Sans GSEC Certification
1.4 Option 1

Personal Digital Assistants And Securing them.

Sans GSEC Certification
1.4 Option 1
Personal Digital Assistants and securing them

Introduction

The portable world has now enveloped our very existence; we no longer operate in isolation from machines and can only function in our personal and professional lives with the likes of mobile phones, pagers, mini disc players and Personal Digital Assistants (PDA's). Working in security its been my job to examine the possible security risks that some of these devices may cause to the organisation, and I've been frustrated by what little information is available on securing such devices.

The aim of this paper is to help those in the same position that I have found myself in. I intend to cover the worrying prospect of an all out virus attack on PDA's, the introduction of wireless communication for PDA's, user authentication, Data Protection and physical security. Based on this investigation I have also compiled a template for designing a Mobile Computing Policy.

I have found that many different specialists give their professional opinions on the subject, some saying that PDA's and other similar devices will be the downfall of modern life and will allow the thief easier access to sensitive company and personnel data. In contrast to this, is the belief that PDA's are a useful tool and lack of security is unsubstantiated. Unfortunately, as the administrators we cannot afford to wait until the chairman's salary is available on the Internet because a lost, stolen or hacked PDA had that data stored on it.

During my research I have come across many types of software and different techniques for improving security, below I intend to document them and show what I believe would be best practice. Hopefully protecting and preparing us for the worst.

Virus attack.

As we all know a virus can be the most destructive force we are likely to come across in the day-to-day world. Now for years the industry has been fighting to secure us from that one virus that brings the modern world to a stand still. We have been pushed to the limit on a number of occasions with such menaces as the Love-Letter, Melissa and a host of email aware worms. Since these attacks the antivirus providers have been selling protection for every type of hardware you can imagine from the PC to E-mail servers. Now you can even get protection for your PDA.

There are two known viruses out there that are designed to attack the PDA these are 'Phage' and 'Liberty'. What concerns me is that not all antivirus providers feel the need for protection. I will now examine if these viruses pose a real threat to the PDA.

Phage Virus

This virus, which was detected in September 2000, was the first to be recognised as a possible threat to PDA security. At the time of detection, virus protection for PDA was pretty non-existent. The virus would infect all Palm programs and effectively render the Palm useless:
"It has always been possible to write malicious code for the palm operating system" Graham Cluley, senior technology consultant for Sophos Antivirus. However, most antivirus providers classed the threat as low and still do today.

Liberty Trojan

This Trojan was distributed in the warez community as a crack for the liberty application (Game boy emulator) for the Palm PDA operating systems. Instead of illegally cracking the software the Trojan deletes all programs on the palm. The designer of the Trojan only intended it to go to a couple of friends as a harmless joke. This virus was also first detected in 2000.

Since the introduction of these viruses in 2000 the PDA has moved on a long way from the simple Palm. To day we are looking at devices almost 10 times more powerful such as the Compaq I-Pac – HP Jornada and Palm VI.

Leading British Antivirus provider "Sophos" does not currently provide protection for PDA. Their stance on the situation is that by having antivirus protection on the host PC/s then a virus could not be transmitted to the PDA during synchronisation and would prevent any virus being sent to the PDA and visa versa. Which is a fine approach to take although now that these devices have built in modems or as outlined below wireless capability a virus could be transmitted over other connections, and potentially damage the PDA if not the desktop.

Antivirus provider "F-Secure" currently has protective software (Pocket PC AV)[1] simply designed to work on the Windows Pocket PC operating system (Previously Windows CE). It was one of the first providers to offer Antivirus software, selling it on the basis that it is just a matter of time until viruses for mobile devices are as common as viruses for its bigger brother, the desktop. The benefits of this software are that all updates can be delivered to the PDA during a connection with the host PC and can be completely automated, to reduce the user interaction. This obviously fixes the problem that Antivirus protection is only effective if it is kept up to date. The only problem you have is that users will need to synchronise on a regular basis.

This has brought me to the conclusion that the following steps should be taken to protect the PDA from infection.

[1] Antivirus Pocket PC AV
http://www.f-secure.com/wireless/pocketpc/pocketpc-av.shtml

- Disable Wireless communication devices if not needed
- Remove any communication device or disable built in modems
- Disable infrared. (Prevent data transfer)
- Prohibit the synchronising of devices with any machine other than work PCs.

