs on PDAs they have been initiated into the cruel world that is the Connected Internet. With the introduction of Brador, PDAs have gotten their first taste of malicious computing.

PDAs have a ways to go before they are as hardened as their desktop equivalents. The OSes need to mature, and the third party applications like AV scanners and firewalls need to be brought to PDA users' attention. The more prevalent PDAs become in the every day world, the more they'll need protecting.

6 PDA Protection Products

This is a list of common PDA security products as adapted from [14]

Product Type	Product Name	Company	URL
Anti-virus, encryption, and authentication solutions	FileCrypto, SSH, Anti-Virus	F-Secure	www.f-secure.com
Anti-virus & logging	Security for PDAs	Kaspersky	www.kaspersky.com
Anti-virus & logging	Anti-virus for Handhelds	Symantec	www.Symantec.com
Database security and authentication	Cradle Robber and ALP	Denton Software	www.dentonsoftware.com
Electromagnetic shielding bag	mCloak	Mobile Cloak	www.mobilecloak.com
Encryption	CCrypt	Freeware Palm	www.freewarepalm.com
Encryption and authentication solutions	Pointsec for Pocket PC, Pointsec for PalmOS	Pointsec	www.pointsec.com
Encryption, password protection, hotsync protection, bit wiping, VPN client	PDA Secure	TrustDigital	www.trustdigital.com
Firewall	Mobile Firewall Plus	Bluefire	www.bluefiresecurity.com
Forensics	PDA Seizure	Paraben	www.paraben-forensics.com
Password enforcement, hotsync security and IrDa port security, bit wiping, database security	PDA Defense / Surewave Mobile Defense	Asynchrony Solutions (JP Mobile)	www.pdadefense.com
VPN	VPN-1 SecureClient	Check Point	www.checkpoint.com
VPN and encryption	MovianCrypt, MovianVPN	Certicom	www.certicom.com
VPN gateways for PDAs	VPN 3000	Cisco	www.cisco.com
Anti-Virus, Firewall, Encryption	Airscanner Mobile Antivirus Airscanner Mobile Encryptor Airscanner Mobile Firewall	Airscanner	www.airscanner.com

Figure 1 PDA Protection Products

7 Bibliography

[1] Lee Schlesinger, *PDA Viruses? Don't buy the FUD.*, ZDNet, 1 April 2001, (20 Oct 2004) http://news.zdnet.com/2100-9595_22-503538.html

[2] Joel Strauch,*PDA Virus Found in the Wild*, PC World, 5 August 2004, (10 August 2004) http://www.pcworld.com/news/article/0,aid,117278,00.asp

[3] Ryan, *EMEA Q1 Mobile Device Marketshare Report*, 20 April 2004, (15 Oct 2004) http://www.palminfocenter.com/view_story.asp?ID=6735

[4] Intel Corporation, *PDAs: Integrating Consumer Technologies into the Work Environment*, 2002, Intel Corporation (10 Oct 2004) http://www.intel.com/business/bss/infrastructure/mobility/pda.pdf

[5] Cyrus Peikari et al., *Details Emerge on the First Windows Mobile Virus (Part 1 of 3)*, informit.com, 3 Sept 2004, (10 Sept 2004) http://www.informit.com/articles/article.asp?p=337069

[6] Cyrus Peikari et al., *Details Emerge on the First Windows Mobile Virus (Part 2 of 3)*, informit.com, 10 Sept 2004, (10 Sept 2004) http://www.informit.com/articles/article.asp?p=337070

[7] Cyrus Peikari et al., *Details Emerge on the First Windows Mobile Virus (Part 3 of 3)*, informit.com, 17 Sept 2004, (21 Sept 2004) http://www.informit.com/articles/article.asp?p=337071

[8] Seth Fogie, *Embedded Reverse Engineering: Cracking Mobile Binaries*, Defcon 11 presentation, 2003, (10 Sept 2004) http://www.airscanner.com/pubs/fogieDC11.pdf

[9] Eric Chien, *Security Response: Backdoor.Brador.A*, Symantec Corp., 10 Aug 2004, (10 Aug 2004) http://securityresponse.symantec.com/avcenter/venc/data/backdoor.brador.a.html

[10] Kaspersky Labs, *PDAs under attack*, Kaspersky, 5 Aug 2004, (10 Aug 2004) http://www.kaspersky.com/news?id=151142122

[11] Adam Young and Moti Yung, *Malicious Cryptography: Exposing Cryptovirology*, ch 1-5, Wiley, 2004, ISBN: 0764549758

[12] ARM, *ARM Instruction Set Quick Reference Card v2.1,* ARM Limited, 2003 (15 Aug 2004) http://www.arm.com/pdfs/QRC0001H_rvct_v2.1_arm.pdf

[13] Laura Taylor, *Learn the Basics of Handheld Security*, RIMRoad, 2 June 2004, (21 Oct 2004) http://www.rimroad.com/articles/2004/6/2004-6-2-Learn-the-Basics.html

[14] Laura Taylor, *Security Basics for PDAs and Handheld PCs*, Small Business Computing.com, 27 Aug 2004, (21 Oct 2004) http://www.smallbusinesscomputing.com/webmaster/article.php/3400641

[15] Laura Taylor, *Handheld Security: Part II - Understand Vulnerabilities*, Small Business Computing.com, 17 Sept 2004, (21 Oct 2004) http://www.smallbusinesscomputing.com/webmaster/article.php/10732_3409311_1

[16] John Paul Muller, *.NET Development Security Solutions* ch. 4, Sybex Inc., 2003, ISBN: 0782142664

[17] Bob Elfanbaum & Mark Dinman, *Top 10 Items You shouldn't Allow on Employee Unprotected PDAs (and what to do about it)*, RIM Road, 9 Feb 2004, (21 Oct 2004) http://www.rimroad.com/articles/2004/2/2004-2-9-The-Top-10.html