



Portable Computing Device Security

Didi Barnes
First•Base
Technologies

16 September 2003



Document control summary

Document title	WP-PortableComputingDeviceSecurity.doc
Filename & path	D:\FBTECHIES\RESEARCH\IN-HOUSE PROJECTS\R&D - PCD Security\Reports\WP-PortableComputingDeviceSecurity.doc
Owner	Didi Barnes
Date of document creation	16/09/03 18:23
Partner authorisation	Yes
Version #	1.4

Revision history

Date	Revised by	Comments	Version #
16/09/03 18:23	Didi Barnes	First draft	1.0
03/12/03 10:04	Didi Barnes	USB flash drive updates, PDAs running Linux	1.1
18/02/04 14:16	Didi Barnes	Per e-mails from Niels	1.2
27/02/04 10:08	Didi Barnes	Remove incidences of MMIS as this has now been discontinued.	1.3
02/06/04 11:47	Didi Barnes	Amend pagination	1.4



Contents

1. PREFACE	4
1.1 SCOPE	4
1.2 THIS REPORT	4
1.3 DEFINITIONS	4
1.4 CAVEATS	4
2. INTRODUCTION	5
3. RISK ANALYSIS	7
4. SECURITY POLICY CHECKLIST	8
5. SECURITY POLICY GUIDELINES	10
5.1 INTRODUCTION	10
5.2 GENERAL USAGE POLICY AND STAFF AWARENESS AND TRAINING	11
5.3 DEPLOYMENT AND MANAGEMENT OF DEVICES	13
5.4 ASSET TAGGING	14
5.5 PHYSICAL SECURITY	15
5.6 ACCESS CONTROL	16
5.7 DISK / FILE ENCRYPTION	17
5.8 DATA COMMUNICATIONS	18
5.9 EXTERNAL STORAGE	20
5.10 PERSONAL FIREWALL	21
5.11 HUMAN FIREWALL	21
5.12 VIRUS AND MALICIOUS CODE – AV POLICY	21
5.13 BACKUP POLICY	22
6. PDA SOFTWARE	23
6.1 ENCRYPTION & ACCESS CONTROL PRODUCTS	23
6.2 ANTI-VIRUS PRODUCTS	25
6.3 BACKUP	26
6.4 NETWORK ANALYSIS AND ADMINISTRATION TOOLS	27
7. BIBLIOGRAPHY	29



1. Preface

1.1 Scope

To provide a proprietary standard document covering Portable Computing Device (PCD) security (see definitions) in order that this may facilitate in the production of policy, best practice and training documents thus assisting companies in securing such devices.

1.2 This report

This report was researched and produced by Didi Barnes, partner (head of R&D) of First Base Technologies. Thanks go to Peter Wood (Chief of Operations, First Base Technologies) who checked this document for errors.

1.3 Definitions

PCD: means “Portable Computing Device” and should be taken to refer to a PDA, laptop or any other device capable of carrying or processing data, so may also include certain cellular telephone and other devices that technological advances make available.

PDA: means “Personal Digital Assistant”, and will be used when specifically referring to handheld devices, such as Palm OS or Windows CE devices.

External memory: should be taken to mean any removable, portable memory device, e.g. USB flash drives, CF (Compact Flash) cards, SD (Secure Digital) cards, microdrives, memory sticks - any type of external memory device in fact.

POCKET PC: this term should be taken to mean the Windows CE operating system since it is used synonymously when describing that operating system.

WLAN: Wireless Local Area Network.

WEP: Wired Equivalent Privacy: a type of encryption used for wireless data streams.

1.4 Caveats

Didi Barnes and First Base Technologies can accept no responsibility for any consequences should you decide to use the information contained in this report. Whilst various software and hardware are mentioned in this document, this should not be taken as a recommendation of that software and/or hardware.



2. Introduction

Emphasis should be placed upon the fact that the contents of this document can apply to any Portable Computing Device (“PCD”) so is as applicable to laptop PCs as PDAs and other handheld devices. The context will make clear if an element of this text applies to a specific type or brand of PCD.

Hardware constraints previously limited PDAs to being glorified personal organisers, thus laptop PCs have been for many years the portable business tool of choice. However, rapid advances in PDA technology leading to enhanced functionality, such as faster processors, greater storage capacity and wireless communication technologies, are now resulting in these devices being deployed as full-blown business tools in the corporate environment. Their ease of portability is likely to result in their superseding laptop PCs for many environments, heading towards a future of seamless, cable-less connectivity between devices, between people and between networks.

Consider the data a PCD or external memory device (e.g. USB flash drive, CF and SD cards, etc) can carry. PIM¹ information, e.g. address book, calendar, to-dos, notes; all of which can be exploited for the purposes of social engineering, identity theft and to verify identity, e.g. when requesting a password be reset [7]. These devices can contain network connection information providing an attacker with a neat backdoor into the organisation. The other data such devices can contain is merely limited by memory capacity, which is becoming increasingly less an obstacle. That data could be trade secrets, CRM information, personnel data, patient records; all having potentially serious repercussions in the wrong hands.

Even given all this, according to a survey commissioned by access control firm, Pointsec Mobile Technologies, a third of employees leave such business information and access details unprotected on their PDAs [4]. Even if they do have basic security enabled on their devices, these controls may be able to be bypassed by a determined attacker. Whilst many companies have become aware of the particular security issues surrounding the portable nature of laptop PCs and have made due provision for these in their security policies, other PCD devices and associated external memory tend to be overlooked. Their small size has a psychological “out of sight, out of mind” effect. So what then, of the risks?

Device-level risks: As it becomes more difficult for attackers to breach security controls of networks and PCs due to rising awareness and thus better security, attackers will be looking at other ways to bypass these security boundaries. PCDs, particularly PDAs, and external memory cards will become an increasingly attractive target; theft and other compromises will thus become more likely.

¹ PIM = Personal Information Management.



Communication-level risks: most PCDs nowadays have one or more wireless technologies, e.g. 802.11x, Bluetooth, IrDA, built-in. Those that don't, usually have facility to attach hardware to implement them externally, e.g. via a CF Bluetooth card, or a PCMCIA 802.11x card (a PDA may require a "sleeve" or "expansion pack" to take a PCMCIA card). Each of these technologies carries its own set of risks, for example the risk of data capture over the air by traffic analysis (sniffing), the risk of connections being made with unauthorised devices, and other exploits.

Companies urgently need to implement a suitable security policy to address these issues. Staff awareness and training campaigns should be implemented. If users know the risks and how to ameliorate them, this will provide an excellent first layer of security. Disaster contingency plans should be made should a device or its data fall into the wrong hands.

