Identifying the risk involved in allowing wireless, portable devices into your company.

Sans Security Essentials Practical Assignment
Claire McDonough – version 1.4b, option 1

Table of Contents

INTRODUCTION **3**

THE VULNERABILITIES **3**

RISKY INFORMATION 3

PORTABILITY 4

VIRUSES 4

Liberty Crack Trojan *5*

Phage *6*

Vapor *6*

Timofonica *6*

COMMUNICATION CHANNELS 6

Serial / USB Cable *7*

Infra red *7*

Bluetooth *8*

WLANs – 802.11b *8*

LACK OF AUDITING SOFTWARE 9

THE THREATS **10**

DEFENDING OURSELVES **10**

THE QUESTION OF OWNER SHIP 11

PHYSICAL SECURITY CONTROLS 11

EXTENDING AUTHENTICAT ION REQUIREMENTS 12

DISABLE UNAU THORISED SYNCHRONISING ACTION S 12

ENCRYPT DATA ON THE PDA 12

VIRUS PROTECTION 12

CONCLUSIONS **12**

REFERENCES **13**

Introduction

Defence in depth is a strategy strongly promoted throughout the security community, so to leave a network open at a single point of risk is a situation we all fear and work to avoid. In that context, this paper addresses the risk that small portable devices are leaving our networks open to every day.

Personal Digital Assistants (PDAs), mobile phones, portable email devices like the Blackberry (RIM) device are gaining in their power and application. They are mobile and portable and, as such, are brought outside the scope of traditional security measures like firewalls. In an informal study among non-security conscious colleagues, most people admitted keeping passwords or PINs on their PDA, business sensitive information that they would regret falling into the hands of the competition. With the emergence of wireless communications abilities, issues of securing the methods of communication as well as securing the content also emerge.

Risk is directly related to the level of threat and vulnerability you face. So what are the threats and vulnerabilities facing us through the medium of portable devices and what can we do to defend ourselves against them?

The vulnerabilities

The SANS GSEC course tells us that vulnerability is weakness in your systems or processes that allow a threat to occur. The next few paragraphs examine the latest issue of portable device and illustrate their weaknesses.

Risky information

The additional functionality possible with the latest range of devices, (e.g., their capability to connect to enterprise applications, the additional methods of communication), can unintentionally be turned to a weakness by an unsuspecting user. Users are known to be one of the biggest security weaknesses in any system. As PDAs become ever more powerful and provide additional features and functionality the likelihood of users storing ever more sensitive data on the device increases.

This information can be visible to the user:

- Passwords and PINs,
- Client sensitive information,
- Emails

Users believe that using the basic capability provided on most PDAs to mark items as *private*, only accessible by entering a password, protects the information from unauthorised user. However, later in this document there will be information about how misleading this is. Also many users, who use the basic password protection provided, use the same password on the device as they do on the corporate network. Exposing the network before even connecting to it.

The data stored on portable devices can also be invisible to the user. It is stored in the device without the user being conscious of the risks they are taking when they put the device in danger. For example the following information can be stored on the current issue of PDA:

- Shared encryption keys, e.g., WEP keys
- Known and accepted MAC addresses
- Other authentication and encryption information, e.g., for virtual private network connections to the corporate network

It is the ever-increasing sensitivity of the information being placed on these devices that increases the magnitude of the loss when the devices go missing.

Portability

The portability that is the very attraction of the devices can also be a considerable weakness. Business people like to stay in touch wherever they are and these devices provide a method of supplying just such a service. The scale of the penetration of the portable device into the corporate world is evidence of its wide popularity. Even though the shipment of PDAs dropped nearly 10 percent in 2002 there were still 12.1 million devices sold worldwide.[1]

But short of chaining them to the users' wrists they will be lost and/or stolen at a rapid rate. They are easy to leave behind on the taxi seat, in the hotel or even on the bus. This magnifies the risk of attacks that need physical access to the device being successful. If a malicious user can easily gain access to the device, we must make sure that he/she cannot gain access to the information on the device or use the device to gain unauthorised access to our network.

