Securing the handheld environment– An Enterprise Perspective

Effective security is a critical component of any viable enterprise handheld implementation. An increase in enterprise workforce mobility is driving an aggressive transition to increased usage of handheld computing solutions. Successful IT organizations will build handheld computing security into their overall corporate IT strategy.

This paper provides an overview of the issues surrounding handheld computing security, discusses current capabilities, provides a recommended strategy, and offers a view into the future of handheld security capabilities.

Security in an Insecure World

Security is not a new issue for IT organizations. Most enterprises have long-standing security policies designed to protect access to the organization's network and desktop computing resources. This protection is critical to ensuring not only the integrity of the organization's data, but also its confidentiality.

Laptop and notebook computing represented an important wave in the evolution of mobile computing. And yet, there are a number of circumstances where it's not reasonable to sit down and power up a notebook, for example, during a lunch meeting, at a patient's bedside, or on a shipping and receiving dock. That's where handheld computing solutions come in. Adequately addressing the unique requirements of handheld computing security requires a multidimensional approach.

Controlled User Access

As more and more mission-critical information is stored on handhelds, the need to secure that information has become a top-priority IT challenge. Data security begins with basic password protection for locking access to a handheld computer and hiding records. These capabilities are inherent in the operating system of Palm OS handhelds.

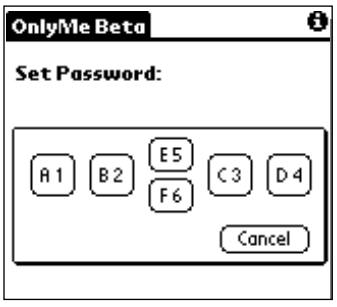
Palm OS version 4.0 supports enhancements to the built-in security application, such as ways to enable automatic device locking ("Never," "On power off," "At a preset time," "After a preset delay").

Palm OS 4.0 also offers new encryption, integration with the Palm Desktop software, and password hinting for unlocking sensitive data. For example, when users set up passwords, they can enter a short hint that only the user would know to help in case of forgotten passwords. These administrative capabilities of the Palm OS reduce IT organization's support burden and increase the overall productivity of the enterprise.

A number of vendors are capitalizing on the momentum in the handheld market by providing enhanced password protection that offers a wide range of capabilities. For example, one option requires pressing a specific combination of buttons, another requires the use of a stylus to write a unique character on the handheld screen, and yet another requires tapping a unique ID on an ATM-style keypad on the handheld screen before access is given. Some excellent solutions from Palm OS developers for protecting data from unauthorized access are provided below.

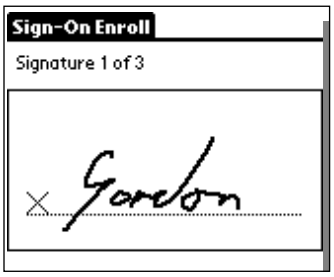
Password Protection

OnlyMe from Tranzoa (www.tranzoa.com) automatically locks a Palm OS handheld whenever the device is turned off and will ensure that no one can read the information on the device without entering the right password.



Only Me allows one-handed operation by mimicking the buttons on the front of your handheld.

Sign On from Communication Intelligence Corporation (www.cic.com) offers a log-on/password security utility for Palm OS handhelds that uses signature verification to limit data access. To unlock the handheld a user simply signs any memorable word or name and the software verifies the unique signature before unlocking the device.



Both *Only Me* and *Sign On* can survive a warm reset as well, so even sophisticated hackers will be restricted.

Trust Digital (www.trustdigital.com) offers *PDASecure* and *ForeverSecure* that provide Palm security software for handheld devices. *PDASecure* enables secure password and data encryption for Palm handhelds. In the event that a Palm handheld is stolen, *PDASecure* will restrict unauthorized synchronization. PDASecure allows selection from six different security algorithms, including the Rjindael algorithm to be described in the section "Developing Secure Applications." *ForeverSecure* provides security to your desktop PC applications, including Palm data on the PC.

On-Device Encryption

Limiting access to the device using password protection is an excellent starting point, but may not go far enough for certain security-sensitive applications. Often it is necessary to provide a redundant level of protection by encrypting particular databases or applications. For the Palm OS, on-device data protection and encryption generally takes one of four forms:

- Encryption of private records
- Encryption of the entire Memo Pad
- Organization and encryption of the user's passwords or other confidential bits of information
- Encryption of databases.