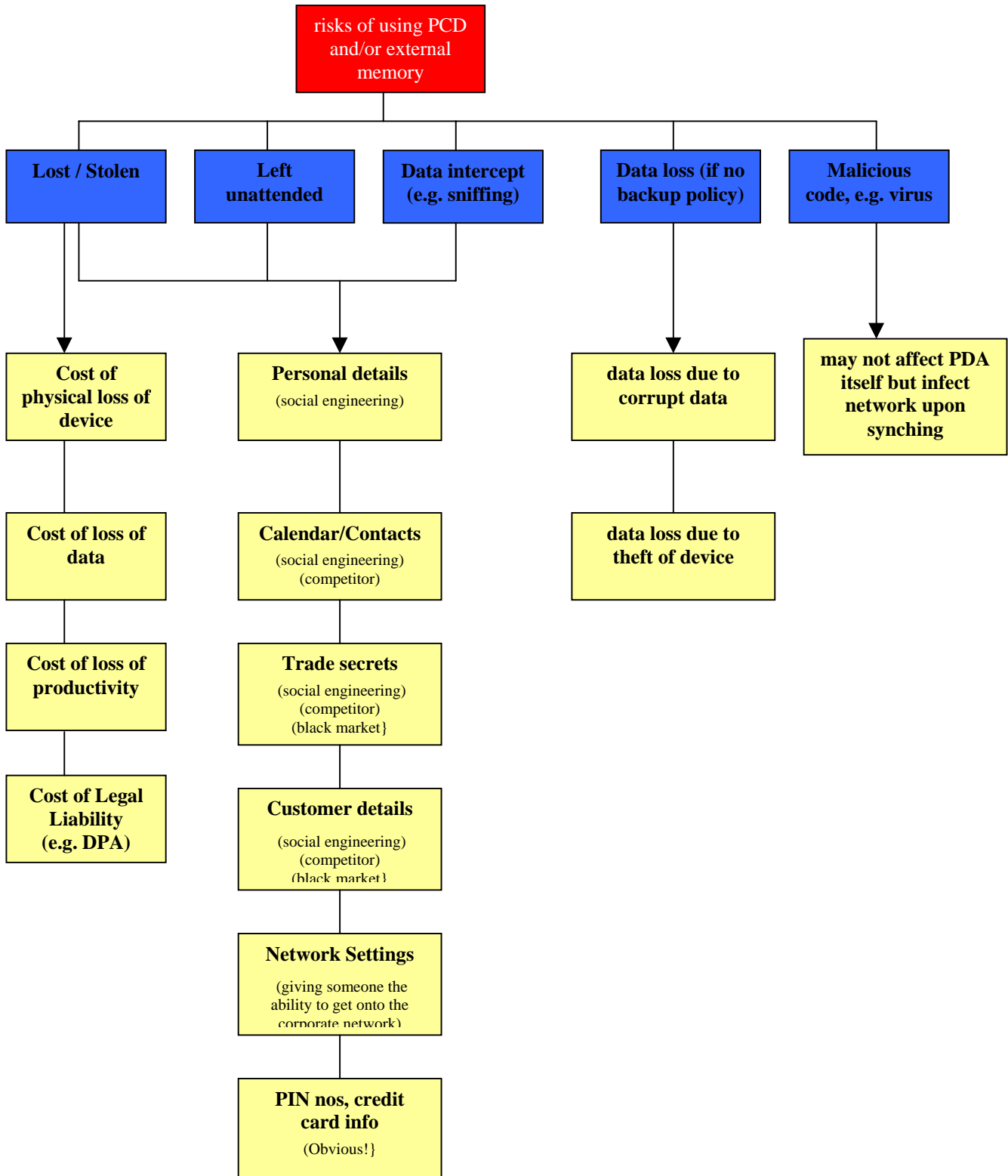
To conclude this section, the big question to ask is:

Q) "what would the impact be on our organisation if the device, external memory devices, data contained on them or being transferred via networks - got into the wrong hands?"

This question, and ideas to reduce the vulnerabilities associated with it, will be explored in the remainder of this document.



3. Risk Analysis





4. Security Policy Checklist

The right-hand column contains cross-references to more detailed information that can be found in the next section.

PCD policy should take into account wireless, homeworking, remote access, backup, anti-virus and windows security policies.	5.1
PCDs should be forbidden without prior authorisation	5.2
Only authorised PCDs are permitted to connect to the network	5.2
Train staff how to spot and report suspicious activity / rogue PCDs	5.2
Those authorised to use PCDs should receive training prior to their issue	5.2
Only company-owned PCDs should be authorised, privately owned devices and external memory should be prohibited.	5.2
PCDs should be used for business-use only - no personal data / software	5.2
Users should not be allowed to install software, change settings on their PCD	5.2
Define reporting procedures should security be breached	5.2
Ensure personnel know the value of data and the risks if it gets into the wrong hands	5.2
Purchase PCDs that offer the best security options	5.3
Define responsibilities for deploying, installing and managing PCDs	5.3
Employ a method of patch and update management for PCDs	5.3
Standard-build should be mandatory for all PCDs	5.3
A user should not usually be an administrator on the PCD	5.3
Check regularly for rogue PCDs	5.3
Check regularly that PCDs continue to conform to security policy	5.3
Employ some form of asset-tagging on PCDs	5.4
Don't allow owner information to be displayed on the PDA (i.e. "owner information" settings).	5.4
Use external locking facilities, e.g. Kensington lock, where possible	5.5
PCDs should be kept locked away when not in use and external memory stored separate from the PCD.	5.5
PCDs should be kept in a way as to obfuscate them, e.g. not in an obvious looking laptop case, for example	5.5
PCDs should be used out of public view (if possible) and kept out of public view as much as possible.	5.5
PCDs should preferably never be left unattended, if they are, they should be locked away.	5.5
Laptop PCs should be configured in a way as to take account of operating system security, e.g. Windows 2000 security policy	5.6
Laptop PCs should employ BIOS, boot and hard disk passwords	5.6
All PCDs should have unnecessary services, ports and devices disabled.	5.6
PCDs should have OS and application settings set in a way as to maximise security.	5.6
Enable audible alarms on PCDs where possible to alert the user to e.g.	5.6

Portable Computing Device Security



someone trying to connect.	
Use a third party access control package, preferably one that offers biometric or picture-based access controls; don't rely on the device's access controls	5.6
Use software that provides a "logic bomb" in order to wipe data should access controls be breached, if feasible for your organisation.	5.6
Consider all data carried on PCDs and external storage as sensitive, however innocent it may seem.	5.7
Choose a suitable disk / file encryption tool and ensure personnel know via policy and training which data should be encrypted. Audit that they are using encryption and are remembering to use it for external storage as well.	5.7
Communications devices should be kept disabled between uses, e.g. disable Bluetooth.	5.8
Decide what communications technologies are authorised and disable those that aren't or remove the device.	5.8
Users should be within eyeshot of one another if doing peer-to-peer networking and initiate the connection by verbal request first!	5.8
Use a product that can help prevent unauthorised synching.	5.8
Change the default settings to secure communications devices; refer to our papers on wireless and Bluetooth to assist with this.	5.8
Have a different network logon to the device logon, preferably different to the one you'd use on your desktop and in a different user group with different policy.	5.8
Use external authentication if possible, e.g. RADIUS	5.8
Treat all PCDs as untrusted where possible, especially devices using wireless, they should be firewalled.	5.8
Consider using two-factor authentication to protect access to web-based resources.	5.8
Encrypt network / connections settings where possible, certainly avoid having passwords on the device, users should enter them manually.	5.8
Use a Secure VPN solution for protecting data in transit, especially if over wireless networks.	5.8
Consider using Microsoft Exchange 2003 ² or similar	5.8
Decide which policy you are going to have for external memory and ensure users adhere to it	5.9
If external memory is allowed, it should be kept separate from the PCD when not in use	5.9
Make sure your encryption policy covers external memory	5.9
Privately-owned external memory should be banned	5.9
Use a personal firewall, e.g. Zone Alarm on a laptop, eTGuard Pocket PC on PDAs.	5.10
Make use of a "human firewall"	5.11
Use anti-virus software and have an update policy	5.12
Ensure to implement a backup / synchronisation policy	5.13

