NIST United States Department of Commerce
National Institute of Standards and Technology

Mobile Device Survey

DRAFT NIST Interagency Report

June 2002

Tom Karygiannis
Wayne Jansen
Vlad Korolev
Serban Gavrila

Table of Contents

Index of Figures and Tables

1. Introduction

This survey provides an overview of the hardware and software capabilities of Palm, Pocket PC, and Linux-based Personal Digital Assistants (PDAs). The survey provides an overview of general characteristics and, where useful, focuses on a particular model or software version to illustrate the best features of the product line. Since our interest is in the development of security mechanisms for these devices, we also discuss the different software development environments and a summary of commercially-available and open source security mechanisms available for each PDA family. Handheld device technologies are changing rapidly. New products and features are being introduced almost daily. Because of the fast pace with which handheld device technologies are evolving, this document represents a snapshot of the handheld market at the present time. Much of the information has been gathered from vendor web sites and the links have been included to provide access to the most up-to-date information.

2. PDA Platform Families

This section provides an overview of the hardware configurations of low- and high-end PDAs of interest. The discussion focuses on their distinguishing physical characteristics (e.g., size, weight, processor speed, memory capacity) and hardware expansion capabilities (e.g., flash ROM programmability, external interfaces). Table 1 highlights the general characteristics of selected Palm, Pocket PC, and Linux PDA models.

	Samsung SPH-I300 PDA/phone[1]	**iPAQ Pocket PC H3850[2]**	**Zaurus[3]**
Size	4.9” x 2.28” x 0.82”	5.3" x 3.3" x .62"	5.5” x 3.2" x 0.79"
Weight	6 Oz	6.7 oz. Including battery	220 g Including battery
Processor	Motorola DragonBall VZ 33 MHz	206 MHz Intel StrongARM 32-bit RISC Processor	206MHz Intel SA-1110 StrongARM processor
OS	Palm OS 3.5	Microsoft Pocket PC 2002	Lineo's Embedix Embedded Linux with Linux kernel 2.4.x
RAM	8 MB	64 MB	32MB DRAM and 16MB Flash
Display	256 color screen	Color reflective thin film transistor (TFT) LCD, 64K colors	240 x 320 dots, 65,536 colors, 3.5-inch reflective-type color TFT LCD (with frontlight)
Input	Touch-screen	Handwriting recognition, soft keyboard, voice record,	Keyboard, stylus, scroll keys
Battery	Battery installed (max) 1 - Lithium Ion	1400 mAh Lithium Polymer	3.6 V, DC lithium-ion rechargeable battery (AD-T51BT)
Expansion Slots	None	SD Memory Slot, Optional expansion packs for PCMCIA and CF	CompactFlash type II , Secure Digital (SD) card slot for secure memory storage or other
Price Range	$500	$620	$550

Table 1: A Hardware Comparison of the latest representative PDA models

[1] Complete specification http://computers.cnet.com/hardware/0-2709830-404-7703904.html?tag=topfive
[2] Complete specification http://www.compaq.com/products/handhelds/pocketpc/H3850.html
[3] Complete specification http://amiga.emugaming.com/sharp/zaurusspecs1.html

An overview of the characteristics and prices ranges of a wider range of PDAs can be found on vendor web sites and product review sites.[4, 5]

2.1 Palm PDA

Palm was able to establish itself as the market leader in the PDA market by focusing on simplicity and ease-of-use. Palm was able to capture 80% of the market by 2000, but strong competition has reduced Palm's market share over the last two years. Palm devices use 16- and 32-bit processors based on the Motorola DragonBall MC68328-family of microprocessors. The latest Palm PDAs offer two expansion modes: the Palm Expansion Card Slot and Palm Universal Connector System. The Palm Expansion Card Slot accommodates MultiMediaCard and Secure Digital (SD) cards. The MultiMediaCard[6] is a removable solid-state Read Only Memory (ROM) and is less expensive than the SD cards. Secure Digital SD Card[7] memory capacity ranges from 8MB to 128MB and has better speed, security features, and I/O capabilities than the MultiMediaCard. The Palm Universal Connector System will be the hardware add-on module standard for all future Palm devices. Handspring has licensed the Palm OS and sells their own PDAs with the main distinguishing feature being the availability of a variety of expansion modules. Handspring makes the proprietary SpringBoard development environment available to its developer community to encourage the production of new modules by third parties. Currently available Handspring expansion modules include GPS, video, audio, wireless modems, and storage modules.[8]

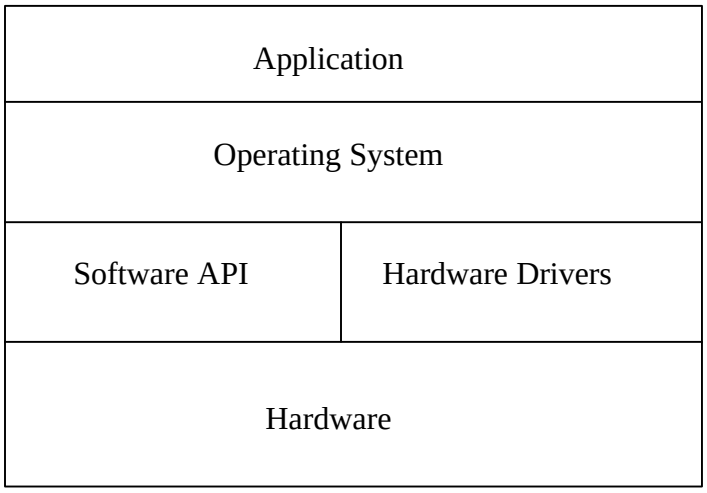

Figure 1: The Palm OS Architecture

The Palm OS is a proprietary operating system, but the source code is available for licensing. The Palm OS is single-threaded and is not generally considered a secure

[4] For PDA product reviews and prices on the latest models see http://www.cnet.com
[5] For an online comparison of PDAs http://www.davespda.com/resources/compare/
[6] The MultiMediaCard home page http://www.mmca.org
[7] The Secure Digital home page http://www.Sdcard.org
[8] For a complete list of SpringBoard Modules see http://www.handspring.com/products/sbm_all.jhtml

operating system as a user or an application can access program code, data and the processor itself. The Palm OS is stored in ROM while applications and user data are stored in battery-powered RAM. Date is stored in records and records are grouped into databases where the database is analogous to a file.