Viruses

The first virus for the palm device was released on the 21st September 2000. It was called phage and it caused a storm in the security community. Predictions flared for the next year about this new direction that viruses were taking and anti-virus software for all portable devices became available.

However, the predicted eruption of viruses for all types of portable device has not been forthcoming. In all there have been only three pieces of malicious software reported to have been released for the palm device and a so-called cell phone virus which in reality targeted the SMS server on the network that transmits to the cell phones. There have been many threats, like the one posted on the Slovak website (virus.cyberspace.sk) in June 2000 which announced

> `Let's go to work. We are starting Cell Phone Virus Challenge. Any contribution welcomed (the more funny, the better). Deadline has not been set.' *(This page has since been removed from the site.)*[1]

However the lack of a sustained threat has led to articles entitled, "PDA viruses? Don't buy the FUD" from industry sources like zdnet news.[3] In that

[1] "A White Paper on Handheld Device Security." F -Secure Corporation.

article Lee Schlesinger proposes that if all a virus can do is destroy the information on your PDA then it's not that big a deal. All you have to do is reset the device and resync with your PC to be back where you started.

Portable devices, therefore, have a safety net against the corruption of data built into their usage model that gives them an edge, the act of synchronising with a PC. This frequent backup of information is a good start to combating the effects of even the most devastating piece of malicious code. As long as precautions are taken not to transfer a virus to or from the PC in the synchronisation process.

The latest devices, though, can connect to the Internet and email other devices. They can spread a virus in ways that was not previously possible. New weaknesses are being introduced into the portable device model, and security professionals everywhere are awaiting the appearance of the related vulnerabilities.

"There are four common methods of transmission by which a virus could infect a PDA:

- Through infected e-mail when using a PDA over a wired or wireless Internet connection
- When syncing with an infected PC
- Via an infected file transferred from another PDA via infrared (IR)
- By downloading infected files from the Internet" [2]

Below there is a short description of the viruses affecting portable devices that have been documented to date. Though these are not current they serve to illustrate the different ways a PDA can be infected. All of which are still valid on today's issue of device.

Liberty Crack Trojan

The liberty crack Trojan was discovered on the 28th August 2000. Liberty was a piece of software that allowed PalmOS users to run Nintendo Game Boy games and liberty crack claimed to be a crack to turn the freeware version of Liberty software into a full registered version.

How the software came to be released into the public domain is a contentious issue. The co-author of Liberty, Aaron Ardiri, wrote the Trojan software but claimed that it must have been one of the people he trusted with it who released it into the wild. However, anonymous posters on palmstation.com claim that Ardiri released the Trojan himself to seek revenge on those people who run cracked software.

When run, the Trojan attempts to delete all third party applications from the PDA and then reboot it.[5]

[2] Cardoza, P. "Block PDA Viru ses"

Phage

Phage was discovered on the 21st of September 2000. It was the first virus designed for the PalmOS.

> "This virus infected all third-party applications on the PDA device, overwriting the first section in the host .PRC file. When an infected application was run, the screen turned dark grey and the program terminated. New programs copied to the Palm system via infrared transfer executed normally the first time, but ceased to function after the application was closed once.
>
> This virus was spread from one Palm OS device to another when infected files were shared via infrared beaming or installed through a docking station … In order to delete this virus, the user had to delete and re-install all third-party applications. Recovery of information required a hard-reset followed by a hot-sync of the PDA device. However, only backed-up third party applications were restored. Both data and applications not backed up were lost." [3]

Vapor

Vapor was discovered on the 22nd of September 2000. It was another Trojan, not a virus as it is misnamed in many places. It simply removed all third-party applications icons from the launcher window, but it didn't delete the applications themselves. A recovery required a hard reset and a reboot.

Timofonica

Timofonica was marketed as a "cell phone" virus when in actual fact it was simply a clever variant of the good old email virus. It appeared in June 2000. Victims received an email with an exploitative attachment. When the attachment was executed an email was sent to every entry in the victim's address book and an SMS message was sent to random cell phones on the Telefonica network in Spain. The SMS message did not erase any critical information from the phone or cause any damage to the phone's operating system. It didn't spread from phone to phone. It was merely a variant of the Spam we receive every day in our email inbox.