Some very sophisticated algorithms for data protection on the device have been developed, using well-known standards throughout the cryptographic community such as Blowfish, IDEA, SAFER-SK, and 3DES.

The Palm OS supports private records, which involves a special flag which can be set for individual entries in the Address Book, Calendar, Memo Pad, and Tasks/ToDo. The user can then assign a password and enable record hiding within the Security application, which ships with every Palm OS device. This prevents an unauthorized user from seeing records marked as private on the device.

For encryption of the entire Memo Pad, the *MemoSafe* product from DeepNet (www.deepnettech.com), uses a SAFER-SK public domain block-cipher to encrypt Memo Pad records while not changing its functionality. Encrypted memos are shown with a lock symbol (see below).

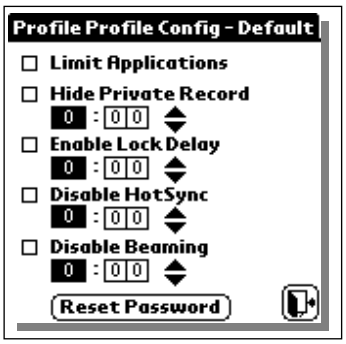
For protecting collections of passwords, you can use a product such as Portable Projects' *PalmSafe* (www.portableprojects.com), which uses the Blowfish algorithm and can also encrypt other confidential information like PIN numbers, logins, and URLs.

For encrypting databases on the device, there are products like *JawzDataGator* from Jawz Inc. (www.jawzinc.com) and Movian Crypt by Certicom (www.certicom.com). MovianCrypt utilizes the 128-bit Advanced Encryption Standard (AES) to encrypt all data on the Palm handheld. With MovianCrypt, the applications are un-modified. The data is encrypted as it is stored and decrypted as the data is accessed.

Using Profiles to Limit Access to Specific Data

Another level of security can be provided by offerings such as *Restrictor* by ISComplete (www.iscomplete.com) and *Enforcer* from Electric Pocket (www.electricpocket.com) —both for the Palm OS. These software 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. *Restrictor* offers important capabilities such as enabling an administrator to push a program to a user, and after the user completes a HotSync their device is locked down. Next, *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 Hot Sync capabilities.

Traditional name and password for Enforcer's authentication



Restrictor Device Configuration

These applications can be used to provide two-tier 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 Palm applications such as network settings and Palm preference panels. This keeps users from inadvertently compromising important settings for remote access and more.

Minimizing Loss & Theft

Companies such as Kensington Technology Group (www.kensington.com) offer *PDA Saver*™, which uses a galvanized steel cable and a lock to secure a handheld to the desktop environment. Several innovative companies are applying new technologies such as motion detection and proximity alarms to the handheld world. The personal nature of handhelds has led to some stylish interpretations of restraint devices such as the Palm V neck strap from Force Technology (www.force.com) that offers a bond product and neck chain to attach handhelds to a users body. Another concept is a holster/vest (www.eholster.com) which can fit under a coat, and is designed to hold a PDA and other electronics such as a cell phone or modem.

Expect to see the evolution of physical security products to mirror those that have been established for notebook computing.

Securing Handheld Communications

A Computerworld.com article discussed the essential questions that any computing security system must answer: Who are you? Do you belong here? What rights do you have? How do I know you are who you say you are?[1]

The successful operation of an enterprise relies heavily on concealing confidential information and ensuring the integrity of data. Prohibiting unauthorized handheld access—in either wireline or wireless mode—to corporate databases, and information contained in intranets or extranets, is vital to an effective security strategy. Palm and its partners in the Palm economy offer solutions that address security issues involving Remote Access Service (RAS), Virtual Private Network (VPN) access, IEE 802.11b, client-level authentication, and Palm VII wireless solutions.

"The best security policies must begin with company-provided mobile devices, which are easier for IS departments to manage. If a company allows users to purchase their own PDAs, however, IT should at least establish a short list of supported models and standardize the way they interface with the network."