2.2 Pocket PC

Microsoft's first entry into the PDA market was with the Windows CE handheld operating system that is now called Pocket PC[9]. Although the first releases of these PDAs were not as easy to use and considerably more expensive than the Palm PDAs, these devices have shown marked improvement and are leveraging all of Microsoft's resources from desktop application compatibility to software development tools. The Pocket PC grew out of the success of the Palm PDA and the realization that a market existed for similar devices that had more processing power and networking capabilities. Microsoft has included handheld devices in its new .Net strategy to encourage developers to build applications that can be accessed from a wide range of Microsoft platforms. Having Microsoft backing in any new technology area is a formidable advantage and the Pocket PC will certainly benefit from Microsoft's financial and technical support.

The architecture of the Pocket PC is shown in the diagram below. The services are grouped in a number of modules, which can be included or excluded when building a Pocket PC image for a specific target system. Everything up to the programming and communications interfaces level is part of the operating system; above that are the applications.

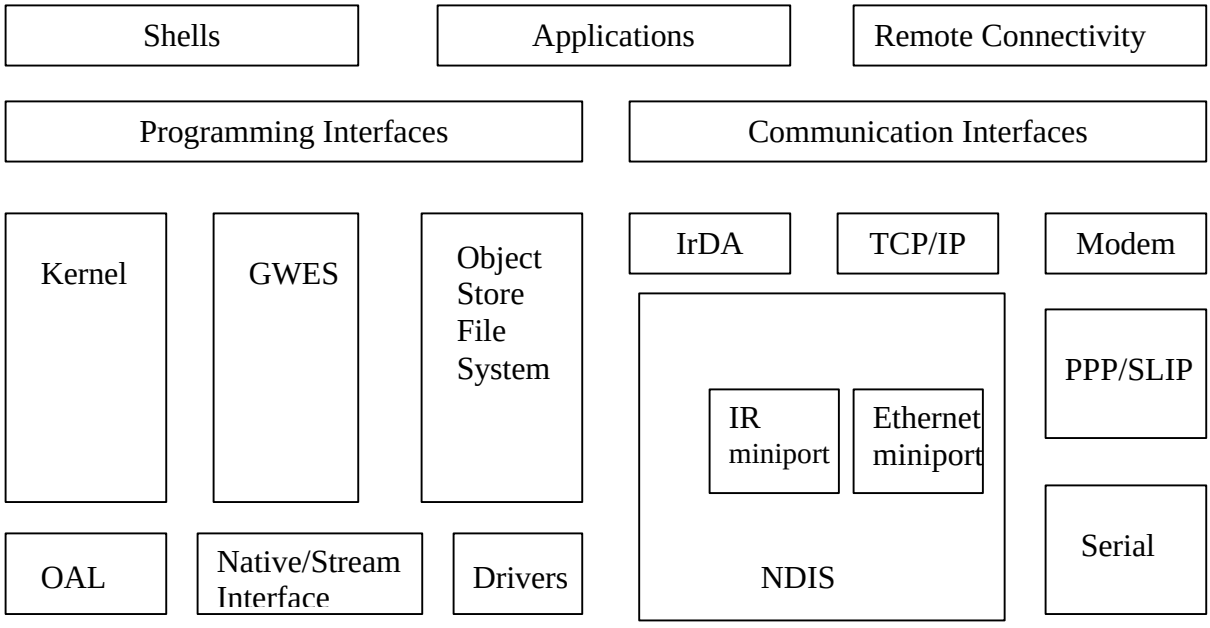

Figure 2: The Windows CE Pocket PC Architecture[10]

[9] See http://www.microsoft.com/mobile/pocketpc/default.asp
[10] http://www.gesytec.de/common/html/embedded-pc_help/architecture.htm

Pocket PC allows the hardware developer, system integrator, or developer to determine which services are incorporated in their Pocket PC version. The Pocket PC components use a subset of familiar Microsoft API's. This allows Pocket PC system to fit to the requirements of any embedded PC application, while keeping the programmability of PC's by using the subset of Win32 and other Microsoft API's that have been implemented in Pocket PC.

Pocket PC runs on the Compaq iPAQ, HP Jornada, and Tablet PC. It has just recently been upgraded to a 2002 version and supports a completely new development environment reportedly much better than that for the previous version. The Compaq iPAQ has even more flexibility, supporting both compact flash and PC cards (their flash ROM can also be reprogrammed), and support Java (Insignia's Jeode). The iPAQ seems to be the leader in the Pocket PC PDA market. The Jornada supports industry standard compact flash devices for memory, communications, etc. (and uses 32 bit processors with significant memory). The Jornada has been discontinued, but some models are still being sold on the market.

2.3 Linux PDA

The Linux PDAs presently offer the same advantages and disadvantages encountered in the ongoing Linux open source debate. As technology advances are likely to allow for more processing power, and more on-board memory, the factors influencing the selection of a PDA operating system will become essentially the same as those influencing the choice of operating system for desktop workstations. Linux has had success in the server market. The success of Linux-based PDAs rests on the open source model and its ability to engage the software development community to produce useful applications.

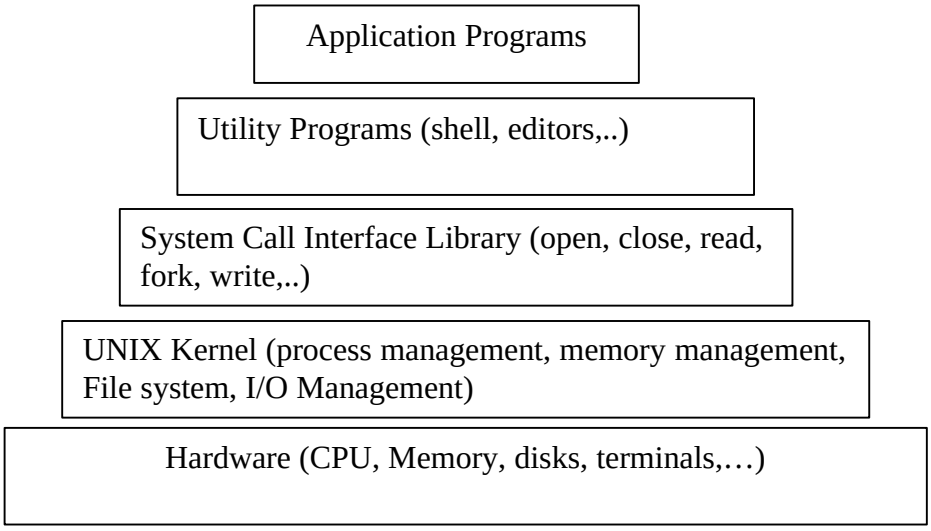

Figure 3: Conceptual Linux Architecture Diagram[11]