Communication Channels

The latest issue of portable device have four main methods of communicating with other devices:

- Serial / USB cable
- Infra red
- Bluetooth
- WLAN protocols

[3] McAfee.com. "Wireless Security Center Protects Against First Palm Virus and Newly Identified Palm Trojan"

Of these communication channels three are wireless methods of communication, which leave the device open to attack without the need for actual physical access to the device. That doesn't mean, however that attacks via the serial connection can be discounted. Because of the high risk of devices being lost / stolen this method of attack is as dangerous as any of the others.

These paragraphs list a few of the vulnerabilities that have been exposed and discussed in the security community relating to each of these interfaces.

Serial / USB Cable

In January 2001, @Stake released information about a debugging process that it was possible to initiate on a device running PalmOS. Physical access to the device was needed to exploit this vulnerability. Entering a short Graffiti keystroke combination on the device enters the debugging interface. The device then monitors the serial port for communication. This backdoor can be entered even if the lockout functionality on the device has been activated, belying the widely held belief that placing the device in lockout mode protected it from unauthorised access.

The debugging interface allows an unauthorised user to perform a number of commands including

- Retrieving an encoded version of the password which can then be decoded,
- Obtaining all database and record information on the device
- Installing and / or deleting applications.[12][15]

A soft reset will exit debug mode leaving no evidence of use. This can allow a malicious user to place a key logger or other piece of software onto the device and place it back into the hands of the user. At a later stage the attacker could regain access to the device and also to all of the information input to the device in the meantime.

Infra red

In September 2000, @Stake released information about a vulnerability in the protocols used during the Hotsync process, exposed by the ability to fool a PDA running the PalmOS into believing that another PDA running the software Notsync was in fact a PC initiating a synchronisation process. Communicating via the infrared port, the malicious PDA could gain access to an encoded form of the password from the victim PDA and determine the password due to a weak reversible encoding scheme.

The password is used to protect information that the user has marked as "private". Private records often contain passwords to other systems, financial data and company confidential information because users are misled into believing that this information cannot be accessed by an unauthorised user. [13][14]

Bluetooth

The Bluetooth specification has taken security issues into account. It defines security measures for devices, services and modes. There are security entities defined in the specification simply to aid in secure communication over the Bluetooth protocol.

However, there are weaknesses in the security settings for Bluetooth, particularly in the following areas:

- **Key generation:**

  The initialisation key, which is used during session establishment and for authentication purposes, is generated using among other things a personal identification number (PIN). The PIN can be merely four (4) digits in length. This leaves just 10,000 different possibilities and given the fact that the user can chose the PIN makes the likelihood of it remaining at the default '0000' quite high.

- **Key management**

  Authentication and encryption are based upon a shared secret. If two devices A and B are communicating and choose A's unit key as their shared secret and at a later time A and C are communicating and also choose A's unit key as their shared secret, B can calculate the new shared key and decrypt the communications of A and C. It can also pose as device A to device C and as device C to A thus perpetrating a Man-in-the-middle attack.

- **Encroachment of privacy**

  Each Bluetooth device has a unique address. This means that all communications traffic can be traced to a particular device and it makes it easy to track and monitor the traffic from one device.

The general consensus seems to be that Bluetooth is good for small simple applications but no sensitive or business critical data should be transmitted using it.[10][11]

WLANs – 802.11b

Portable devices of all types are now being given the ability to communicate over wireless LAN technology using the IEEE 802.11b specification. Security vulnerabilities present in the various implementations of this specification have been well documented and an in-depth discussion of each issue would not be appropriate here. Instead lets see how these issues are applicable to portable devices.

MAC address filtering

One of the security mechanisms specified within the 802.11b specification is MAC address filtering. An access point is given a list of the MAC addresses of all devices that are authorised to associate with it. All devices with MAC addresses not in this list are denied access.