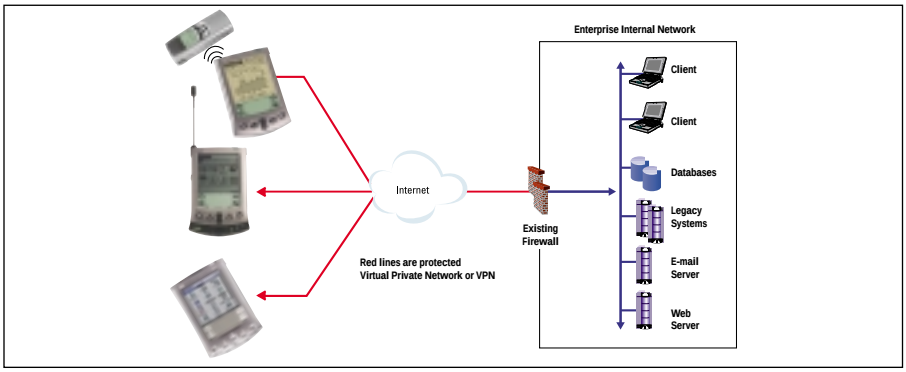
—Sarah Scalet, "Remote Control" CIO Magazine, November 15, 2000

Remote Access Service

Palm OS based handhelds offer password authentication and challenge-response security protocols including Microsoft Challenge Handshake Authentication Protocol (CHAP), all out of the box. CHAP is a type of authentication in which the authentication agent (typically the network server) sends the client program a key to be used to encrypt the username and password. This enables the username and password to be transmitted in an encrypted form to protect them against eavesdroppers.

VPN Access

Many corporations are migrating from RAS to VPN to provide better security. VPNs are used to provide secure access to intranet and extranet resources and data. It is common practice today for mobile laptops and home office desktops to gain remote access to corporate data using VPNs.



1 Kay, Russell. "Authentication." Computerworld.com, March 27, 2000

Certicom (www.certicom.com) and V-One (www.v-one.com) offer VPN access for the Palm OS via clip-on CDPD modem, attached ricochet modem, an attached cell phone, or a clip-on telephone modem to dial in to an ISP and create a VPN tunnel to the corporate router.

IEE 802.11b

This newly embraced industry standard has continued to gain in popularity. Coupled with corporate VPNs, 802.11b's ability to deliver secure high-speed network data transmission ensures it's continued growth. Xircom, (www.xircom.com) has recently released the wireless LAN Module for Palm's m500 series. This easy to attach sled provides users secure wireless data transmissions, peer-to-peer links, and high speed access to the internet, email, and network resources.

Client-Level Authentication

Unique device identification is an important component for authorizing network access via a handheld computer. Handhelds based on the Palm OS 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 unique device IDs can be used to authenticate the handheld for network access and can allow Palm handhelds to be used as a physical token for two-factor authentication. Cedars-Sinai Health System uses two–factor authentication using the MAN and ESN.

Another form of client-level authentication involves the use of software tokens such as RSA Security's (www.rsasecurity.com) *SecureID* solution for the Palm OS. In this case the device itself essentially becomes the authenticator.

Palm VII Wireless Security

The Palm VII was designed with strong security features from the beginning. Each Palm VII has a customized Elliptical Curve Cryptography (ECC) library, developed by Certicom, which fits in only 29K of memory. Using this library, the Palm VII executes a 163-bit elliptic curve Diffie-Hellman key exchange. This key is roughly the equivalent of an RSA 1024 bit key. This solution uses the public half of a Palm.net private key pair, the private key being held at the Palm.net server facility.

An encrypted session key allows the Palm VII to fall back to a 184-bit DESX encryption. The Palm VII derives added security via a stored server key that is updated occasionally by a special administrative key that is also stored on the handheld. To increase efficiency, a special one-pass protocol was designed to cut down the number of handshake exchanges needed to establish identity over the low-bandwidth connections.

Server-Side Security

Enterprises are rapidly embracing server synchronization to extend information on corporate servers to a community of handheld users. Server synchronization also addresses a number of security-related issues, such as:

- Leaving desktop workstations on and unprotected when out of the office.
- Centralized backup and restore of mission-critical data restricting access to particular types of data based on being job function.
- Establishing an electronic "paper trail" (audit feature) detailing which data was retrieved and by whom.

A server-based synchronization server, such as Palm's HotSync Server, or Extended Systems' XTENDConnect Server, can address all of these security issues and at

the same time the management of the handhelds in the enterprise. Server synchronization solutions allow IT organizations to restrict access to corporate data by requiring that each user have a unique ID and password before synchronization can initiate (this is stored in the user's profile on the server).