These steps can only be applied if this will not restrict business use. In cases where these cannot be carried out and providing antivirus protection is not a viable option, then a good teaching program should be introduced to instruct your users on the safety, security and acceptable use of such devices and by introducing a Mobile Device Policy outlining the responsibility of all parties involved you should be able to limit the risk. This will be discussed further on in the paper.

Wireless Communication

Wireless communication is not a new concept, in fact the goal of many service providers is to reduce the confines of the office, allowing users the freedom to roam and locate anywhere in a building/airport or coffee shop this must all be achieved without wires. As the need for freedom in the work place becomes an essential part of the organisation, we are adding blue tooth communication devices to the PDA effectively allowing the user to access emails, make notes and send them anywhere in the network. Now without the correct security this can be a very dangerous tool.

The latest fads for hackers/attackers is “War-driving & War-Chalking” this simply means searching for unprotected wireless networks and marking the surrounding area with a mark so that other hackers are notified and can access the victim. There was an article in a British newspaper recently “The Mirror”[2] that investigated the ease of doing this in London. The newspaper reporter along with security experts drove through London with a laptop and PDA and made multiple connections without detection.

To protect this wireless communication W.E.P.(Wired Equivalent Privacy) was created. In the current version of pocket pc this can support 40 to 128 bit keys and is known as 802.11b. It is still necessary to remember that these keys are easy to break and should not be relied upon solely. The latest wireless encryption is called 802.11z this encryption relies on the use of certificates issued by the server and these are then used to encrypt data unfortunately the current version of the Pocket PC operating system does not support this yet.

My suggestions for securing wireless communication between PDA and network would be to activate the encryption protocol even though it is not

[2] The Mirror
Our raid on Downing St.
By Graham Johnson – August 18th 2002

100% secure it would prevent simple sniffing from reading data during transfer.

By restricting the user to only utilising the wireless function of the PDA to within the company walls should reduce the risk of any transfered data from being detected.

User Authentication.

We all know the need for user codes and passwords but many do not activate simple built in password access on a company PDA. This is possibly because there is the assumption that because the PDA is with you all the time no one else would be able to access it. Unfortunately this is a well adopted fallacy, as I will explain further on in the paper, a common thief is not always after your data but just after the device. Therefore you must make the device unattractive to the opportunistic thief as well as the hacker/attackers.

I have investigated all the common PDA's such as the Compaq I-Pac – HP Jornada and Palm VI, and all have the ability for user authentication, this is a fundamental part of the Pocket PC operating system and should be configured and activated in accordance with the company password policy. Ensure that the user authentication is active before the PDA is distributed to users, and that any existing PDA's are recalled and the security options are checked and modified where necessary.

The user authentication section of the Pocket PC operating system is found in the password section within settings. The password strength can range from a four digit pin to a strong alphanumeric password, you will also find the time out section here this can be set between 0(Requested at logon only) to 24 hours. There are two known problems with this password mechanism the first is if you mistype your password you will have to wait longer and longer each time you try, this is a design feature added to prevent brute force attacks. The second is that there is no way of resetting the password if you have forgotten it, the only way round this is a hard reset, resynchronise and install applications again.

The use of a third party authentication device such as a key fob would also improve security but only if used in tandem with user codes and passwords.

Data Protection

This new super device is holding all that data that you will need to access to keep you going in or out of the office. You can hold contacts, calendars, meeting agenda's, notes, bank details and even system passwords. Now this is great for the user, but even better for the person trying to access your systems. All they need to do is find your PDA and read the information or with the use of Infrared or wireless connection the data could be sent to another PDA or printer and you would never be the wiser.

To stop this happening you can write a company policy prohibiting this data being stored on a PDA but that's no good for the sales team who spend one day in the office a week. So you turn to encryption. There are many types of software packages that will provide encryption of stored data such as the F-Secure crypto package.[3] If you do decide that this is the path you want to take then the rules for applying encryption must be followed.

- A copy of all encryption keys must be stored in a safe location, it may be necessary to use the keys if a problem occurs or the original keys are lost or if requested by law enforcement.[4]

- An encryption policy can be used to outline what can and cannot be encrypted, stating company standards and cipher strengths.