² This version supports various mobile technologies and secure synchronisation of PDAs, etc.



5. Security Policy Guidelines

5.1 Introduction

Please note that the software mentioned in this document is described in more detail and has links provided in Section 6.

A security policy is a legal document that empowers you to take action if any of its rules are broken – you can't enforce what you don't have!

The next few pages give more detailed background to the checklist on the previous page, to assist with writing a suitable policy for PCDs. However, it should be noted that such policy needs to take into account related policies, some aspects of which may not be given in much detail in this document, such as:

- Wireless and network security policy
- Windows security
- Anti-Virus policy
- Backup policy
- Home-worker and mobile networking policy
- Remote access policy



5.2 General Usage Policy and Staff Awareness and Training

Many of the aspects below are considered in more detail later in the document. This is intended to be a guideline to policy specifically relating to personnel, and to staff awareness and training aspects.

All personnel:

Devices not allowed: Personnel should be informed that any PCD (PDA, laptop computer, and any other type of portable computing device which may emerge onto the market) are not allowed within the vicinity³ of the organisation without prior and written authorisation. They should also be informed that connecting to any networks with any devices other than devices they are authorised to use (e.g. their desktop PC) is forbidden.⁴ These points should also be written into the employee induction process and their contract of employment should refer them to the relevant policy/ies handbook. It should be clearly stated the disciplinary action that would be taken should they breach these regulations.

Suspicious activity: Personnel should also be informed that PCDs may be used to launch attacks on the organisation and should be required to report any “suspicious” activity. For example, personnel should be trained to be suspicious of someone outside or inside the building walking about with a PDA or laptop – is that person authorised or is perhaps hacking the network? Such staff awareness could avert a large number of attacks launched via wireless or wired networks if policy-makers thought to include this angle in their training.

Those personnel authorised to use a PCD:

Such personnel should be given (or informed where to find) copies of corporate policy pertaining to PCDs, and related policies. They should be given training upon issuance of such devices and only granted permission to use a device once they have been “signed off” as having received the appropriate training. This training should cover the items below (which should also be included as part of policy anyway):

Only business-owned devices should be authorised: privately owned devices and external memory should be forbidden (it is difficult to enforce controls on privately owned devices).

How to use the device: upon issuing a device, users should be trained how to use it from a general productivity perspective. This will avoid users wasting time by not being productive, and avoid accidental security breaches, through not knowing how to

³ “vicinity” because the presence of a WLAN will circumvent the ‘obvious’ physical boundary of your organisation/premises.

⁴ As to the above, if it is stated they are not allowed to connect this clearly covers if they try to connect to a WLAN (for example) outside the physical area of your building, e.g. in the car park.



do something, e.g. connect using Bluetooth and their mobile phone. This may also include training them on how to use individual applications and how to perform such tasks as synchronisation and file encryption, for example.

General Security Awareness: users should be made aware of the security risks surrounding using and carrying PCDs *and* external memory. They should be educated as to the value of data – many personnel just don't think about the value or significance of the data they are carrying, if they did, they would probably instinctively take more care.

Software/data: no personal data or programs should be allowed. Policy and training should state who is authorised to install software or change settings and what data is permitted to be on a PCD/memory card, for example. If someone has permission to install software, they should ensure it is approved software before installing it. Passwords and credit card numbers, etc., should not be stored on the PCD. All this may require tailoring to notional groups of personnel, e.g. some personnel may be allowed to add software, others may not, some people may be allowed to use e-mail and remote access, others may not. The aim of all this is to reduce the chance of applications/data/settings being added or changed, potentially compromising security.

External memory: you need to decide if this allowed at all. If it is, you need to decide how it should be used as per the above and ensure to include this in policy and training. Policy should state that all such memory should be handed in for secure destruction if it fails. See section 5.9 for further details.

Encryption and other security controls: personnel should be made aware of encryption, access control (e.g. password) and anti-virus policies. They should be given the appropriate training to ensure they know how to conform to these policies.

Backup policy: users should be informed – and shown – how to ensure their device is backed up to avoid the risk of data loss (for example through device failure or theft). They should be informed of the synchronisation policy (which may just be all – or part of – backup policy for PCD devices). They should be trained how to implement this part of policy.

General security: Users should keep their ownership of a PCD obfuscated (section 5.4). Your policy and training should include physical security issues such as how a PCD should be secured when not in use. The training should, for example, include a demonstration of how a Kensington lock should be used (see section 5.5).

Reporting: Define reporting procedures for employees to follow if they discover a breach in security, e.g. inform a particular contact name and backup contact/s name/s immediately a device is lost or stolen. This should also include reporting suspicious activity (see “suspicious activity” under “all personnel” above).

Enforcement: should state that users should follow the appropriate security policies and should define how users are to use their devices in order to facilitate device, data



and connections protection. They should be told that failure to follow policy could result in recall of the device, possibly dismissal.

5.3 Deployment and Management of Devices

Following on from the previous section, below are pointers for policy for administrators themselves, rather than users. There are many software tools available to facilitate many of these requirements, see section 6.

Purchase of devices: administrators should ensure that there is a standard for the brand of equipment and attempt to ensure that only equipment that a) offers the best security options and management (e.g. logging) options, and, b) is compatible, is purchased. For instance purchasing devices that do not have wireless functionality – or that don't permit wireless PCMCIA or other cards to be inserted – could entirely avoid the security problems inherent in wireless technologies.

Responsibilities: who will be responsible for installing and managing the devices and for patches and upgrades.

Asset tagging: should be employed. See section 5.4.

Standard build: should be mandatory, based upon thorough testing of what software and settings are required. The standard build should also include a) additional access control software (see 5.6), b) encryption software (see 5.7) and c) anti-virus software (see 5.12). Cloning software available to help putting standard builds onto PDAs (see section 6). Care should be taken to configure settings as part of the standard build specification in such a way as to maximise security.