The server can be accessed using a proxy agent via the standard desktop cradle, but also can be accessed in many other ways not requiring a workstation to be on, such as with a snap-on modem (e.g., the Palm modem), wireless sled (e.g., the Novatel Minstrel modem), cell phone connection (cabled or infrared modem), infrared to Ethernet adapter (e.g., EthIR LAN by Clarinet Systems), or the Palm Ethernet cradle, which is ideal for providing server-based data access from a conference room, hallway or other remote location where Ethernet is present.

With Palm HotSync Server software, a user is able to check email, calendars, or enterprise data residing in back-end databases while traveling, with their desktop workstation off. When the user is authenticated and successfully synchronizes to the server, their activities are audited in the server's relational database, and the server can push software updates and backup or restore the contents of their device. The data they receive can be keyed to their membership in one or more groups defined at the server level. An administrator can generate reports off any information stored regarding users and their activities on the server, using a standard report writer capable of interfacing with a relational database.

Developing Secure Applications

A large number of Palm OS developers use the Certicom (www.certicom.com) 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.

Other Palm OS developers have alternatively built their own cryptographic solutions. One example is Centura (www.centura.com), which specializes in secured, real-time database applications, and provides end-to-end data security over the Palm.net wireless network. Enterprise handheld applications can build in an additional layer of security by accepting only incoming connections from known IP addresses.

Another example is NTRU (www.ntru.com), whose Security Toolkit for PalmOS uses the Rjindael encryption algorithm, which was recently approved by the National Institute of Standards and Technology (NIST) as the next Advanced Encryption Standard (AES). A recent Federal Information Processing Standard (FIPS) regulation is expected to be written by summer 2001, to incorporate the AES including NTRU's Rjindael toolkit. This is particularly significant for Federal customers requiring FIPS compliance in the encryption-related products they purchase.

FIPS compliance is already present in other products used on the Palm platform, including Certicom's ECC used on the Palm VII and the V-One SmartPass VPN client for the Palm (www.v-one.com).

Security & Enterprise Management

Many of Palm's key enterprise software partners extend their security solutions to the Palm OS and offer management solutions to easily inventory Palm OS handhelds to enforce security policy. These tools are in addition to Palm HotSync Server software discussed previously in this paper.

Computer Associates (www.ca.com) offers *eTrust*, a suite of solutions that address encryption of traffic, user authentication, and access control. *eTrust* enables eBusiness by safeguarding all mission-critical resources, from the brows-

er to the mainframe. *eTrust* solutions offer risk assessment, attack detection, loss prevention, and more.

Aether Systems (www.aethersystems.com) offers a complete set of software tools and technologies enabling enterprises to rapidly build, deploy and manage mobile and wireless solutions. Two important software solutions include *ScoutIT* and *ScoutSync*. *ScoutIT* provides tools IT professionals need to extend their information infrastructures to the new mobile computing generation. Key features of *ScoutIT* related to security include real-time activity logging and database storage of all utilization activity, local or remote monitoring, flexible device-state alert system for both users and administrators, administrator choice of level of security from three levels of encryption.

Extended Systems (www.extendedsystems.com) *XTNDConnect Server* enables IT departments to integrate and manage mobile devices. This solution synchronizes Palm, Windows CE, 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, DES-X, and 128-bit ARC4 encryption.

Critical Devices (www.criticaldevices.com) *Asset Services Management* (*ASM*) suite allows enterprises to gather and monitor vital information on all handheld devices without having to physically touch each one. The *ASM* suite supports any wired or wireless connection, such as infrared, Ethernet, and analog or wireless modems. *ASM* employs one-way communications that are sent via Certicom-encrypted data packets over the Internet. This ensures the information sent over the Internet cannot be easily intercepted or read. *ASM* makes it affordable to identify, track, monitor and manage IT assets—including handhelds.

Tivoli (www.tivoli.com) *Smart Handheld Device Manager* extends the Tivoli management environment, enabling administrators to centrally discover existing handheld devices, install and remove applications, receive real-time inventory information, maintain high availability, and perform various configuration management functions.

Xcellenet's (www.xcellenet.com) *Afaria* offers an enterprise-wide solution for managing all mobile devices including laptop computers, Palm OS 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, securing backup of copies of critical data. Afaria employs rigorous security measures that include user authentication, data encryption, configuration management, and data security.