A vulnerability in this mechanism has been identified. It is possible for an unauthorised user to sniff the traffic and identify the authorised and associated

MAC addresses. The attacker needs only to change the MAC address of his wireless network interface card to an authorised one and when the traffic from the genuine card ceases, the unauthorised user makes an attempt to associate with the Access Point. Because he is using a MAC address that is known to the Access Point the malicious user is allowed to associate.

PDAs with wireless cards pose another threat to this mechanism. Because of the ease with which a small portable device is lost / stolen, a MAC need not even be faked. The device itself contains the authentication information needed to gain access to the wireless access point. This makes the management of a scheme that depends on MAC address filtering for its security a very difficult and time-consuming process.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy is a proprietary encryption mechanism for use with 802.11b. It is used to encrypt data passing between clients and access points and is supposed to maintain the confidentiality and integrity of data. However many flaws have been found with the manner in which it has been implemented. It is possible to use either 40 bit or 128 bit keys. However, the vulnerabilities that have been exposed are in connection with the manner in which initialisation vectors are handled and apply to traffic encrypted with keys of both lengths. Therefore using the longer key does not decrease the likelihood of the key being recreated and the traffic being decrypted. Data being passed between wireless clients and access points encrypted using WEP cannot be thought of as being secure. Can you allow your portable devices to connect to your enterprise servers if the information being transmitted could be eavesdropped upon?

One of the main causes for the weaknesses in the implementation is the use of static keys. It is a symmetric encryption algorithm, which means the same key is used for encryption and decryption. Both the access point and the client must have access to this key. All initial implementations of the specification demand that the key be input to the client and access point before communication is possible. All clients must have the same key in order to communicate with the access point. Because of this if one client is compromised, the key becomes known to an unauthorised user. The attacker can then decrypt all the traffic between all other clients and the access point until the symmetric key is changed for all communicating parties. The impact of this vulnerability becomes greater when the devices on which the key is stored are small, portable and easily accessed by an attacker.

Even though these vulnerabilities have been clearly documented and publicised, the realisation of the security risks they represent does not seem to have dawned on the users of this technology. According to a survey commissioned by RSA Security in London recently, 63 percent of networks surveyed were left on the default configuration, which clearly identified the company owning the data and where it was coming from.[17]

Lack of Auditing Software

The lack of in-built auditing capabilities mean that even if an attack is launched on your corporate network or another type of security incident takes place using the handheld device, no audit trail will be in place and incident handlers will not be able to trace the attack to a particular portable device.

This leaves the network open to future similar attacks with no clear way of identifying the threat and protecting themselves against it.

The threats

The previous paragraphs described the various vulnerabilities associated with portable devices but as stated above risk is a product of the vulnerability vector and the threat vector. If the threat is zero then the risk is zero too.

The SANS GSEC Course states that vulnerabilities are the gateways through which threats are manifested. It is when a threat is able to connect to its specific vulnerability that the result can be system compromise. Let us examine the threats in place in the portable device usage model and put them together with the numerous vulnerabilities outlined above to establish the risk that we are facing by allowing portable devices access onto our networks.

Due to the usage model of the PDA, they are brought outside the confines of the network perimeter. Security measures that would be adequate while in the protection of the existing security perimeter are no longer enough. Vulnerabilities that need physical or local access to the device in order to exploit them are now more likely to be open to exploitation.

For example the vulnerability described above associated with the serial cable interface to a device running PalmOS requires physical access to the device. A malicious user would not be able to exploit this vulnerability unless the device was placed in a situation where the malicious user could gain physical access. For a PC the threat would not be large as a PC is rarely moved outside the network perimeter. However, because of the use model of portable devices, they are often brought into these kinds of situations and as a result the threat vector is large.

Because of the lack of inbuilt security restrictions on portable devices users can over ride security controls that have been put in place by security personnel. Thus making users a threat to the safety of the devices. Users can install unevaluated applications leaving the devices open to the threat of viruses and other types of malicious code.

Communicating with other PDAs to exchange information is a common activity for users and brings its own risks, leaving the PDA open to attacks on the communication channel.

Therefore it is the very nature of the portable device that is its greatest threat. That it is brought outside of existing security defences means that each device must have all its security controls built-in. It has no other security measures to rely on. Unfortunately because it is a small portable device, emphasis has been placed on efficiency of power usage and usability. Security is pushed aside in the default model.