Limit user rights: preferably, a user should not be a local administrator on the device. Only administrators should be enabled to install and deploy devices and change settings. Users should not be allowed to make changes to standard build, e.g. by adding their own software. If certain users are allowed to add software to their device, policy should state that they should only install authorised software. Use of permissions and user/groups can be used to limit what a user can do. This will mean that you can keep control of the device – and therefore its security.

Checks for rogue devices: administrators should regularly perform checks, as part of policy, to ensure that only authorised personnel have PCDs. This could be implemented by ensuring that heads of departments or supervisors know who is and is not allowed such devices and to ask them to report any unauthorised devices. They should be informed that evidence of an unauthorised device may be the presence of a synchronisation cradle at someone's work area, as well as someone using a PCD. This method should enable rogue devices to be identified and removed before a more serious security breach occurs. Such devices are often those that through poorly configured security or lack of awareness of the owner, have the greatest potential to breach security.

Checks for security: administrators should check devices on a regular basis to ensure that the devices continue to conform to policy, e.g. settings have not been changed, or



programs added which may compromise security. They should interview users to ensure that they are continuing to use devices according to policy – people get lazy.

(Details of tools that can assist with many of these processes may be found in Section 6).

5.4 Asset Tagging

All PCDs should be tagged, their details and those of the user recorded on a database. This will facilitate speedy identification of unauthorised “rogue” devices, which will be those not documented on the asset register. It will also assist in the safe return of devices should they fall into the hands of an honest person. It will also assist for insurance purposes should the device be permanently mislaid or stolen.

Kensington sell a tracking device called “CompuTrace”⁵ which enables tracking and recovery for laptop PCs, as well as motion detector alarms. Such products may be useful in that they can, with use of appropriate stickers on the device, act as a deterrent to all but the most determined attacker. There are likely to be such products available for a PDA.

Australian Projects sells a product called “STOP anti-theft system” (<http://austprojects.com.au/stop.htm>) which provides a numbered identification plate beneath which lies an indelible registration number and a “stolen equipment” warning. They also provide a red warning sticker, which can be affixed to the device. Again this is a deterrent but since there are still a lot of honest people about, such a technique will enable an honest person to report a mislaid device that can then easily be tracked to its rightful owner.

A company called Idstrip.com (<http://www.idstrip.com>) provides labels with an identifier that identify the machine to that company should the finder phone the number on the label.

A related issue is whether or not to have owner information on the device. If someone obtains unauthorised access to a PDA, they can use such information for social engineering. In addition, depending on the company name that is showing, it may make it even more tempting for a potential attacker to find a way to subvert the device than if the owner information didn’t exist or had something trivial such as “brain” on it. Whilst owner information can be useful to enable a device to be returned to you if it goes missing, it is better to rely upon some form of asset tagging service as the means to get the device returned.

If a third party asset tagging method is really not an option, then the owner information should have a telephone number – preferably unlisted – that someone

⁵ <http://www.kensington.com/html/1145.html>



could call in a situation where they find a mislaid device. The phone number should be answered without giving out any company details.

In this case, you would make it part of policy to forbid users to enter owner information. If this really cannot be done, then at least *untick* the “show information when the device is turned on” box within the “owner information” settings (Windows CE)⁶.

5.5 Physical Security

Policy could include the following, for example:

Locks: Kensington or other locking devices should be used when possible and appropriate, in order to secure the device to a fixture or fitting that is not easily moved. It is perhaps surprising that people will loop the cable around something that can be easily lifted up - users need to be made to think about what they are doing.

Whilst there are not so many ways currently on offer to secure PDAs compared with laptops, this is likely to change due to demand. Force (<http://www.force.com/>) sells a product called “The Bond” which they describe as compatible with Palm III, Palm IIX, Palm VII, IBM WorkPad PC and Symbol SPT-1500 devices.

General best practice: these tend to be based on obfuscation and not leaving a device unattended without due care:

- Devices should be kept locked away when not in use, and a Kensington and/or Bond device (see previous page) should be employed where possible.
- When travelling, devices should be transported in a way such as to obfuscate them. It is preferable to avoid using an “obvious” looking laptop or other case. This very simple technique would avoid many of the thefts that occur!
- Devices should be kept out of public view as much as is possible – if someone sees you have one, they might begin thinking about ways they could steal it or connect to it! If possible, if a device needs to be used, the user should go somewhere private to use it and keep it locked away when not in use.
- PCDs should never be left unattended. Devices should not be left in cars, for example. If a device must be left in the hotel room, it should be locked in the hotel room’s safe. If the item is too big for the safe, it should be locked in a case (preferably not an “obvious” looking laptop case) and hidden from view; perhaps hidden behind a chair and locked to a central heating pipe for example. External memory cards and other external memory devices should be removed and kept with the person in their wallet or purse and kept in a place separate from the device that uses it.

⁶ Note that even if the “show information” box is unticked, the basic details such as name, company and phone number will still be shown on the “today” screen anyway!



5.6 Access Control

Laptop computers

Laptops should be dealt with using the same security policy as desktop PCs but with even more vigilance due to their portable nature. For example, suitable password policy, NTFS or Linux file permissions, turning off shares, disabling guest accounts, enabling a good lock-out policy, not displaying last user, disabling unnecessary services and ports, etc. Don't let the user have administrative rights. In addition, BIOS passwords, boot passwords *and* hard disk passwords should be employed. Make sure your BIOS settings have the hard disk as the bootable device (disable boot from floppy/CD). Preferably, only the administrator should know the BIOS password - then only they can access the BIOS to make changes. It would be good - if possible - for the user to have a username and password different from the domain logon used on their desktop. A disk encryption product should be used for sensitive data and additional access controls, if necessary.

PDA's and other such devices

PDA's will have one of the two major operating systems for PDA's: Palm OS (Palm Pilot, Sony and Handspring Visor) or Windows CE "Pocket PC" (Compaq and HP Ipaq, Casio, etc.). There are some PDA's such as the Sharp Zaurus that run on a Linux and Java™ platform too, and much guidance on the Web as to how to convert an Ipaq (for example) to the Linux platform.

Basic measures: such operating systems have similar problems to conventional operating systems. Basic measures are disabling unnecessary ports, services and devices and disabling communications services between usage.

Change default settings: default settings do not generally offer adequate security. All application and operating system settings should be checked and changed where necessary before deployment of devices, to ensure the device offers the maximum protection.

Audible alarms: Enabling whatever audible alarms are available can be useful (or make use of software that provides them). If an alarm is set to go off if the device is being tampered with, a request for data transfer is received, etc., the user will be alerted (if they are near enough to hear it!) and hopefully in time to prevent a security breach. There are motion detectors available for these devices, for example.

There are a number of password crackers on the market for Palms, e.g. www.palmgear.com ("Sword") and www.freewarepalm.com. Most likely there are also password crackers for Windows CE in the same way that there are for Windows (e.g. L0phtcrack, LC4 etc.). This means that the default access controls do not offer sufficient protection. It is highly recommended to employ a more comprehensive and secure solution via third party software, preferably a biometric or picture solution.