If you do decide to use encryption you will then have to decide what to apply it to. The latest version of Pocket PC can utilise 128-bit SSL encryption through the pocket Internet Explorer unfortunately the version of the browser when queried by the web server returns with the version 3.02, and as we know the version that utilises high encryption is version 5 this will cause the web server to refuse connection, there is a work around in "Regking 2002" (www.doctorce.com/regking.htm) this will allow you to change the version number to 5.0. This fix is not ideal but will allow access to the resource and utilise the higher encryption.

Pocket PC does not support the ability to encrypt individual files, it will not be able to synchronise password protected word and excel files the best alternative would be Pretty Good Privacy (PGP). The operating system does however support the new secure digital (SD) cards, you can store data on to these, and then you are able to encrypt the cards.

Physical Security

Keep the PDA safe at all times, this may sound like common sense but it should be kept in locations where it cannot be easily accessed don't leave it out on show and when in transit make sure that it is not easily recognisable.

There have been cases recently where laptops have been left at train stations because the user was absent minded. This happened to a MI5 (British intelligence) engineer thankfully the laptop was returned before any damage was caused[5]. This is not the only high profile case. A NATO general misplaced his laptop, which contained strategic bombing plans. Cases of

[3] File Crypto
http://www.f-secure.com/wireless/pocketpc/pocketpc-fc.shtml

[4] Check local laws governing the use of encryption it does differ from country to country.

[5] BBC news
Laptop safety – a guide for spies 28th March 2000
http://news.bbc.co.uk/1/hi/uk/693470.stm

this type highlight the danger of leaving your PDA unattended. The data could not only be useful to a Hacker/Attacker but to a competitor as well, below I have suggested a few ideas in preventing this from happening.

I feel that the following minimum precautions should be sufficient when protecting your PDA.

- Ensure that there are appropriate training and awareness programs to instruct users on aspects of physical security for their PDA's.

- Ensure that the name and contact details are inscribed on the device somewhere so that in the event of loss it can be returned. Some organisations may see this as a possible breach in security itself. In this case a company called *Idstrip.com* offer a service where their details are inscribed on the device and when returned they compare it to a database and then return it to you. This will hopefully prohibit a thief from stealing the device, as it will be harder to sell if company details are all over the casing.

- Do not leave the PDA on show and ensure that it is carried in a case or hidden within a separate bag at all times.

- Even when in the office it is still necessary to take precautions do not leave the device on show when at lunch and ensure that it is not left out at night.

The metropolitan police force in the UK has an acronym for a personal safety checklist. "PLAN" Prepare, Look alert, Avoid risks and Never assume its safe.

Mobile Device Policy

This is an essential part of the protection and no company should consider introducing PDA's before this has been drafted and users are fully aware of their responsibilities. The following few recommendations should be considered when developing a policy.

The overview

The policy should aim to remove as many of the risks associated with the use of PDA's through the introduction of clearly defined controls and guidelines.

Purpose

The policy should establish the requirements for the creation, maintenance administration and acceptable use on or off company premises.

Scope

The policy should apply to any employee utilising a company owned PDA be it connected to the company network or not.

Creation and maintenance

It would be advisable if a security team was given the responsibility of ensuring that all company owned PDA's conform to a predetermined standard this should include the make and model of the PDA. It is a lot easier to secure a device if you only have one make to worry about. The standard should also include the following points:

- All software that is installed on the device must conform to the company standards
- Any and all service packs/ patches must be applied. All PDA's should be kept up to date. To ensure that this is done they should be returned to the team responsible on a regular basis, a record of this should be kept (will be useful in the event of any breaches).
- Any antivirus software should be set to look for updates during synchronisation and users should be informed that it is their responsibility to ensure this is done regularly.
- The ability to access the bios of the systems should be password protected and should remain with the administrative team.
- During a period of inactivity the device should be set to lock and password re-entry should be set. The period of time will depend on the device. A 10 minute period should not prevent the user from working.
- All devices and peripherals must be engraved with the company name.

Administration and maintenance

In the event that devices are lent or borrowed a record should exist detailing: make, model, serial numbers and the user assigned. This will ensure that devices are returned. This database should also include all staff that use a company owned PDA, for in the event of termination it will be necessary to remove all company data even if the device is not to be returned.

The user must be made aware that he/she is fully responsible for the use and safety of the device.

Access to the device must be made through a suitable user code and password that is associated to the user access without these access should be prohibited.

The user is also responsible for backing up all data held on the device and they should ensure that it is backed up on a regular basis.

Acceptable use.