[11] http://se.uwaterloo.ca/~mnarmstr/report1/node9.html

The figure above shows a conceptual architecture for the Linux operating system. The Linux kernel is composed of modular components and subsystems that include device drivers, protocols, and other component types. The Linux kernel also includes the scheduler, the memory manager, the virtual filesystem, and the resource allocator. APIs, programming interfaces that provide a standard method by which the Linux kernel can be expanded, glues these to the core of the Linux kernel. Data flows from the system call interface requesting a service from the file or process control subsystem, which in turn requests a service(s) from the hardware. The hardware then provides the service to the kernel and passes data back up through the kernel to the system call interface. Control flow is passed from the system call, to the appropriate subsystem, down to the hardware, and then back up to the system call interface. Concurrency issues, however, may allow the control of a process to be transferred to another during a context switch in either direction.

The most common Linux PDAs are G.Mate's YOPY, Sharp's Zaurus, and the Agenda VR3. Linux also runs on iPAQ, and Tablet PC (there is also an effort for Palm devices), and is open source. Linux-based handheld devices are being introduced to the market at a very rapid pace. For the latest news on Linux-based handheld devices web sites must be monitored on a weekly basis.[12]

The Zaurus uses Embedix, an embedded Linux kernel from Lineo, and Qtopia desktop environment from Trolltech for the windowing and presentation technology. Embedix Plus PDA is based on a networked kernel with built-insupport for 802.11b, WiFi, Bluetooth and wireless modem technologies, as well as associated security and encryption modules. The Zaurus also comes with Java (Insignia's Jeode). The device has a 206MHz Intel StrongARM processor, 64MB of RAM, and a 3.5-inch 240x320-pixel color LCD. There are both Compact Flash (CF) and SD slots (the SD slot will also take MMC). A small QWERTY keyboard is integrated into the device and becomes visible by sliding down the thumb pad and application button panel.

YOPY G.Mate[13] is Linux-based multimedia PDA that includes Bluetooth support, a 206MHz microprocessor, Compact Flash Slot for storage, memory, an Infrared port that allows the user to exchange information at 4Mbps and within a 1 meter range, and a docking cradle that includes RS232C & USB Serial Port for synchronization with a PC. The YOPY is targeted toward multimedia users and not the enterprise user.

The iPAQs come pre-installed with Microsoft's Windows for Pocket PC. Linux can replace the Microsoft OS in the unit's 16 megabytes of flash ROM. While Compaq won't sell a unit without Pocket PC, they are contributing considerable resources to making Linux work on the machines [Halsal]. One example of a Linux distribution for the iPAQ is the Familiar[14] distribution, a lightweight package with Python and XFree86 with anti-aliased fonts, using the Blackbox window manager. Familiar also includes a new packaging system called ipkg, which is like RPM or DEB packages for desktop Linux.

[12] For the latest on Linux devices see http://www.linuxdevices.com
[13] http://www.gmate.com/english/overview.htm
[14] See http://familiar.handhelds.org for more information.

Put together by Alexander Guy and Carl Worth, Familiar version 0.4 was just released as a stable version [Halsal].

Online embedded Linux portal report the introduction the following new Linux PDAs introduced this year Infomart Kaii, Invair Filewalker, Empower PowerPlay, HanGil C3224 multimedia PDA, and MasterIA PDA.

The Invair Filewalker[15], by Invair Technologies (Stuttgart, Germany), unveiled a new Linux-based PDA at CeBIT 2002 in Hannover, Germany. The device was designed to be operated with one hand, weighs a mere 0.2 lbs, and is small, at 3.4 x 2.2 x .74 in. It is based on an Intel StrongARM 133MHZ processor and includes 32MB SDRAM and 16MB Flash ROM, has a 160 x 240 pixel grayscale LCD display, and provides IrDA and USB interfaces plus an expansion slot for SD and MMC cards

The CIIT multimedia PDA[16] is based on an Intel 206 MHz StrongARM SA-1110 system-on-chip processor with 32MB of DRAM and 32MB of Flash storage memory. I/O connections include USB, serial, and Ethernet ports, and there is a CompactFlash slot for additional expansion (memory or I/O). The display is a 240 x 320 pixel, 4096-color LCD.

The SK Telecom IMT2000 WebPhone[17] is a combination cell phone plus PDA. It has a 4-in. LCD screen and a built in video camera. The PDA functions of the device are based on a StrongARM SA1110 206MHz CPU, and the device contains 32MB of RAM plus up to 32MB of internal flash memory. The operating system software is PalmPalm's Tynux embedded Linux[18], with Qt/Embedded for GUI support plus Opera's browser. A separate microprocessor controls the cell phone functions. The PalmPalm web site displays a Sharp Zaurus running the Tynux embedded Linux.

Pengachu[19] is a research effort at MIT to build a $50 handheld Linux computer, using 900MHz, 1mW, 200Kbps peering or hub-and-spoke internet gateways for wireless mode and a RS-485 wired LAN.

The table below provides an overview of the Palm OS, Pocket PC, and Linux operating systems. The table focuses their distinguishing characteristics (e.g., source code availability, development environment, Java support) and capabilities (e.g., software architecture and security mechanisms).