If it would be catastrophic if the data got into the wrong hands - you should consider using the type of access control that offers “logic bomb” capability, i.e., will wipe all the data on the device should access controls be breached. It is also advisable to enable audible alarm functions should access controls be breached.

Examples of access control software available are:

Biometric fingerprint readers: For example Authentec (<http://www.authentec.com/>) is a biometric fingerprint reader that can fit on the handheld.

Biometric hand writing recognition software: as a cautionary note it should be noted that if an attacker has found a document with the user’s signature, they may be able to copy this and log on anyway. Some products allow a password to be used in addition to the signature, which provides an extra level of security. Or users can use a word other than their signature as their biometric logon. Examples are:

- CIC Sign-on;
- KeCrypt also provides encryption solution;
- PDALok;
- Safeguard PDA

Picture-based access controls: two types:

- Those that allow access upon selection of the right combination of thumbnail images, e.g. Pointsec for Pocket PC and Safeguard PDA.
- Those that, through using a stylus to touch certain points of a picture, allow you to obtain access, e.g. Visual Key.

“Logic Bomb” Software: that will wipe data from the device should access controls be breached. This facility is optional in certain software such as the military grade PDA Defence.

5.7 Disk / File Encryption

It is advisable to keep all data encrypted on a PCD, however “innocent” it may appear. Whilst the data may not be sensitive in the classic sense, it may contain information that can be exploited for social engineering purposes as previously mentioned. Thus the safest approach is to consider all data as sensitive. However, this is unlikely to be feasible in a large organisation. Nonetheless, encryption of sensitive information should be a minimum requirement and policy should clarify what should be encrypted and the type of encryption to use.

128-bit encryption should certainly be used as a minimum and there are a number of products that can fulfil this requirement, either as their whole function or part of an access control solution. See section 6 for examples of such software.



5.8 Data Communications

There are various factors to consider when reviewing risks and potential vulnerabilities surrounding data communications. These can relate to laptop PCs as well as to handheld devices:

Unauthorised use of device: if someone obtains access to your device via theft, for example, and it has an account on the network and perhaps other settings such as WLAN, dial-up, etc., it may mean that person has an account on the network. Such unauthorised access to a PCD may thus result in a network compromise, not just a device compromise.

Unauthorised connections: unauthorised pairing of devices, for example.

Synchronisation: connecting via a cradle to your local PC/laptop/corporate network carries its own set of potential vulnerabilities.

Wireless connection (e.g. 802.11x) to e.g. a hotel WLAN for purposes of using their Internet connection, or connecting to a corporate WLAN for using the network, which may include using the Internet, synchronisation, browsing and using network resources for example.

Dial-up when “on the road”, using e.g. a Bluetooth, IrDA or cable connection to a GSM device (e.g. cell phone) which acts as the intermediary for using the resources of the Internet via the GSM device. Or via conventional dialup using a modem card connected to a hotel’s telephone system, for example.

Security Guidelines:

- Employ methods to reduce chance of loss or theft (see section 5.5);
- Decide which technologies are permitted and disable those that are not;
- Educate users to disable communications devices when not in use (e.g. if not using wireless, disable wireless adapter);
- Users should, where possible, verbally request a connection before making it and be within eyesight of one another (e.g. particularly relates to Bluetooth). This can help reduce the chances of unauthorised connections, not least because if it is policy that someone wanting to connect should ask first, if a connection request comes in and the person has not been asked, it can be assumed that the connection request is perhaps unauthorised. This is just another idea to add a layer.
- Use a product which can as part of its access controls (see section 6) prevent unauthorised synching via password protection;



- Users might not understand the significance of just pressing “ok” if they get a connection request they are not expecting. They should be informed of the risks and to click “no” if in any doubt whatsoever. [2]
- Change the default settings within communications services, which usually do not provide sufficient levels of security, e.g. enable 128-bit WEP (for 802.11x);
- Don’t store passwords on the device - untick any “remember password” boxes. This will require passwords to be manually entered each time, but will make it much harder for an attacker to use the device to attack your network. Preferably disable any Windows password stores (and their logon window) and deploy a third party access control instead.
- Disable “allow other devices to connect to me” (WinCE, may be different for Palm OS), and use encryption and suitable pairing passwords, etc;
- Have a network logon different from the device logon. Users frequently get set up on the domain with an “easy to enter” password because it is a nuisance to enter a long password onto a PDA. However, “easier to enter” equates to “easier to guess”, thereby compromising the security of the entire domain! Preferably use an external authentication method e.g. RADIUS or DigiPass.
- Treat all PCDs as untrusted, especially PDAs and any devices using wireless technologies, and only allow them to connect via a firewall;
- Consider using a two-factor authentication solution to protect access to web-based resources, e.g. RSA Mobile;
- Encrypt network / connection settings where possible and use a Secure VPN solution or something similar for protecting data in transit, especially over wireless network connections;
- Consider using Microsoft Exchange 2003 or similar (see section 6).

I have a separate paper on wireless (802.11x) security and Bluetooth security, both of which offer more in-depth guidelines for best security practice concerning these technologies.



5.9 External storage

This is worth a section all on its own, due to its significance as far as security is concerned. Memory sticks, CF (Compact Flash) cards, SD (Secure Digital) cards, Microdrives, USB flash drives and other external memory devices are small and somehow psychologically not associated with the serious data they may be carrying. This can lead to carelessness - the small size of such external memory lends them to be easily mislaid or stolen.

Users should be educated that such memory should be considered as important as the device that utilises it, and that it may actually be *more* valuable than the device itself, depending on the nature of the data contained within it!

There are three philosophies concerning deployment of external memory:

- a) **Keeping data on external memory only:** meaning that users are not allowed to store data on the PCD itself. This primarily relates to PDAs, unless you consider having removable hard drives for your laptops using this same philosophy. In this situation, a user keeps all data, therefore reads/writes to, the external memory device which, when the PCD is not in use, is removed and kept separately from the PCD (e.g. in the user's wallet). This is, of course, analogous to keeping a cheque card separate from cheques. If the PDA is stolen, so long as the card has been removed, there will be no valuable data on the PDA. You could then purchase PDAs with just enough non-volatile memory to store programs, which could help reduce the chances of data being written to the PDA. Of course, encryption should be used for data, whether it is on the PDA itself or the external memory.
- b) **Banning use of external memory completely:** in this case, the thought is that users won't be using – and perhaps losing or having stolen – external memory. To facilitate this approach, PDAs would need to be purchased that have sufficient internal memory for programs *and* data and, in addition, preferably purchase devices that don't have the facility for attaching external memory.
- c) **Keeping some data on external memory, some on PCD:** this may be essential, for example where a PDA does not have the internal memory to cope with demand. However, policy should dictate what, and what not, to store on external memory, and the encryption policy surrounding that data. Users should be educated on the value of external memory. They should be informed that that they are not allowed to store personal data or programs on the external memory (in the same way as they aren't on the PCDs themselves). They should also be informed that privately owned external memory devices are forbidden.