On Technology's *On Command CCM* (www.on.com) 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.

The Anti-Virus Issue

The handheld industry experienced its first virus in 2000. Patches were posted within hours by a variety of vendors that create anti-viral software. Virus attacks are nothing new. Any electronic platform can be susceptible to hackers who create viruses, and IT organizations need to be prepared. But just as the usage model for a PC is very different from that of handheld, so is the operating system and the potential impact of viruses, worms, and Trojan horses.

The Palm OS has to date been relatively safe from attack, despite considerable coverage in the media. Safeguards built into the Palm OS protect user data on many levels, making Palm handhelds by nature very secure from these kinds of attacks. In contrast, handhelds based on Windows CE are exposed or vulnerable to the thousands of viruses that currently permeate the Windows world.

In addition, infrared beaming is by nature secure since it requires close physical proximity (4 feet or less) to the beaming device, and the recipient is prompted and must tap on the screen to accept all incoming beams (there are no unsolicited beams). Palm OS devices also have built-in "sleep" thresholds (typically 1-3 minutes), and when sleeping the device cannot accept an incoming infrared beam. The user also has the option to disable beam receive altogether through the system preferences on the device.

In addition, Palm handheld computers are not susceptible to viruses developed for the Windows platform (email attachment-based or otherwise), and also cannot be used to stage viruses passed to the device then back to the desktop. Third-party products developed for Palm OS, such as DocumentsToGo from DataViz, Inc.(www.dataviz.com) and QuickOffice from Cutting Edge Software (www.cesinc.com), remove macros from Microsoft Word and Excel files upon transmission to the device.

Even though to date there have been no true replicating viruses, Palm takes this threat very seriously and is working with the best in class anti-virus software vendors such as Symantec, McAfee, and Computer Associates to ensure protection against potential hacker threats.

Computer Associates has made available *InoculateIT* (www.ca.com) for the Palm OS platform. *InoculateIT* offers virus detection for PalmOS v3.0 or greater devices. *InoculateIT* for Palm OS Platform is specifically designed to provide immediate and complete protection against all current known malicious attacks targeted at the Palm OS platform.

Symantec (www.symantec.com) has a product called *Palm Scanner*, which scans Palm files looking for signatures of viruses, Trojan horses, and worms, and prompts the user before deletion. They provide a live update feature during each HotSync. For more information see www.symantec.com/avcenter/palmscanner.html.

Network Associates/McAfee (www.networkassociates.com) offers *VirusScan Wireless*, which is deployed to users through an email link, provides automatic updates based on a schedule individual users set, and scans files during synchronization operations.

F-Secure (www.f-secure.com) developed the *F-Secure Antivirus* for Palm (www.f-secure.com/palm) , specifically to target the "Phage" code, which was discovered in September of 2000. Phage is capable of overwriting executables but does not harm databases. The symptom of its presence is the screen going blank when running an application.

Finally, **Blue Nomad**'s *BackupBuddy* (www.bluenomad.com), a popular backup/restore program for Palm handheld computers, also has a built-in virus scanner for Palm files.

Palm recommends that, as with any operating system, users of Palm OS should follow certain procedures in order to maximize the safety of your data. These include:

- Perform a full backup of the contents of your device on a regular schedule, and especially before adding new applications. HotSync the most critical data (e.g., schedules, addresses) even more frequently.

- Obtain software from reputable software providers, such as those listed in this paper.
- If you have access to the Palm OS Emulator, you can load applications into it and run them from a Windows, Mac, or UNIX environment, before loading to your device. The Palm OS Emulator can be downloaded from www.palmos.com/dev/tech/tools/emulator.

The Future of Handheld Security

A number of new security solutions for handheld computers are well on their way including smart cards, biometrics capabilities, motion detection solutions, and secure digital and multimedia cards.

Smart cards are another level of security that can be added by requiring users to physically have something, such as a smart card—a credit-card-size device that can contain identifying information and a decryption key. Smart cards can be used to authorize activation of a handheld computer. It is expected that this identification method will soon become a component of handheld authentication. Early products have already been released, such as the SmartClip sled for the Palm III and V series, from Sunderland Technologies (www.sunland-group.com).