[15] See http://www.invair.de/
[16] See http://www.linuxdevices.com/products/PD7458959208.html
[17] See http://www.linuxdevices.com/articles/AT3334419107.html
[18] See http://www.palmpalm.com/
[19] See http://web.media.mit.edu/~rehmi/pengachu/frame.htm

	Palm OS	**Pocket PC**	**Linux PDA**
Open Source	License Source Code	No	Yes
Multitasking	Single Threaded	Yes	Yes
Application Support	Palm	Microsoft	Similar to Linux Desktop
OS Upgrades	Software	ROM/Hardware	CVE
Java Support	Limited KVM	Insignia Jeode Pda Edition Vm	Insignia Jeode Pda Edition Vm

Table 2: A comparison of PDA operating systems

3. Development Tools

3.1 Palm OS Development Tools

The Palm OS Emulator[20] is software that emulates the hardware of the various Palm models. It is used for writing, testing and debugging Palm applications on a PC. The Emulator allows users to model the behavior of "virtual" handheld devices by running the Emulator on Windows, Mac OS, or Unix workstations. Emulated devices can be loaded with new ROMs, an application can be tested with virtual devices, including different models, foreign language ROMs, and debug-enabled ROMs for extra error checking and debugging features. The Emulator is good for debugging applications, but does not offer any help in testing I/O ports which must be tested on the handheld device itself.

The X-Master is a system extension manager for the Palm Pilot. It utilizes an open standard for separately-downloadable "Hack" files, and provides the means of managing them. It helps developers with installing and uninstalling the patches, and even maintains a proper chain of Hacks that try to patch the same trap. It allows the developer to install and uninstall them in any order, instantly, without restarting. It also records the currently active set of extensions, and gives the option of automatically reinstalling them after a soft reset. The HackMaster is a freeware software distribution that provides the same functionality as the X-Master. HackMaster provides a "control panel" interface to enable and configure extensions to the PalmOS, called Hacks. This application is required in order to utilize most Hack files. Both the HackMaster and the X-Master allow developers to develop applications with more control over the PalmOS, but they should not be used as the basis for building any serious security tools for Palm PDAs.

The Code Warrior[21] Integrated Development Environment (IDE) is a set of tools for developing software using a graphical user interface (GUI). The tools that make up the IDE are the project manager, editor, compiler, linker, and debugger. Code Warrier includes a Conduit Wizard that generates conduit DLLs on Windows and provides supports for one-way or two-way synchronization. Additional Palm development tools such as the Palm SDK and Conduit Development Kit (CDK) can be downloaded from the PalmOS web site.[22]

3.2 Pocket PC Development Tools

The original Pocket PC, the new Pocket PC 2002, and the upcoming Smartphone 2002 are all mobile platforms based on Windows CE. The Pocket PC 2002 SDK[23] along with Microsoft eMbedded Visual Tools 3.0, make up the development environment for creating applications for the Pocket PC. eMbedded Visual Tools 3.0 is the set of tools embedded developers use to write software applications for new-generation, 32-bit devices based on the Microsoft Windows® CE operating system. Included are full

[20] http://www.palmos.com/dev/tools/emulator/
[21] http://www.metrowerks.com/products/palm/
[22] To download Palm development tools see http://www.palmos.com/dev/tools/
[23] http://www.microsoft.com/mobile/developer/downloads/ppcsdk2002.asp

versions of Microsoft eMbedded Visual C++® 3.0 development system, Microsoft eMbedded Visual Basic® 3.0 development system, SDKs, remote tools, and documentation The Pocket PC 2002 Software Development Kit (SDK) includes an emulator that uses a virtual machine to run the full Pocket PC 2002 operating system and software. Microsoft provides a tool set called Platform Builder for tailoring the Pocket PC operating system for a specific device.[24] For example, the Pocket PC 2002 platform consists of: well-defined hardware (defined by Microsoft and implemented by OEMs such as Compaq or Hewlett-Packard), Windows CE 3.0, and the Pocket PC extensions such as the Pocket PC shell, the Connection Manager, the Object Exchange and the Notification API.

3.3 Linux PDA Development Tools

Kernprof (Kernel Profiling) is a set of facilities for profiling the Linux kernel. It consists of a kernel patch that implements a number of profiling data collection mechanisms, as well as a device driver for controlling them, plus the user level command kernprof that allows a user to configure and control the kernel profiling facilities. At this time it also includes a small gcc patch that is necessary to build correct i386 kernels.

The KDB v1.2 (Built-in Kernel Debugger) is part of the Linux kernel and provides a means of examining kernel memory and data structures while the system is operational. Additional commands may be easily added to format and display essential system data structures given an identifier or address of the data structure. Current command set allows complete control of kernel operations including single-stepping a processor, stopping upon execution of a specific instruction, stopping upon access (or modification) of a specific virtual memory location, stopping upon access to a register in the input-output address space, stack tracebacks for the current active task as well as for all other tasks (by process id), instruction disassembly, et. al. [25]

Qt/Embedded from Trolltech[26] provides developers with the tools they need to create graphical user interfaces for embedded applications. Qt/Embedded is a C++ GUI toolkit and windowing system that brings the full power of Qt, and all of its advantages, to embedded Linux systems. It combines small size, rich functionality, and the ability to build code in familiar environments to allow programmers to develop solutions for embedded systems. Porting existing Qt-based applications to Qt/Embedded can be done a simple cross-compile.

Insignia's Jeode platform incorporates a "Sun Authorized Virtual Machine" that fully supports PersonalJava(TM) 1.2, including the Abstract Windowing Toolkit graphics class library. Jeode provides the Lineo software platform with complete Java functionality, including the ability to view Java applets, such as real-time stock tickers; play Java-based games; and run Java-based enterprise applications, such as sales force automation and order entry. It also enables device manufacturers to leverage other key benefits of Java

[24] For more development tool information see
http://www.microsoft.com/mobile/enterprise/papers/_Toc536024920
[25] http://oss.sgi.com/projects/kdb/
[26] http://developer.sharpsec.com

technology, including access to thousands of available third-party Java-based applications that can be incorporated to add value to SHDs and other types of information appliances. Moreover, Java's cross-platform support allows manufacturers to maintain their applications software investment even if the underlying hardware architecture changes in future product versions.

The SourceForge Linux Driver Foundry is a place for driver developers to get and give help, and for hardware vendors to release specs and otherwise support the Open Source community.[27]

[27] https://sourceforge.net/foundry/linuxdrivers/

4. Commercial Security Solutions

4.1 Palm OS Security Mechanisms

4.1.1 Physical Security

Kensington Technology markets PDA Saver, which uses a galvanized steel cable and lock to secure a handheld to the desktop. Several companies are applying new technologies such as motion detection and proximity alarms to handheld devices. [Palm Security White Paper]

4.1.2 Authentication

OnlyMe from Tranzoa automatically locks a Palm OS handheld whenever the device is turned off, and will ensure that no one can see information without entering the right password [Palm Security White Paper].

