September 2002

White Paper: **Handheld Security for the Mobile Enterprise**

Mobile Computing: Opportunities and Risk

By providing on-the-go professionals with convenient mobile access to email, business applications, customer information and critical corporate data, businesses can help employees become more productive, streamline business processes and enable better decision making. But these benefits are not without risks. Sensitive corporate information stored on and transmitted by handhelds is vulnerable. With the new ease of access to information comes a responsibility to protect the corporation's data as well as the investment in handheld devices.

In many ways, security risks for mobile computing are similar to those for other computing platforms. There are the usual concerns of protecting data, authenticating users and devices and shielding against viruses and other malicious code. But because of their mobility and compact size, handhelds present some additional challenges:

- Because of their ease of use, handhelds tend to access corporate networks more often than other mobile platforms such as laptops.
- Because handhelds frequently connect wirelessly, robust wireless security becomes essential.
- Handhelds are more easily lost or stolen than laptop or desktop computers.
- Users often treat handhelds as personal devices and must be trained to consider the security risks when they use a handheld to access corporate data and networks.

Fortunately, the technology necessary to secure handheld access to corporate networks exists today. Strong security is multi-layered and must be woven into the very fabric of an organization. This paper examines some of the key issues in handheld security and discusses security solutions available for Palm™ handhelds.

Contents

Securing Enterprise Data in a Mobile World

Although conventional risk assessment would require that organizations carefully assess the cost of a security breach before it occurs, many of the benefits of security cannot be measured until security is compromised. In a survey of 503 companies by the Computer Security Institute of San Francisco in conjunction with the Federal Bureau of Investigation, 90% of the companies reported security attacks during 2001. Estimated average loss was $1.9 million per company.[1]

Another hard-to-quantify security risk is loss of reputation. For some companies, losing the confidence and goodwill of customers and business partners can be even more costly than the direct damage from a security breach. Prudent security measures not only protect assets but also safeguard business relationships.

Three major concerns are at the forefront of handheld security: data interception, theft or loss of the handheld and malicious code.

Data Interception

Today's handhelds offer a variety of ways to access and transmit data, including wireline synchronization, infrared (IR) ports, wireless LAN technology like Bluetooth and 802.11, and wireless Internet. As handhelds become increasingly connected to private and public networks, the danger of data interception rises exponentially.

Wireless wide area networks (WWANs) and wireless local area networks (WLANs) are particularly susceptible to data interception since data is transmitted over the air. There has been a flurry of

[1] The Economist, Inoculating the Network, June 22, 2002. (Only 233 of the 503 respondents were willing/able to quantify losses. Their combined losses were $456 million—nearly double their combined losses of the previous year.)

press recently about the ease of intercepting wireless transmissions, particularly in networks using the 802.11 protocol. If unencrypted data is intercepted, not only is the current data compromised, but the eavesdropper may be able to determine the identities of the communicating parties. Once an identity is obtained, the perpetrator can begin to masquerade as a legitimate user and send false or altered messages or access system resources. (This is often referred to as a "man-in-the-middle attack.") By implementing sound security procedures such as authentication, data encryption and message integrity checking, corporations can safeguard their data and communications.

User authentication ensures that only authorized users can gain access to system resources. User authentication is a common first line of defense. For example, before Mary can access the system, she must present credentials to prove she is indeed Mary. These credentials may simply be a username and password. For valuable assets, multi-factor authentication is advisable. The first factor is typically something a user knows (like her PIN, password or passphrase), and the second factor may be something a user has (such as a hardware or software token, certificate or smartcard). Biometric authentication (something the user is) can be used alone or in combination with the other authentication mechanisms.

Server authentication allows Mary to confirm that she is indeed talking to Company A's server and not to a bogus server masquerading as Company A. Server authentication should be used in transactions where the user is providing sensitive information such as a credit card number. To prove its identity, the server can use Secure Socket Layer (SSL) or Secure Electronic Transaction (SET) to send a digital certificate, signed by a Certificate Authority, to the user.

End-to-end encryption ensures that even if data is intercepted, it will be useless to the interceptor. There are two general categories of encryption algorithms: symmetric key encryption and asymmetric (or public) key encryption. Symmetric encryption uses the same key for both encryption and decryption. Asymmetric encryption uses two keys, one public and one private. The public key is widely known, while only the key owner knows the private key.

Mobile devices present unique data encryption challenges. Different algorithms require different amounts of processing overhead. In a handheld platform, it is important to employ an efficient encryption algorithm that protects data without degrading handheld performance or battery life. For example, Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are faster and use less battery life than Triple DES (3DES).

The intended application also influences encryption algorithm and method selection. Symmetric key cryptography requires less computational overhead, so data can be encoded and decoded more quickly than with an asymmetric key. This type of encryption works well for applications such as encrypting data on the handheld where the encryption key never leaves the device. Public key cryptography is typically used to establish communication between two parties. In many applications, these methods are complementary. For example, wireless messaging may use asymmetric keys to establish a session between a client and server, then use symmetric keys to encrypt the data that is exchanged.