5.10 Personal Firewall

A personal firewall should be employed on all PCDs, e.g. Zone Alarm for laptops and desktops. There are personal firewall and IDS systems emerging for PDAs, but these are somewhat limited at the moment. It seems that CheckPoint may have one on offer.

5.11 Human Firewall

Staff (especially reception staff) should be encouraged to be aware of the dangers of visitors bringing such devices onto the premises and should be required to report if a visitor is carrying such a device. Certain organisations may consider installing some kind of scanning device at reception that visitors have to walk through that may detect the presence of such devices. All staff should be encouraged to report any suspicious activity (e.g. someone sitting in their car with a PDA or laptop that looks suspicious may be an intruder attempting to connect to the wireless network, for example).

5.12 Virus and Malicious code – AV Policy

The rest of this section will refer specifically to PDAs, because it is likely that laptop PCs use the same AV policy as desktop PCs, although this should be checked!

Viruses that have been directed towards the PALM OS are PalmOS.Liberty.A, PalmOS.Phage.A, PalmOS.Vapor.A. There do not seem to be any targeting Pocket PC ... yet[6].

The hardware constraints imposed on PDAs tend to mean that the operating system⁷, and many of the applications that have been designed to run on them, are stripped-down versions of those that run on conventional PCs. This also means that such programs have weaker security than their PC equivalents. It may be that boundary checking has been eliminated in some areas, so facilitating the potential for buffer overflow attacks. [2]

Whilst PDAs haven't been a target for malicious code attacks so far, that is likely to change as such devices become more commonplace and attackers realise the potential of exploiting them. Meanwhile, one of the major concerns is the ability of PDAs to act as transport vectors for malicious code onto the corporate network. For example, were a user to open an e-mail attachment that contained malicious code (e.g. a virus) on their PDA, whilst the malicious code may not affect the PDA itself, it could be carried onto the corporate network upon syncing.

⁷ Windows CE, for example is a stripped down version of W95 with a few applets added [5]



Thus, as with any other type of computer, it is important to implement some form of anti-virus policy on PDAs. There are two types of virus scanner for PDA:

- a) **Local:** those that run on the PDA itself. F-Secure's Anti-Virus for Pocket PC is an example of such a scanner, which scans e-mails as well as files loaded onto the PDA. Updates are pushed to the device from the user's PC or may be downloaded via a wireless connection. There needs to be policy for how updates are handled and the frequency with which a user should obtain them. Note that the volume of virus signatures may give a problem with memory on some devices.
- b) **Remote:** the virus signatures sit on a server (e.g. the machine to which the PDA is to be connected for synching). When the PDA (client) connects for synchronisation via a PC or directly onto the network, it connects to a server which scans the PDA before any infections can occur. McAfee's "VirusScan PDA" is an example of this type of scanner, which scans PDA files upon synching. However, Sophos say that if their product is installed on the desktop, its on-access scanner will detect any viruses transmitted when the PDA or mobile phone synchronises with the desktop PC" - so it may be that having a good desktop solution is enough...

5.13 Backup Policy

Your policy should state how backups should be implemented.

If the device is used for manipulating data, rather than just referencing it (i.e. where it is contained elsewhere) backups should be carried out at least once a day. Thus your backup policy will really be dictated by the way in which devices are used.

If a member of staff is out in the field, then hopefully they will have a laptop PC with which to synchronise their device. If not, perhaps they could use an external memory card for backing up data (and keep the card separately from the PCD, as mentioned previously).

It may be that synchronisation is the way in which backups are performed, therefore synchronisation policy will be synonymous with backup policy. If this is the case, staff should be informed that this synchronisation process provides the only way of backing up their data, then they will take more care about doing so!



6. PDA Software

This section attempts to give a good overview of software tools that are currently (Sept 2003) available for PDAs. The software is listed in alphabetical order under each category.

Handango (<http://www.handango.com/>) is one of the best resources for PDA software on the web. Much of the software listed below is available from there ...

6.1 Encryption & Access Control Products

Some of the below offer both Encryption and Access Control, others offer each as stand-alone features.

<p>CIC Sign-on</p> <p>http://www.cic.com/products/signon/</p>	<p>Their site says, "...is the first log-on security utility for handheld organizers that uses biometric signature verification to keep the data on your device safe! Sign-On will allow you and only you to gain access to the data on your organizer. Just sign your name or create a personalized drawing or design and Sign-On will verify your signature or personalized design to unlock the device."</p>
<p>Cryptinfo</p> <p>http://www.cryptinfo.com/cryptinfo/index.shtml</p>	<p>Their site says, "CryptInfo is a secure password manager for the Palm and the PC. Securely store your passwords, credit card numbers, and more! Synchronize your information between your PC and your Palm device. Your privacy is protected with strong encryption technology that scrambles your information so that only you can see it!"</p>
<p>Digipass for Pocket PC</p> <p>http://www.vasco.com/products/product.html?product=24</p>	<p>Their site says, "Many Pocket PC devices have wireless connectivity capabilities, relying on WAP, GPRS or similar technologies. With such connected Pocket PC's, Digipass provides strong user authentication and digital signatures for over-the-air mobile commerce transactions." "Multiple profile support is one of the many features of the Digipass for Pocket PC. It allows more than one virtual token on one Pocket PC, each with its own secret key for access to different servers, networks and web sites."</p>
<p>F-Secure FileCrypto™</p> <p>http://www.f-secure.com/products/filecrypto/</p>	<p>Their site says, "...protects stored data from unauthorized access. The solutions are strong, automatic and transparent to the end user."</p>
<p>Handango Security Guard™</p> <p>http://www.handango.com then search for it.</p>	<p>The site says, "a robust enterprise-class security tool that enables file and folder encryption ...this application secures data and controls application access...168-bit encryption..." Note that Handango have many other security products available too.</p>
<p>Kaspersky® Security for PDA</p>	<p>See anti-virus software section.</p>
<p>KeCrypt</p> <p>http://www.kecrypt.com/home.htm</p>	<p>Their site says: "KeCrypt – as unique as your signature KeCrypt's unique patented technology is the world's first to offer genuinely effective security based on new biometrics and PKI technology".</p>