Sign On from Communication Intelligence Corp. offers a logon/password security utility for Palm OS handhelds that uses signature verification. To unlock the handheld, you simply sign any memorable word or name, and the software verifies the unique signature before unlocking the device [Palm Security White Paper]. Both Only Me and Sign On can survive a warm reset, so even sophisticated hackers will be restricted.

Unique device identification is an important component for authorizing network access via a handheld computer. Palm handheld devices can take advantage of several methods to identify a unique handheld, including flash ID, Mobile Access Number (MAN), device ID, and Electronic Serial Number (ESN). Any of these can be used to authenticate the handheld for network access and can allow Palm handheld devices to be used as a physical token for two-factor authentication. Another form of client-level authentication involves the use of software tokens such as RSA Security's SecureID for the Palm OS. In this case, the device itself essentially becomes the authenticator [Palm Security White Paper].

4.1.3 Encryption

For encrypting databases, there are products such as JawzDataGator from Jawz, Inc. and Movian Crypt by Certicom. Movian Crypt utilizes the 128-bit Advanced Encryption Standard (AES) to encrypt all data on the Palm handheld. With Movian Crypt, the applications are un-modified. The data is encrypted as it is stored and decrypted as the data is accessed [Palm Security White Paper].

For encryption of the entire Memo Pad, MemoSafe from DeepNet uses a SAFER-SK public-domain block cipher to encrypt Memo Pad records without changing its functionality. Encrypted memos are shown with a lock symbol [Palm Security White Paper].

For protecting collections of passwords, you can use a product such as Portable Projects' PalmSafe, which uses the Blowfish algorithm and also can encrypt other confidential information such as PIN numbers, logins, and URLs [Palm Security White Paper].

4.1.4 VPN

Certicom and V-One offer VPN access for the Palm OS via a clip-on CDPD modem, attached ricochet modem, attached cell phone, or a clip-on telephone modem to dial in to an ISP and create a VPN tunnel to the corporate router.[28] The MovianVPN interoperates with popular VPN gateways and supports the IPSec security standard, providing a cost-effective solution for simple integration with existing wireline VPN infrastructures. VPNs are available for the following Palm handheld devices: Palm® III, V, Vx, m100, m500 Series, Handspring™ Edge, Prism and Platinum , and the Sony Clié, PEG Series. SmartPass VPN client from V-One is also another commercially available VPN solution for Palm handheld devices.

4.1.5 Antivirus

Computer Associates offers InoculateIT for version 3.0 and above of the Palm OS. Symantec markets Palm Scanner, which scans handheld files looking for signatures of viruses, Trojan horses, and worms, and prompts the user before deletion; it also provides a live update feature during each HotSync operation. Network Associates (McAfee) offers VirusScan Wireless, which is deployed through an email link. It provides automatic updates based on user-set schedules and scans files during synchronization operations [Palm Security White Paper],

F-Secure developed the F-Secure Anti-Virus for Palm OS specifically to target the Phage code, which was discovered in September 2000. Phage can overwrite executable files but does not harm databases. The symptom of its presence is the screen going blank when running an application. Finally, Blue Nomad's BackupBuddy, a popular backup/restore program for Palm handheld devices, also has a built-in virus scanner [Palm Security White Paper].

4.1.6 Enterprise Tools

Another level of security on Palm Powered handhelds is provided by software such as Restrictor by ISComplete and Enforcer from Electric Pocket. These applications allow an administrator to create profile categories for different users, as well as a default profile, on a single handheld. These profiles limit the applications to which an individual user has access through another layer of password protection.[Palm Security White Paper]

Both applications can provide two-tiered device control access. Profiles can be created for the user and for the IT administrator, who can be given greater access to facilitate IT support. In addition, an IT manager can lock down applications for Palm handhelds such as network settings and preference panels. This keeps users from inadvertently

[28] http://www.certicom.com/products/movian/movianvpn.html

compromising important settings for remote access and more [Palm Security White Paper].

Restrictor's other capabilities include enabling an administrator to push a program to a user, and then locking down their handheld once the HotSync® operation is completed. Restrictor offers a lock delay to password-protect the device as well as private records. When the handheld is shut off, it is automatically locked. Finally, Restrictor allows an administrator to enforce data avoidance by configuring a device to disable IR and HotSync capabilities [Palm Security White Paper].

Computer Associates offers eTrust, a suite of software solutions that address encryption of traffic, user authentication, and access control. eTrust safeguards all mission-critical resources from the browser to the mainframe. eTrust solutions offer risk assessment, attack detection, loss prevention, and more [Palm Security White Paper].

Aether Systems markets a complete set of software tools and technologies, including ScoutIT and ScoutSync, that enable enterprises to rapidly build, deploy, and manage mobile and wireless solutions. ScoutIT's security features include real-time activity logging and database storage of all activity, local or remote monitoring, flexible device-state alert system for both users and administrators, and administrator-selected security levels (from three levels of encryption) [Palm Security White Paper].

The XTNDConnect Server, from Extended Systems, enables IT departments to integrate and manage mobile devices. This solution synchronizes Palm, Pocket PC, and Symbian EPOC mobile devices with corporate groupware servers, including Microsoft Exchange, Lotus Domino, IMAP4, SMTP, WCAP/iCAL, and any ODBC-compliant database. XTNDConnect manages data and applications on mobile devices with backup/restore, installation, configuration, and reporting capabilities, and ensures secure data transfer with ECC [Palm Security White Paper].

Critical Devices offers the Asset Services Management (ASM) suite, which lets companies remotely gather and monitor vital information on handheld devices. The ASM suite supports any wired or wireless connection, including infrared, Ethernet, and analog or wireless modems. ASM uses one-way communications that are sent via Certicom-encrypted data packets over the Internet. This ensures the information cannot be easily intercepted or read [Palm Security White Paper].

The Smart Handheld Device Manager, from Tivoli, seamlessly extends the Tivoli management environment, enabling an IT administrator to centrally discover handheld devices, install and remove applications, receive real-time inventory information, maintain high availability, and perform various configuration management functions. [Palm Security White Paper]

Xcellenet's Afaria is an enterprisewide solution for managing all mobile devices, including laptop computers, Palm Powered handhelds, smart phones, and interactive pagers. Afaria's technology enables enterprises to securely deploy and manage mobile,

device-based business solutions by tracking hardware and software assets, deploying and maintaining software, monitoring device and wireless network performance and availability, and securing backup copies of critical data. Afaria's rigorous security measures include user authentication, data encryption, configuration management, and data security [Palm Security White Paper].