Biometrics and motion detection are emerging technologies that are just beginning to gain popularity in the notebook world. The term biometrics refers to capabilities that identify users by their fingerprints, irises, or even handwriting. Motion detection security systems require users to program a series of movements such as lifting one side of the device a certain number of degrees and then back again to enable access to the device. Expect to see these capabilities expand to the handheld world.

Palm's Expansion Standard

Secure Digital (SD) and multimedia (MMC) cards are part of Palm's expansion strategy, allowing Palm handheld users to carry secure credentials in a very small removable card the size of a postage stamp. These cards currently store up to 64 MB of data as RAM, with capacities in the hundreds of MB expected within a year, and also allow for the development of I/O applications such as cameras, GPS, etc. These secure credentials can be removed from the device, which makes it impossible for any unauthorized person to engage in a transaction or to unlock the data in the device.

Palm believes SD is by far the most appealing standard for expansion on a handheld platform, given its widespread industry adoption, relatively low cost, fast I/O speeds (up to 12 megabits/sec.), superior small form factor, and advanced

security including check in and check out. Each SD card features a physical write protect tab, much like with floppy disks, to prevent accidental overwriting. In addition, MMC allows for the storage of applications and data in ROM. This is the same technology used to secure copyrighted digital music.

For more information on Secure Digital, please read our white paper: Palm's New Dual Expansion Architecture (http://www.palm.com/products/accessories/expansioncards/

Although Palm has chosen SD as the standard for its next-generation devices, the Palm OS 4.0 and beyond will support not only SD, but the expansion standards chosen by Palm licensees including Handspring, Sony, and TRG Products. This gives our Palm OS developers the widest array of output choices, as well as potential market, for their applications.

Handheld Security Checklist

A valid security policy for handheld solutions will:

- Control user access to data resident on the device through the use of password protection and user profiles to restrict access to specific data and administrative resources.
- Minimize the risk of loss or theft through a variety of physical security products.
- Secure handheld communications in wireless and wireline modes
- Offer authentication and encryption capabilities via RAS and VPN access methods.
- Ensure client-level authentication by uniquely identifying handheld computers.
- Offer server-side security solutions that provide greater control and monitoring of handheld security aspects.
- Provide an opportunity to develop unique security solutions.
- Leverage enterprise application system management solutions to enforce security policy and enhance handheld security.
- Take advantage of anti-virus measures to protect handheld data.

Palm and its partners provide solutions that address all the critical security issues for handheld computing.

Palm Software Download Sites

www.palmgear.com

www.tucows.com

www.zdnet.com/downloads/powertools/

www.download.com

Real-World Solution

Handheld devices have made their mark in companies and industries around the world. The issue of security is ubiquitous.

Not only do these companies and industries require a strategy to protect their own corporate data, but many are strictly governed by regulatory agencies that mandate additional levels of security.

One organization where security has played a fundamental role in the successful deployment of handhelds is Cedars-Sinai Medical Center (CSMC) in Los Angeles.

At CSMC, security and confidentiality has always been a high priority. CSMC implemented a wireless interface to clinical information for physicians based on the Palm VII, a wireless digital network, encrypted data transmission, secure web servers, and a clinical data repository.

The CSMC application supported the organization's security needs in a variety of ways:

- Random and patient-specific confidentiality warnings to users
- Detailed logging of all user accesses or attempted accesses to patient data
- Automatic daily audit reports for accesses to sensitive patient accounts or test results and employee medical records
- Interactive applications to support ad-hoc audits on either a per-user or per-patient bases

Some security issues that are specific to the Palm VII implementation are as follows:

- Firewall traffic control and alerts—the firewall performs protocol-level filtering, exposing secure web servers and other selected machines to non-campus users for approved types of connections, while blocking and logging all other connection attempts from the Internet
- Data encryption—Wireless data transmission and land-based traffic over BellSouth's Mobitex network are encrypted with Certicom's proprietary Elliptical Curve Cryptography technology.
- Client-level authentication—The Palm VII's unique device ID, which is transmitted in each data packet to the secure web server, allows the Palm VII to be used as a physical token for "two-factor authentication." The server side of the Palm application tracks the physical ID of all Palm VII devices used by physicians and, if a Palm VII is lost, can be configured to lock out attempted access by that specific device. To prevent subversion of the Palm application by someone using an ordinary web browser, the web server's virtual directory for the Palm application is configured to only accept incoming connections from the known IP addresses of the Palm and Omnisky proxy servers.
- Application-Level Authentication—The Palm user must supply a valid login and password. The system enforces a password change at least every 90 days. Each Palm access to clinical data is logged with the user's name, patient name, medical record number, the date and time, and specifics of the data viewed.