Portable Computing Device Security



<p>Microsoft Exchange 2003</p> <p>http://www.microsoft.com/exchange/evaluation/overview/</p>	<p>As well as the usual features, this provides support (it replaces MMIS – Microsoft Mobile Information Server which has now been discontinued) for mobile devices. It can for example help secure data in transit and can also manage how user' use their devices, i.e. which applications need security as well as securing synchronisation.</p>
<p>MobiPassword™</p> <p>http://www.mobipassword.com/</p>	<p>Their site says "MobiPassword is a multi-platform Personal Identification organiser, providing an all-in-one solution for the security, mobility and automatic use of your personal identification information." "... the only application featuring automatic matching of login names and passwords to their place of use."</p>
<p>movianCrypt™</p> <p>http://www.certicom.com/products/movian/moviancrypt.html</p>	<p>Their site says "movianCrypt™ integrates a password-based user log-in system with strong encryption technology to achieve data security on your Palm OS or Pocket PC device ...transparent to end users...automatic encryption."</p>
<p>PDA Defense™ <i>(previously known as "PDA Bomb")</i></p> <p>http://www.pdadefense.com/enterprise.asp</p>	<p>Their site says "the industry standard in PDA data security, provides multi-layered security for Palm, Pocket PC and Blackberry devices." "With its high level of security [it is] being used within all branches of the military, the White House, the FBI and civilian enterprises throughout the world." It lets administrators mandate security settings and push them to a PDA upon synchronisation. It also provides data wiping if access controls are breached.</p>
<p>PDALok</p> <p>http://www.pdalok.com/</p>	<p>Their site says, "PDALok™ is security software added to your Pocket PC that restricts access to unauthorised users unless a live signature from the rightful owner is presented. It locks it from access or from synchronisation, so all data held on your Pocket PC is fully protected.</p>
<p>PDASecure Enterprise</p> <p>http://www.trustedigital.com/prod16c.htm</p>	<p>Their site says that the product offers "centralized managed security, database encryption, sync protection, beam protection, wipe password, configurable by end user and administrator, single-key encryption, 3DES, AES, you can select specific applications to protect, directory integration with NT Domain, ODBC & LDAP." They also offer a range of other products "each addressing a unique area of need in total security architecture."</p>
<p>PGP Mobile</p> <p>http://www.pgp.com/products/enterprise/mobile.htm</p>	<p>Their site says: "PGP Mobile for Palm OS devices provides capabilities similar to PGP Disk for secure data storage and PGP Mail for secure messaging. PGP Mobile for Windows CE provides the secure-messaging capabilities of PGP Mail for Pocket PC devices, allowing PGP Mail-compatible messages to be sent and received securely. PGP Mobile also syncs PGP-specific information such as key-rings between Windows computers and handheld devices." However, different options are available for Palm OS compared to Windows CE.</p>
<p>Pointsec for Pocket PC</p> <p>http://www.pointsec.com/solutions/</p>	<p>The list of features on their site says "Real-time encryption, removable media encryption, media encryption policy, enforceable mandatory access control, Picture PIN™ authentication, QuickPIN™ authentication, central administration with Pointsec profiles, user account lockout, authenticated ActiveSync, user transparent encryption, remote help, XTNDConnect management abilities".</p>
<p>SafeGuard PDA</p>	<p>Their site says: "... a powerful solution to protect your</p>

Portable Computing Device Security



<p>http://www.utimaco.de/eng/indexmain.html</p>	<p>[PDA] and the data stored on it against unauthorised access." "... Innovative authentication mechanisms such as biometric signature recognition or Symbol PIN offer optimal user convenience, the strong encryption protects your data while stored or in transit over the Internet, the centrally enforceable security policy keeps your environment consistently protected."</p>
<p>Secure Star – various encryption products</p> <p>http://www.securestar.com/</p>	<p>Their site says, "The leader for real-time hard disk encryption" and they do many such products.</p>
<p>Sentry 2020</p> <p>http://www.softwinter.com/sentry_ce.html</p>	<p>Their site says "...enterprise security tool utilising transparent encryption...128-bit, operates at the volume level so is faster..." The site also has other useful PDA tools as well.</p>
<p>Visual key</p> <p>http://www.viskey.com/</p>	<p>This is a picture-based access control product where access will only be allowed if certain previously defined spots in the picture (one of theirs or one of your choice) are clicked upon in the correct order. Palm OS and Pocket PC are supported and there is a PC version too – a really useful product.</p>

6.2 Anti-Virus Products

<p>avast! 4 PDA Edition</p> <p>http://www.avast.com/i_idt_155.html</p>	<p>Their site says that this product is not due for release until summer 2003. It announces the product as being "... designed to protect pocket devices (PDA) from viruses. The importance of PDAs is growing every day, and so these devices are likely to be a target of virus attacks rather soon. As their connectivity gets better and better, such an attack is easier to do" and says both Palm OS and Windows CE are supported.</p>
<p>F-Secure Anti-Virus for Pocket PC</p> <p>http://www.europe.f-secure.com/wireless/pocketpc/pocketpc-av.shtml</p>	<p>Their site says "...is an anti-virus software solution that runs locally on the pocket PC device. It provides up-to-date and always available protection...since the solution runs on the mobile device, it is able to detect and delete also all malware that enters the device through wireless connections."</p>
<p>Kaspersky® Security for PDA</p> <p>http://www.kaspersky.co.uk/buyonline.html?info=971980</p>	<p>Their site says: "...a comprehensive approach to anti-virus protection of data stored on PDAs, as well as information transferred via PC or extension card." It also "protects against unauthorized access to data stored on PDAs as well as secures access to the portable device itself using a password system. The ability to block access to PDAs running Palm OS for fixed time periods."</p>

Portable Computing Device Security



<p>McAfee's VirusScan™ Wireless</p> <p>http://www.networkassociates.com/us/products/mcafee/antivirus/remote_user/vs_wireless.htm</p>	<p>Their site says: "McAfee® VirusScan™ Wireless, the first member of the McAfee Wireless product family, is a comprehensive virus security solution for mobile and handheld devices, such as PalmPilots and PocketPCs, that connect to your network. As millions of users turn to powerful, pocket-sized devices, the threat of infection through PDAs increases. VirusScan Wireless is a comprehensive way to guard against this threat. "</p>
<p>Sophos</p> <p>http://www.sophos.com/products/sav/</p>	<p>Their site states that, "The threat of viruses infecting PDAs and mobile phones has been widely hyped by some anti-virus companies. However, it is possible for PDAs to carry a virus into a company (thus avoiding any email gateway protection), and for the suspect file to be copied onto your desktop from the PDA. Sophos Anti-Virus protects against this kind of infection through its on-access scanner, detecting any viruses transmitted when the PDA or mobile phone synchronises with the desktop PC."</p>
<p>Symantec AntiVirus for Handhelds</p> <p>http://ses.symantec.com/products/products.cfm?productid=237</p>	<p>Their site says: "... Palm OS and Pocket PC compatible ... deployed and installed to the desktop and then automatically transferred to the handheld device during synchronization ... Wireless and synchronized LiveUpdate™ support ensures up-to-date virus definitions for the handheld. In addition, synchronized LiveUpdate™ enables simultaneous enterprise-wide deployment of virus definitions to desktops using Symantec AntiVirus Corporate Edition."</p>