The user must not install any software or add additional hardware, requests for this must be authorised and carried out by designated staff.

In the event that the device is lost or stolen then it must be reported at the first opportunity.

Users must be aware of their responsibilities with regards to data protection in accordance with the “Data Protection act (1998) and the Computer Misuse act (1990)[6] if responsibilities are unclear then the users must contact the relevant department for clarity prior to using the device. Users must also be informed that PDA’s are only intended for transient data storage and not for long-term data storage.

Enforcement

Like any policy used within the organisation it is necessary to ensure that failure to comply may result in disciplinary action up to and including dismissal.

Exceptions

In the event that an exception to the policy is needed it should be fully documented and approved by senior management.

Check list.

To summarise the points above into a simple to follow guide I have produced the checklist below

1. Ensure users are trained on security safety and acceptable use.
2. Create and adhere to your Mobile computing policy
3. Install antivirus software and ensure it is kept up to date.
4. Engrave contact details on the PDA
5. Back up data regularly
6. Create password logon’s
7. Disable infrared capabilities
8. Remove modems
9. Disable wireless devices or activate WEP
10. Carry the device hidden from view
11. Ensure device is not left unattended
12. Synchronise with known PC

Conclusion

To conclude, the introduction of PDA’s in to our lives has changed our personal and working lives forever, there’s no longer a need for scraps of

[6] Laws may vary depending on country.

paper with phone numbers on, or the need for that wonderful Filofax that took pride of place at the company meetings. Instead, we now have this neat, tidy, portable, very compact and very powerful computer, which has revolutionised the way we organise our daily lives.

As I have outlined above this device is extremely powerful, not only in the sense of its computer capabilities but also because of the way in which is used. Misuse of the device or ignorance of the issues surrounding PDA viruses could result in huge violations of data protection for employers and the user.

As a security engineer, I would advise the stringent use and protection of PDA's and adjoining equipment. I also envisage having to work with other company departments to instil a culture of security within the organisation. As with most computer problems the problem arises due to user ignorance, this is a difficult problem to resolve as the user obviously has other pressing issues to contend with in their professional or personal lives and does not wish to learn about possible IT glitches.

Therefore I believe that to avoid possible PDA issues the solution is twofold, to put the necessary logistical systems in place and follow it up with in house training on why these systems are important. This should then improve the PDA users knowledge of the consequences and so make sure they implement the avoidance procedures.

By following the guidelines stated in this paper I feel confident that every precaution had been taken and that I would be prepared for the worst eventuality.

At the speed that things in the IT industry move, it will not be long before the devices are used instead of a desktop PC. Sooner or later you will be able to run your world from one of these devices so there's no harm in remembering the old boy scout motto "Be Prepared".

References, (in alphabetical order)

BBC news
Laptop safety – a guide for spies 28th March 2000
http://news.bbc.co.uk/1/hi/uk/693470.stm

F-Secure
Antivirus
http://www.f-secure.com/wireless/pocketpc/pocketpc-av.shtml
File Crypto
http://www.f-secure.com/wireless/pocketpc/pocketpc-fc.shtml
Palm OS
http://www.f-secure.com/wireless/palm/av4palm/

Handheld Devices Audit Checklist 2002 by Krishni Naidu.
http://www.sans.org/SCORE/checklists/Handhelddevicesauditchecklist.doc

How Personal Digital Assistants (PDA's) Work - 2002
By Craig C. Freudenrich, Ph.D. http://www.howstuffworks.com/pda.htm

PDA DEFENSE
Defend your information.
http://www.pdadefense.com/products.asp

Pocket PC Security
By Chris De Herrera revised 2/5/2002 version 1.01
http://www.cewindows.net/reviews/pocketpc2002security.htm

The dilemma of PDA Security An Overview by Daniel M. Lyon January 2002
http://rr.sans.org/pdas/dilemma.php

The Mirror
Our raid on Downing St.
By Graham Johnson – August 18th 2002

Sophos Antivirus
Best practices for Multi-tier virus protection. June 2002
Katherine Carr and David Mitchell Sophos, Oxford, UK
http://www.sophos.com/virusinfo/whitepapers/multi_tier.mtml
Graham Cluley Senior Technology consultant 29 August 2000
http://www.sophos.com/virusinfo/articles/liberty.html
Graham Cluley Senior Technology consultant 22 September 2000
http://www.sophos.com/virusinfo/articles/palmphage.html