On Command CCM, from On Technology, offers a unique information database that tracks all installation and configuration changes on a real-time basis. On Command makes it easy to rebuild devices to previous configurations in case of system hangs, virus corruption, or end-user misconfiguration [Palm Security White Paper].

Trustdigital[29] is the developer PDASecure-Enterprise™ which is designed for networked PDAs. It controls access to the PDA and any PC or network to which it is or can be attached. It also encrypts the data on the device on an application-selectable basis. When combined with Trust Digital's ForeverSecure security software for PCs, laptops and servers, it provides additional security to the PDA and a computer or network to which it is synced or attached. To help deploy, manage, and secure a large network of PDAs, TrustDigital offers the PDASecure-Policy Editor™ that works with each device's PDASecure-Enterprise™ software to allow a centralized management solution and a complete record of all the security-related activity on the devices.

Many Palm OS developers use the Certicom Security Builder (TrustPoint tool set) to create application-specific cryptographic solutions. TrustPoint conforms to Internet Engineering Task Force (IETF) guidelines. Certicom also offers the MobileTrust managed PKI service for companies preferring to outsource handheld digital-certificate management rather than building the capabilities in-house.

4.1.7 Miscellaneous

Trust Digital offers PDASecure and ForeverSecure. PDASecure enables secure password and data encryption, and in the event that a Palm device is stolen, PDASecure can restrict unauthorized synchronization. You can select from six different security algorithms, including Rjindael. ForeverSecure provides security for your desktop computer applications, including handheld data on a computer [Palm Security White Paper].

4.1.8 Other

CyberLocator is the authenticated location technology company for locating networks of computers, cell phones, and any other electronic device.[30] Using the Global Positioning System and its unique intellectual property portfolio, CyberLocator provides the only authenticated location solutions on the market today. Server side Voice Authentication can be provided for any voice-enabled PDA through speech recognition technologies offered by Nuance. [31]

[29] http://www.trustdigital.com/prod15c.htm
[30] http://www.cyberlocator.com/
[31] http://www.nuance.com/products/verifier.html

4.2 Pocket PC Security Mechanisms

4.2.1 Physical Security

Physical security solutions for the Pocket PC are the same as for the Palm.

4.2.2 Authentication

Pocket PCPINprint from Applied Biometrics uses a fingerprint reader attached to the handheld,[32] Pocket PC PINPrint can lock the whole device or can be customized to lock an individual application such as sensitive data or access to the company intranet. The reader is self-contained and self-powered, and can connect to the Pocket PC via the serial connection. It can store a local database of 16 fingerprints and can be customized to link to a remote database over a network or dial-up connection [Pocket PC Security White Paper].

Sign-On for Pocket PC is a software-based solution by A2000 and Audata that uses the touch screen of a PDA and a behavioral biometric, developed by Communication Intelligence Corporation (CIC), namely how the user signs their name. While it might be possible for a forger to copy the shape of a signature, Sign-On for Pocket PC also measures aspects that are far harder to copy, such as the rhythm and timing of the signature and how the user holds the pen. This information is used to lock access to information on the device from all except the authorized user[33] [Pocket PC Security White Paper].

The Visual Key software from SFR locks the PDA and displays a selected picture or graphic used for authentication.[34] The picture is divided into cells, which form the character set for a password. An alphanumerical key is generated from the input of selected cells and used to attempt a log in. Access is allowed only if a previously defined sequence of cells of the picture is clicked in the correct order. Visual Key provides a unique method of authentication that is difficult to steal through observation and is not easily lost or forgotten.

BioHub from Biocentric Solutions, Inc. uses a minutiae-based matching technique (vs. correlation-based).[35] Minutiae points occur at fingerprint ridge bifurcations and ridge endings. Their minutiae-based technology scans and records roughly 100 minutiae points then stores them on a template to be used in live comparisons. The device uses a CF card slot (type II). Software controls biometric enrollment, matching, and access to the PDA, which is also used to store the fingerprint template. Five security levels can be selected to determine the number of matching minutiae needed for the live fingerprint comparison.

---

[32] URL: http://www.appliedbiometrics.net/product2.htm and http://www.appliedbiometrics.net/contact.htm
[33] URL: http://www.shopcic.com/Shopping/catalog/viewcart.asp and http://www.a2000d.com/Sign-On.htm
[34] URL: http://www.viskey.com/viskeyce/ and http://www.viskey.com/technik.html
[35] http://www.biocentricsolutions.com/mobile.html

PDALok™ is biometric signature recognition software for the iPAQ that restricts access to unauthorized users unless a live signature from the rightful owner is presented. It locks a PDA from access or from synchronization, so all data held on the device is fully protected.[36] PDALok™ uses Penflow's Biometric Signature Recognition, which measures unique behavioral characteristics, to ensure only the rightful owner is granted access to their Pocket PC. A signature takes up less than 1K on the PDA and requires only a millisecond to be verified

The Reflex 20 device by Schlumberger is Win 95/98/NT and 2000 compliant and has PC/SC support.[37] The hardware module incorporates a smart card reader and uses a PCMCIA Card slot (type II). The reader accepts standard size smart cards, which must be obtained separately. Little support software provided for iPAC or other handheld devices.

4.2.3 Encryption

The Safe from Softwarebüro Müller is designed to store confidential information in an encrypted database. The Safe can be used to store telephone numbers, online passwords, credit card PINs, software licence numbers and the serial numbers of electronic equipment. It uses Triple-DES encryption and occupies around 100kB of memory on the Pocket PC [Pocket PC Security White Paper].

Sentry 2020/CE from SoftWinter[38] is a similar product that uses encryption to protect important information stored on a PDA. Without the correct password, a Sentry volume is just a file with encrypted contents. When the correct password is provided, the volume is mounted and appears as a normal folder on the device. Once enabled, the software automatically decrypts documents when accessed by Pocket Word, Pocket Excel and other applications.