6.3 Backup

<p>Pocket Backup</p> <p>http://www.spritesoftware.com/products/pocket_backup_plus.html</p>	<p>Their site says: "backup directly to your host PC or a Network using the convenient PC Agent. You can backup when connected via ActiveSync or any form of wireless networking (Win XP and Win 2000 only). There is a lot of other functionality – see their site for details.</p>
<p>CF card Backup</p> <p>http://www.handango.com then search for it</p>	<p>Handango's site says: "CF card Backup for Pocket PC 2002 Card Backup Tool lets you quickly and easily backup your Pocket PC memory data to a memory card. Backed up data can be used to restore your system should it start to malfunction due to some data error. Card Backup Tool can let you choose to save ALL Files or PIM Files only. Card Backup Tool can let you choose the Saving Place before Backing up or Restoring it. Select the Saving Place.(Built-in Storage or CF card Storage)."</p>



6.4 Network Analysis and Administration Tools

<p>AirScanner Mobile Sniffer</p> <p>http://www.handango.com and search for it</p> <p>Note such a product could be used in conjunction with the “mini” version of the well-known NetStumbler, and other similar software to be found on our wireless paper.</p>	<p>Handango’s site says: “As a network administrator, you want to protect your users’ confidential data. What better way to do this than to stroll down the hall with Airscanner™ Mobile Sniffer hidden in your pocket? Thanks to our support for Ethereal packet capture format, grabbing your user’s passwords out of the airwaves is as easy as watching a movie! Your users unintentionally send their passwords through the air in clear text, so it is better that you discover this first before a malicious drive-by hacker does it for you. Airscanner™ Mobile Sniffer also works in promiscuous mode, so you can also discover unauthorized users who may be associating with one of your access points.”</p>
<p>Backbone Software NT Services</p> <p>http://www.handango.com and search for it</p>	<p>The Handango site says “... a web based tool for Microsoft windows server administrators that need to monitor, access and edit windows services from remote locations using a pc, pda or a smartphone”. “... Administrators can easily browse their way through workgroups and computers to get an overview of the running, stopped and disabled services on any computer in their network, view detailed information about the computers eventlog, View, start, stop and restart IIS websites, backup IIS metabases, reboot remote servers/workstations, kick/logoff/disconnect terminal service users, kill hanging processes and more.</p>
<p>iAdmin Mobile 2002</p> <p>http://www.jrbsoft.com/solutions/iadminmobile.asp</p>	<p>This tool lets you remotely manage your “Windows NT/2000 or XP infrastructure right from the palm of your hand” so it is different from the other tools in that it is not a tool to manage PDAs, but a tool for administrators to manage their network! Of course such tools can be used for illicit purposes, so it is useful to point out that they exist!</p>
<p>PE Explorer Suite 2003</p> <p>http://www.handango.com and search for it</p>	<p>Handango’s site says it is the most powerful explorer for Pocket PC, can help manage zip files, browse and manage network resources “will fulfil all your file management needs, whether they reside locally, remotely on FTP server or remotely on your windows network.”</p>
<p>Pocket Controller Enterprise</p> <p>http://www.handango.com and search for it</p>	<p>A powerful tool which offers “remote manage and support mobile devices from a central location. Connect to remote mobile devices using Wired or Wireless TCP/IP LAN/WAN, ActiveSync, modem or cellular connections. Support for direct connections or through HTTP, SOCK4, or SOCK5 proxies. Create administrator and user accounts, allow/deny privileges, allow users to accept/reject remote control session requests, configure authentication and encryption settings. It can also view the remote file system or to transfer files to remotely view or edit the registry of remote devices, provides audit logging, printing features, remote DOS box and much more” according to Handango’s site.</p>

Portable Computing Device Security



<p>PocketLANce</p> <p>http://www.pocketlance.com/</p>	<p>A "unique" tool for browsing, managing and transferring windows network resources from pocket PC, can work via ActiveSync connection or via RAS or DUN, it integrates with standard File Explorer on Pocket PC and supports different network access rights and security levels with an optional peer-to-peer operation mode."</p>
<p>z2 PocketLAN</p> <p>http://www.handango.com and search for it</p>	<p>Handango's site says: "... a dedicated network software, main features: enable network folder in pocket file explorer, auto scan remote computer names and browse, open remote computer files, auto detect network connection, reconnect to network resource when it is available, etc.</p>
<p>PocketMySQLAdmin for Pocket PC</p> <p>http://www.handango.com and search for it</p>	<p>Handango's site says: "Connect to a MySQL database server anywhere in the world, maintain multiple Database server profiles, perform full queries and view results, select, update, insert, delete and all other MySQL supported queries supported by the software. Create and delete databases and tables, password protected interface, add delete and modify user rights, works with MySQL version 3.X onwards and supports all Pocket PC PDAs.</p>
<p>Pocket Nanny</p> <p>http://www.handango.com and search for it</p>	<p>Very useful tool that Handango describes as "... an application designed to assist an IT department lock down their deployed base of Pocket PC based devices, so only desired applications can be used."</p>
<p>PortTrakker</p> <p>http://www.handango.com and search for it</p>	<p>Handango's site says: "PortTrakker is the most feature rich and comprehensive TCP/UDP Port Database available for the Pocket PC."</p>
<p>Sprite Clone</p> <p>http://www.spritesoftware.com/products/sprite_clone.html</p>	<p>Their site says "Sprite Clone simplifies the deployment of Pocket PCs across an Enterprise. Set up one Pocket PC, capture a complete image of it, which includes the file system, databases and registry, and deploy this image to your target Pocket PCs." so a very useful tool.</p>
<p>TigerSuite PDA</p> <p>http://www.tigertools.net/tt2kpda.htm</p>	<p>Their site describes it as "Network Security Assessment Software plus network tools" and says "includes modules for remote scanning, service detection, penetration testing, network and file tools such as a hex editor, IP subnetter, host collaboration and remote Trojan scanner with remediations. The suite operates from Main Memory or Storage Card and is compatible with wireless, IrDA and LAN internet and/or network connections."</p>



7. Bibliography

[1] Roberto Di Pietro and Luidi V. Mancini. Security and privacy issues of handheld and wearable wireless devices. In *Communications of the ACM* (September 2003/Vol. 46. No. 9).

[2] Roberta Bragg. Protect your PDAs, PDQ! *MCPmag.com* (February 2003).

[3] John Phillis. Recommendation for a Security Utility to protect Palm organisers.

[4] John Leyden. PDA security slackers, the lot of you. In *The Register* (9 September 2003).

[5] Brian M. Posey MCSE. PDA security with Windows CE. In *TechRepublic* (April 29, 2003, 08:46 BST).

[6] Dave Croxton. PDAs in the Corporate Environment. In *Sans reading room*. (Sept 5, 2001)

[7] Richard Price. The PDA as a Threat Vector. In *SANS reading room*. (March 2003).

[8] Nelson Beach. Handheld Security: A Layered Approach. In *SANS reading room*.

[9] Darrin Murriner. Pocket PC – Secure or Unsecured? In *SANS reading room*. (2001)

For more information, contact First Base Technologies: 01273 454525 / info@firstbase.co.uk.