Data alteration can be undetectable to an unsuspecting recipient, but the results can be just as devastating as a physical theft. As an additional protection against data tampering, message integrity checksums can be used to ensure that data has not been altered. Checksums confirm that the message could only have been created by an entity that knew the appropriate key. Sufficiently robust authentication, encryption and integrity checking mechanisms can effectively counter the risks of data interception.

Handheld Theft and Loss

The same factors that make handhelds attractive to mobile users—their portability, convenience and access to mission critical — also make them attractive to thieves and hackers. Despite a user's best efforts, a handheld may be stolen or lost, placing sensitive data at risk.

To prepare for this eventuality, IT needs to implement the following precautions for every handheld that contains corporate data:

- Mandate authentication. Power-on authentication prevents unauthorized users from gaining access to the handheld and any networks accessible by the handheld. While virtually all handhelds today allow the user to activate password protection, on many handhelds users can also turn off password protection. If users are carrying sensitive data, Palm recommends installing security applications that allow IT to enforce authentication protection and policies. IT then controls attributes such as whether or not a password is required, length and strength of password and expiration.

  Biometric authentication can combine convenience with strength. A variety of biometric authentication methods, such as voice, handwriting and fingerprint, are available for the Palm platform. Authentication thresholds can be set to optimize data security (lower number of false positives) or to minimize user frustration (lower number of false negatives).

- Encrypt sensitive data. Any data that the enterprise wants to protect should be encrypted when not in use. Data should also be encrypted before it is transmitted. Effective encryption protects data from both thieves and hackers.

- Back up data regularly. A recent backup enables quick restoration of lost applications and data in order to minimize downtime. IT should practice configuration management and conduct regular backups so that user data and profiles can be immediately restored.

Set procedures for revoking access permissions. Permissions dictate who can access the corporate network from the handheld. If a handheld is lost or stolen, IT must be ready to quickly remove its access permissions to any corporate networks and servers. Centralizing administration with directories such as LDAP (Lightweight Directory Access Protocol) makes revoking permissions faster and easier.

If these measures are taken, corporate data will be protected even if the handheld falls into the wrong hands, and the user will be able to return to productivity quickly. Since any handheld can potentially compromise the entire enterprise, these policies must be enforced uniformly throughout the organization.

Malicious Code

Malicious code can take the form of viruses, worms or Trojan horses. Viruses are codes that attach themselves to host programs and propagate to other programs that support macros when the infected program executes. As they execute, they can destroy or alter data. Worms perform pre-programmed attacks on networked computers. Trojan horses are programs that masquerade as a harmless application while performing a hostile action (such as opening a vulnerability on the computer or communicating data back to the creator of the code).

The malicious code may execute on the handheld itself or on networked computers once an infected file is transferred onto the network. Infections are generally transmitted through email attachments. A messaging server that inspects attachments before sending them to the handheld can mitigate this risk.

In addition, an anti-virus program with up-to-date signature files is essential for preventing infection of critical enterprise files and data. IT should have enforceable policies for running virus scans whenever new files are downloaded and for keeping the virus signature files up to date. If data is infected, there should be a means to recover it and to quickly restore the system to health.

Digitally signed code is used to verify the code's authenticity and integrity. Authenticity means that the code to be installed or launched is indeed from the stated developer or another trusted party. Integrity means that the code has not been altered since it was signed. Signing code entails taking a hash of the code, then encrypting that hash with the code signer's private key, or digital signature. This digital signature is then embedded in the code. Before installing or running the code, the receiving party verifies the validity of the digital signature, using the signer's public key. Signed code should be verified prior to installing or launching applications.

Foundations of Handheld Security

As more and more mission-critical data is accessed with handhelds, securing that information becomes a top priority for IT. Establishing, communicating and enforcing strong corporate security policies are key to reducing the risks associated with mobile computing. However, security threats and solutions seem to change continuously. What criteria can be used to choose partners and security solutions with confidence?

The Importance of Standards

Industry and federal standards and best practices provide an excellent starting point for formulating sound security guidelines. Standards are a critical component of the information industry, enabling hardware and software from different manufacturers to work together.

Organizations such as ISO (International Organization for Standardization) and IEEE (Institute of Electrical and Electronics Engineers) bring together experts to solve hard problems and create new standards. Other standards include the international Common Criteria and the British Standard 7799.

Depending on the nature of the business, government regulations and laws may influence technology selection. In the United States, the National Institute of Standards and Technology (NIST) develops standards and guidelines for federal computer systems, which are issued as Federal Information Processing Standards (FIPS). Many U.S. federal agencies are required to use FIPS-certified technology, and many companies regard FIPS certification as a proof of quality assurance.