4.2.4 VPN

Microsoft included support for connecting your Pocket PC to a VPN. The VPNs that Microsoft had in mind are running on a Windows NT, or Windows 2000 server. The VPN client does not provide support for other servers or routers that offer VPN connectivity. Movian VPN from Certicom[39] (www.certicom.com) supports some additional servers and routers. The VPN solution supports automatic connections to internal resources whenever the user is connected to the internet and they attempt to access an internal network resource. This is implemented by looking at the host name. If the host name has a period in it, then the request is sent to the internet otherwise it is sent over the VPN to the internal network. The down side to this implementation is that users will not be able to access the internet through the VPN or access any other server that has a period in the host name. The VPN implementation supports 128 bit encryption and NT

[36] URL: http://www.pdalok.com/ and http://www.pdalok.com/buy_pda_security_products/buy_pdalok.htm
[37] URL: http://www.1.slb.com/smartcards/infosec/ipaqdemo.html and http://www.scmegastore.com/cgi-bin/local-net/cs/shopzone30.cgi/st_main.html?p_catid=6
[38] http://www.softwinter.com/
[39] http://www.certicom.com

challenge for password authentication.[40] VPN support is available for the following models: Casio Cassiopeia EM500/EG80/EG800/E-125/E-115/E-100, Compaq Aero 1500/2100, Compaq iPAQ Pocket PC H3100, H3600 Series, HP Jornada 540/560/720, Intermec 700 Series, Symbol SPT 2700/2800, and PDT 8100.

4.2.5 Antivirus

McAfee's VirusScan for Pocket PC runs on a desktop or laptop PC, VirusScan for Pocket PC avoids the resource limitation of the handheld by using the power of the host PC to scan the Pocket PC over a Microsoft ActiveSync® connection. As with all antivirus software, it requires regular updates of its antivirus signature file. McAfee has also announced a wireless security center, which operates as an online service to protect, manage, and maintain a number of handheld platforms, including Pocket PC [Pocket PC Security White Paper].

Computer Associate's InnoculateIT for Pocket PC provides an anti-virus solution for Pocket PC devices connected to networked environments. Innoculute features include Real-Time Cure, Universal Manager, Virus Wall, Virus Quarantine, Hands-Free Updates, Extensive Alerting Options, Internet Web Browser Integration and Messaging Protection [Pocket PC Security White Paper].

[40] http://www.cewindows.net/reviews/pocketpc2002security.htm

4.3 Linux PDA Security Mechanisms

The Linux platform enjoys the benefits of the open source security work of the Linux community.[41] The Sharp Zauris Linux-based PDA is built on the Lineo Embedix Linux 2.4 kernel. Lineo's Embedix Plus PDA[42] is based on a networked kernel with built-in support for 802.11b, WiFi, Bluetooth and wireless modem technologies, as well as associated security and encryption modules. The Linux Embedded Appliance Firewall[43] project has a number of open source gateway, router, and firewall distributions that run on the embedded Linux kernel 2.4.

4.3.1 Physical Security

The physical security mechanisms for the Linux PDA are the same as those available for the Palm and Pocket PC PDAs.

4.3.2 Authentication

The following table summarizes several authentication solutions, with emphasis on the availability of software source suitable for integration into a Linux PDA. Smart card and token-based authentication seem most promising from this point of view. Linux SmartCard Project has a number of smart card drivers[44] for Linux.

Type	**Product**	**Connection**	**4.3.2.1 Available on platform/OS**				**SDK/Drivers/Apps**		
			WinCE	**Linux**	**Palm**	**2002**	**WinCE**	**Linux**	**Palm**
Signature	Sign-on	N/A	x		x				
	PDALok	N/A	x		x				
Visual key	VisKey	N/A	x						
Speech recognition	ASR1600 SDK	N/A					x	x	
Fingerprint readers	BioTouch	PCMCIA	beta						
	PINprint	Custom	x		x				
	BioHub	CF II	x			x	SDK		
Smart card readers	Reflex 20	PCMCIA	demo				demo		
	GemPC400	PCMCIA		x				x	
	GemPC410	RS232		x				x	
	GemPC430	USB						x	
Tokens	IButton	1-Wire					x	x	x

The GemPC 400, 410, 430 Card Readers smart card readers are developed by GemPlus SA[45]. The GemPC 400 (ex GPR400) can be connected to any device equipped with a PCMCIA port. It can incorporate an additional 128 KB of flash memory. The GemPC 410 can communicate to any device through the serial interface RS232. The GemPC 430

[41] http://www.linuxsecurity.com/docs/
[42] http://www.lineo.com/products/embedix_plus/shd/datasheet.html
[43] For more information on the LEAF project see http://leaf.sourceforge.net
[44] See http://www.linuxnet.com/sourcedrivers.html
[45] http://www.gemplus.com/products/

can be connected to any device through a USB port. All readers support ISO7816-compatible cards. Gemplus provides drivers/support for Windows 95/98/NT/2000/XP, but not for PDAs. However, there are open-source drivers and applications for the Linux OS available on the Internet, which could be adapted for Linux PDAs[46,47,48].

Another device that can be used for token authentication is the iButton®, developed by Dallas Semiconductor Corp.[49] The iButton is a 16mm computer chip encapsulated in a stainless steel can. The simplest models, the memory buttons, can contain 64K or more memory; other models also contain a microprocessor. Each iButton is identified through a unique device identifier that can be used in a simple authentication application. A PC or PDA can communicate with a button through the 1-Wire™ protocol. The information can be transferred with a momentary contact, at up to 142K bits per second. The physical connection requires a "Blue Dot" receptor, a serial port adapter, and, in the case of a PDA, a serial I/O CF card. The company provides 1-Wire drivers[50] for Windows PCs and a Software Development Kit. To help developing iButton applications for other platforms, such as Linux, Palm OS, and Windows CE, the company provides a "1-Wire Public Domain Kit"[51]. An authentication application using a Java iButton as a cryptographic token is also available[52].

4.3.3 Cryptographic Algorithms

The Linux 2.4 kernel supports several cryptographic algorithms such as Blowfish[53], IDEA, Serpent, AES, 3DES, DES and others. The MD5 and SHA1 digest algorithms are also supported. The cryptographic modules for the 2.4 kernel can be found online.

The OpenSSL package supports an even greater variety of algorithms including RSA and DSA, and provides tools for working with X.509 certificates.