Defending ourselves

Handheld devices are already in place in most corporate environments. The next thing is to decide what to do about it. A policy is the first step. Time needs to be set aside to sit down and make decisions about what will be allowed within your organisation, what practices will be enforced and software installed to mitigate the risk.

Decisions about which versions of third party security software are most appropriate to your network also need to be made. There will need to be investigations into what anti-virus measures, encryption measures and other security measures are offered by each piece of software.

The following paragraphs describe some of the concerns that an organisation must consider when addressing the issue of allowing PDAs onto their corporate network.

The question of ownership

Before a policy can be put into place, the scope of its application must be clear. To this end, the question of whether or not your company allows privately owned PDAs onto the network must be asked.

This is not an issue that your organisation is likely to have encountered before when writing a security policy. PDAs are affordable and private users account for a large part of the user population. It is likely that there are many employees who already own and use a PDA of their own.

If the company is responsible for all the PDAs, they are responsible for purchasing, registering, supporting and securing the devices.[9] This is no mean feat with small portable devices due to the high risk of the devices being lost or stolen. The issue of personal use of the organisation's PDAs must be addressed. If users are given control over their PDA they will resist the installation of security controls, overriding the restraints put in place. They will also install unauthorised software, putting the devices at risk for viruses and other pieces of malicious code. If the user stores personal information on the device and then synchronises with the corporate network there may be issues relating to privacy to be addressed.[16]

If privately owned PDAs are allowed on the network, however, it will be difficult to restrict the brand and version of PDA in circulation. If there is no uniformity in device, where does that leave your security practices? It is much more difficult to enforce virus protection policies when the version of virus protection software is inconsistent across the corporation.

Physical Security Controls

A lot of the vulnerabilities and threats mentioned above focus on the ease with which these portable devices are lost or stolen, so it makes sense that the first issue to be addressed in the security policy is that of physical security. Most PDA manufacturers offer PDA accessory cases. Make sure that the users know not to leave their PDA in the car. Provide security measures so that users don't leave their PDAs unsecured on their desks, e.g. "Denton Software's Cradle Robber sounds an alarm and disables your PalmOS PDA when the handheld is removed from its cradle. The alarm deactivates when an unlock code is entered or the PDA is returned to the cradle."[4]

[4] Brown, M. "Keep it in your Pocket."

Extending authentication requirements

Many third party applications allow the user to extend the password protection beyond the traditional alphanumeric character set. Communication Intelligence Corporation's Sign-on is a utility that uses a user's signature or personalised drawing to authenticate them. This scheme has two advantages. A signature is not easily guessable and it prevents the user from using the same password on their PDA as on the corporate network.[18][19]

Disable unauthorised synchronising actions

Another facility you may want more control over is the ability to synchronise. There is software available which allow the user to control when and to whom a synchronisation action can take place. [18]

Encrypt data on the PDA

If an unauthorised user manages to gain access to the PDA and bypass the password, it would be important to restrict the amount of information he can retrieve from the device. To this end, there are many encryption tools available for all platforms that will encrypt the databases and other information on the device, e.g., Trust Digital's PDA Secure[5]

Virus Protection

There are many virus protection products available from the usual anti virus software vendors including F-Secure, McAfee and Symantec.

Apart from these virus protection software products it is important to have a policy not to download files or open email attachments unless you know what they contain and to synchronise regularly to minimise the effect a virus can have on the data on your portable device. Again users must take care to ensure they do not transfer malicious code to or from the PC during the synchronisation process.[18]

Conclusions

Small portable devices have become widespread in the corporate world today and will become more popular when users begin to take advantage of the new wireless capabilities.

There are many vulnerabilities associated with a portable device, some of which are weaknesses we are already familiar with from other security models and some of which are unique to the usage model of a portable device. As the devices evolve the number and type of vulnerabilities will increase.

Because of their unique situation portable devices are brought outside the scope of the network perimeter. They are more vulnerable to threats from the outside world. Also because of the lack of in-built security controls, users have more control over the device and the level of security in use.