Glossary

Authentication The process through which the identity of a computer or network user is verified; it's the system that ensures that an individual is, in fact, who (s)he claims to be. It's distinct from identification—determining whether an individual is known to the system—and from authorization—granting the user access to specific system resources based on his/her identity.

Biometrics Biometrics literally means "life measurement." In the realm of security, it refers to automated methods for identifying people based on their unique physical characteristics or behavioral traits. Types of biometric methods include fingerprint scanning, iris scanning, retina scanning, handwriting analysis, handprint recognition and voice recognition.

Certificate Authority A trusted third-party organization or company that issues digital certificates used to create digital signatures and public key pairs The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

Challenge-Response A common authentication technique whereby an individual is prompted (the challenge) to provide some private information (the response). Most security systems that rely on smart cards are based on challenge-response. A user is given a code (the challenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.

CHAP Challenge Handshake Authentication Protocol is a type of authentication in which the authentication agent (typically the network server) sends the client program a key to be used to encrypt the username and password. This enables the username and password to be transmitted in an encrypted form to protect them against eavesdroppers.

Diffie-Hellman Whitfield Diffie and Martin Hellman invented public key cryptography in 1976. For this reason, public key cryptography is sometimes called Diffie-Hellman encryption. This kind of encryption uses two keys—a public and a private key—to encrypt data transmissions.

Digital Certificates Digital certificates are data files used to establish the identity of people and electronic assets on the Internet. They allow for secure, encrypted online communication and are often used to protect online transactions.

Elliptical Curve Cryptography (ECC) Certicom's proprietary encryption technology.

Encryption Encryption is a method to make E-mail messages, data files and electronic-commerce transactions secure. Encoded blocks of data, called keys, are used to lock the message from outside view when it's traveling across the Internet. When it gets to the recipient, that recipient also must use a special key that can unlock the message. Previously, the U.S government used a 56-bit block of data for its encryption standard, but because computers are getting so much faster and better at breaking codes, 128-bit blocks of data now are being used as the new standard.

Extranet A private, TCP/IP-based network that gives users from the outside access to your internal network.

Firewall A firewall consists of hardware and/or software that lies between two networks, such as an internal network and an Internet service provider. The firewall protects your network by blocking unwanted users from gaining access and by disallowing messages to specific recipients outside the network, such as competitors.

Hacker An unauthorized person who breaks into a computer system to steal or corrupt data.

Internet Protocol Security (IPsec) A suite of protocols used for secure private communications over the Internet. IPsec protocols create a standard platform for securing IP connections on private networks.

Intranet An internal TCP/IP-based network behind a firewall that allows only users within the organization to access it.

Packet A piece of data that contains information, along with the address of where the data is going on the network.

PKI Short for Public Key Infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI.

Secure Sockets Layer (SSL) Secure Sockets Layer (SSL) is a protocol that protects data sent between Web browsers and Web servers. SSL also ensures that the data came from the Web site it's supposed to have originated from and that no one tampered with the data while it was being sent. Any Web site address that starts with "https" has been SSL-enabled.

Smart Card A small electronic device about the size of a credit card that contains electronic memory and possibly embedded integrated circuit (IC). Smart cards are used for a variety of purposes, including: storing a patient's medical records, storing digital cash, generating network IDs (similar to a token).

Two Factor Authentication Authentication using data entered (such as a password or PIN) combined with something held in possession (such as a device ID or token). Generally considered more secure than authentication based only on user id and password.

Virtual Private Network (VPN) A wide area network interconnected by common carrier lines, or that uses the Internet as its network transport.

Viruses, worms, Trojan horses, zombies Malicious software: Any software written to cause damage to or use up the resources of a target computer. Malicious software is frequently concealed within or masquerades as legitimate software. In some cases, it spreads itself to other computers via e-mail or infected floppy disks. Types of malicious software include viruses, Trojan horses, worms and hidden software for launching denial-of-service attacks.

Palm, Inc.
5470 Great America Parkway
Santa Clara, CA 95052
U.S. 1-800-881-7256
www.palm.com/enterprise