4.3.4 Firewall

Since most of the Linux PDAs support the full version of Linux kernel, all firewall features available in desktop version of Linux are available on the PDA as well. The firwall options range from simple packet based firewalls (ipchains) to full-blown statefull firewalls (iptables). However it must be noted that memory constraints of the PDA might limit the usefulness of statefull firewalls.

The LEAF project firewall supports Policy firewall, IP Masquerade (NAT), port redirection, port translation, port load balancing, transparent proxy, numberless interface spanning, interface load balancing, and interface aliasing. LEAF supports Ethernet,

---

[46] http://www.linuxnet.com/smartcard/sourcedrivers.html
[47] http://mobilix.org/smart_linux.html, http://ludovic.rousseau.free.fr/softwares/ifd-GemPC/ifd-GemPC.html
[48] http://www.debian.org/
[49] https://store.ibutton.com/cgi-bin/ncommerce3/CategoryDisplay?cgrfnbr=810&cgmenbr=776&cg=810
[50] http://www.ibutton.com/software/tmex/index.html
[51] http://www.ibutton.com/software/1wire/wirekit.html
[52] http://www-users.rwth-aachen.de/dierk.bolten/pam_ibutton.html

[53] See http://www.counterpane.com/blowfish.html for source code and documentation.

WAN (DS1+), Wireless, ISDN, Serial, Parallel port interfaces. The LEAF documentation also states that it supports the following advanced networking capabilities: IPX, Token Ring, Tunneling, Crypto VPN, traffic limiting and shaping, and policy based routing.

4.3.5 VPN

VPN support for the embedded Linux kernel 2.4 is also provided by the aforementioned LEAF project and allows for IPSec, GRE and IPIP tunnels with end-points. Leaf incorporates Shorewall[54], a Netfilter (iptables) based firewall for this purpose. The Shorewall firewall is available as freeware under the terms of Version 2 of the GNU General Public License.

Secure Shell Protocol implemented by OpenSSH[55] supports forwarding of selected TCP ports in a secure fashion.

FreeS/WAN implements IPSEC and IKE protocols and can be used as a client to the popular Firewall.1 firewall by Checkpoint.[56]

Calibri[57] is an open source embedded Linux appliance that claims to offer a low cost solution for firewall, VPN and routing demands. The Calibri-133 model is also fully compatible with all Linux Open-Source software.

4.3.6 Antivirus and Integrity Checkers

Linux viruses are much less common than virus written for other operating systems such as Windows or Macintosh, but there have been numerous reports of Linux viruses in that last few years. Most Linux antivirus software runs on Linux servers, but scans for viruses that infect Windows or Macintosh desktops. Panda Antivirus[58] for Linux is an antivirus for Linux servers and desktops. The aim of Panda Antivirus for Linux is to scan and disinfect Windows and DOS workstations connected to a Linux server, as well as the Linux server itself. McAfee VirusScan supports a broad range of platforms including Windows XP, 2000, NT4.0, and 9x; Linux; HP-UX; SCO; AIX; and Solaris.[59] Some viruses, such as the Linux.Winux virus, have been reported to infect both Windows and Linux machines. Linux.Winux is a non-memory resident virus. It can replicate under Windows 95/98/Me/NT/2000 (Win32) and Linux operating systems and it infects EXE (Windows executable) and Linux executable ELF files.[60]

TripWire can be used for checking integrity of the important system files. The integrity is checked by computing the checksums of the system files, and then comparing these

[54] For information on the Shorewall firewall see http://www.shorewall.net/
[55] See http://www.openssh.org
[56] See http://www.freeswan.org
[57] See http://www.calibri.net/
[58] See http://www.pandasoftware.com/com/linux/linux.asp
[59] http://www.mcafeeb2b.com/products/desktop-protection.asp
[60] See http://www.wired.com/news/technology/0,1282,42672,00.html

checksums against its internal database. So if a virus a malicious hacker changes replaces any of the system files, such change will be picked up by the TripWire.

4.3.7 Miscellaneous

Viper[61] is a Personal Information Manager (PIM) suite for PDAs (Personal Digital Assistants) developed by TUXIA to address the growing need for a stable, robust, flexible, highly secure and high performance platform. Viper can be configured to run on and iPAQ and a Palm. Viper enables to be synchronized with the desktop using applications such as Jpilot[62]. Jpilot runs on a Palm Pilot running the Linux 2.4 kernel.

[61] See http://www.tuxia.org/viper/index.html
[62] See http://www.jpilot.org.

5. Summary

A comparison of processor speed, memory, flash and screen quality, makes little difference in overall cost to the consumer whether the device is powered by Palm OS, Pocket PC or Linux. The availability of applications is the key concern among most organizations (managing personal information, automating a sales force, managing customer relationships and so on) for selecting a PDA.

The Pocket PC 2002 Phone Edition has just been released. The Pocket PC Phone Edition supports data and voice communications.[63] This latest version of the Pocket PC allows the mobile workforce access the following services: email, web browsing, Instant Messaging, voice communication, and SMS text messaging. There are also many Palm- and Linux-based PDA-Phones devices on the market and these devices can become a necessity for the mobile workforce.

	Advantages	**Disadvantages**
Linux	• Open Source • Open Standard Support • Secure OS design • Wide Availability of free applications and utilities • Active embedded Linux community • Manufacturers pay no OS licensing fees.	• Limited driver support • Fewer applications • Does not support Microsoft applications
Pocket PC	• Support for most Microsoft applications and development tools • Familiar development environment for third party developers • Growing user base • Strong Microsoft and Compaq backing	• Proprietary OS • Expensive entry-level models
Palm	• Ease-of-Use • Largest User Base • Thousands of freeware and shareware programs available • Inexpensive entry-level models • Add-on modules	• Insecure OS • Limited support for Microsoft Applications (Outlook)

Table 3: A Summary of the Advantages and Disadvantages between PDA Families

[63] See http://www.microsoft.com/mobile/phones/default.asp

6. References

[Halsal] The Agenda VR3: Real Linux in a PDA, by Chris Halsall, 05/18/2001
Linux on an iPAQ, by Chris Halsall, 06/01/2001

[Palm Security White Paper] < URL:
http://www.palm.com/enterprise/resources/securing/index>

[Pocket PC Security White Paper] <URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/mobile/maintain/MBLSECUR.asp >