But, we must face the reality that the portable device is not going away and so decisions must be made about how to control their use and keep our network

[5] http://www.trustdigital.com/prod15b.htm

secure at the same time. A policy must be put in place and users educated about the risks they put the organisation in by misusing the devices.

It is important to address the issue of allowing portable devices onto our networks. Otherwise we could be leaving ourselves open at a single point of weakness.

References

[1] McLindon, A. "PDA Shipments tumble in 2002." Electricnews.net January 29, 2003. URL: http://www.enn.ie/news.html?code=9172770 (February 18, 2003).

[2] Cardoza, P. *"Block PDA Viruses."* Tech Republic. April 25 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2862764,00.html (February 19,2003)

[3] Schlesinger, L. *"PDA viruses? Don't buy the FUD."* ZDNet, April 1 2001. URL: http://zdnet.com.com/2102-1107-503538.html (February 7, 2003)

[4] Press Release. *"McAfee.com Wireless Security Center Protects Against First Palm Virus and Newly Identified Palm Trojan."* McAfee, September 22, 2000. URL: http://www.mcafee.com/aboutus/press_room/press_releases/pr09220001.asp (February 19, 2003)

[5] Lemos, R. *"Trojan Horse Kicks the Palm."* Tech Republic, August 29 2000. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2620913,00.html (February 19, 2003)

[6] Worley, B. *"PDA Virus Help."* Tech TV. May 23, 2001. URL: http://www.techtv.com/callforhelp/answerstips/story/0,24330,3329073,00.html (February 19, 2003)

[7] Mcafee, *"Virus Profile: PalmOS/Phage.963."* Sept. 21 2000, URL: http://vil.mcafee.com/dispVirus.asp?virus_k=98836& (February 19, 2003)

[8] Delio, M. *"Palm virus hits, but don't worry."* Wired News. Sept 22, 2000. URL: http://www.handheldcomputerdepot.com/newspalmvirushitsdontworry.html (February 19, 2003)

[9] "A White Paper on Handheld Device Security." F-Secure Corporation. November 2002. URL: http://www.f-secure.com/products/white-papers/hhsecurity021122.pdf (February 10, 2003).

[10] Vainio, T. V. "Bluetooth Security." Department of Computer Science and Engineering, Helsinki University of Technology. May 2000. URL: http://www.niksula.cs.hut.fi/~jiitv/bluesec.html (February 17, 2003).

[11] Sutherland, E. "Bluetooth Security: An Oxymoron?" MCommerce Times. November 28, 2000. URL: http://www.mcommercetimes.com/Technology/41 (January 7, 2003).

[12] Lemos, R. "Passwords don't protect Palm data, security firm warns." CNET News.com, March 2, 2001. URL: http://news.com.com/2009-1040-253481.html?legacy=cnet&tag=cd_pr (February 2, 2003).

[13] Lynch, I. "Crackers can zap data off Palm Pilots." Vnunet.com, January 19, 2001. URL: http://www.vnunet.com/News/1116644 (February 17, 2003).

[14] Security Advisory. “PalmOS Password Retrieval and Decoding (A092600-1).” @Stake, Inc. URL: http://www.atstake.com/research/advisories/2000/a092600-1.txt (February 17, 2003).

[15] Security Advisory. “Palm OS Password Lockout Bypass.” @Stake, Inc. URL: http://www.atstake.com/research/advisories/2001/a030101-1.txt (February 17, 2003).

[16] Stevens, T. “Securing PDAs.” Information Security Forum.

[17] The Register. “WLAN security still dismal – survey.” Electric News.net. February 17, 2003. URL: http://www.enn.ie/news.html?code=9350104 (February 17, 2003).

[18] Brown, M. “Keep it in your Pocket.” PC Magazine. March 26 2002. URL: http://www.dentonsoftware.com/News/Articles/PC%20Magazine%20-%20Print%20Article.htm (February 17, 2003).

[19] Communication Intelligence Corporation. Sign-On. URL: http://www.cic.com/products/signon/ (February 18, 2003)