Palm™ Solution Group's Crypto Manager is currently pending FIPS 140-2 certification. Crypto Manager provides strong cryptographic services to Palm applications, ensuring that critical security functions such as encryption, decryption, key generation, checksums, and pseudo random number generation are performed correctly. This certification indicates a trusted platform not only for the government but for any enterprise that wishes to protect its digital data.

The Health Insurance Portability and Accountability Act (HIPAA) sets standards for the security of medical records for all health plans, healthcare clearinghouses and healthcare providers that transmit health information in electronic format. The safeguards that comprise HIPAA-mandated security focus on protecting "data integrity, confidentiality and availability" of individually identifiable health information. All the security technologies needed to implement HIPAA-compliant solutions are available for the Palm platform.

Corporate Security Policies

Sound corporate policies are the foundation for preventing costly security breaches. Organizations must establish, communicate and enforce strong corporate policies. Some forward-thinking companies have a Chief Security Officer who issues comprehensive security policies for the entire organization. More commonly, security experts are dispersed throughout the organization. For such organizations, it is helpful to convene these experts as needed to create corporate policies, share best practices, and collaborate on system selection.

When the corporation demonstrates that security is taken seriously, the employees will also take it seriously. As a first step, physical security sets the tone for the entire organization. Second, security policies should be diligently enforced. For example, if the company policy calls for strong password protection, tools like L0phtCrack test whether users have set sufficiently strong passwords. Finally, security policies should be consistently and centrally administered as much as possible. By centralizing security management, the chance of human error is reduced. Consistent policies simplify management and reduce error while ensuring that all parts of the organization are protected.

Extending Enterprise Security to Handhelds

When extending enterprise applications to handhelds, it is important to maintain the same levels of performance, privacy and reliability that users have become accustomed to within the walls of the corporate office. Organizations must craft a security policy that balances protection of sensitive data and communications with usability and cost.

The sections that follow explore in more detail the elements of a successful enterprise mobile security program, including authentication, encryption, malicious code protection, monitoring, security for local wireless networks and disaster recovery. To protect their valuable data, most organizations will choose to implement multiple layers of security.

Authentication

The purpose of authentication is to prove that a party is who he or she claims to be.

Below, we will discuss two levels of authentication: user authentication to the handheld itself and authentication to remote systems.

Handheld Authentication
The first level of authentication involves accessing the handheld itself. Handheld authentication protects corporate data and network access in the event of theft. Desktop computers can easily be physically secured: they can be locked in an office and bolted to a desk. Because handhelds are more difficult to secure physically, it is important to ensure that if an unauthorized person gains possession of the handheld, they will not be able to activate it.

Every Palm handheld running Palm OS® version 4.1 or later has built-in password protection. This simple yet effective application has no back doors and includes features such as automatic password locking options and password hinting for forgotten passwords. To ensure privacy, the password is hashed and only the hash value is stored.

Managed security solutions from Palm Solution Providers enable the IT administrator to enforce handheld security policies. IT can make password protection mandatory for the user and set policies such as length and type of password, frequency of password change and timeouts, as well as control encryption and application access. In addition, such applications protect against brute force password attacks with data-wipe functionality. Policies are persistent on the handheld and can only be changed by the designated Administrator.

Additional handheld security solutions from Palm™ Solution Providers are described in the Appendix.

Remote System Authentication
In addition to being authenticated on the handheld, many enterprise applications require the user to authenticate to remote systems. Corporate networks and servers should require users to authenticate with a username and a secret and/or unique identifier before access is granted.

Palm OS has built-in PPP support using popular authentication protocols including the Challenge-Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), and Password Authentication Protocol (PAP).

Palm also offers multiple methods to uniquely identify the handheld, including Hardware Serial Number (HSN), flash ID, and Mobile Access Number (MAN). Any of these unique identifiers can be used to authenticate the handheld for network access, allowing Palm handhelds to be used as a physical token for two-factor authentication. Popular authentication tokens, such as RSA's SecurID and Secure Computing's SafeWord, can be used with Palm handhelds. Up to eight RSA SecurID tokens can be stored on the Palm handheld, eliminating the need to carry multiple key fobs. Trio Security offers a solution that turns your Palm handheld into a token, while incorporating biometric authentication and single-sign on functionality.

Ideally, handheld security policies should be integrated with a central user directory and consistent across systems. Such best practices simplify administration, ensure a base level of security on all systems and prevent common mistakes such as removing a user from only one system rather than all systems.

For more on available authentication solutions as well as VPN clients for the Palm platform, please see the Appendix.

Encryption

Encryption is one of the pillars of data security, and any data that the enterprise wishes to protect should be encrypted. Modern cryptographic techniques use a combination of a cipher and a key to maintain privacy. The strength of the privacy depends on the strength of the algorithm and the size of the key, measured in number of bits. Any data that is stored on non-secured media or being transported across a network is susceptible to attack.

Handheld Encryption
Encryption of data stored on the handheld is vital to comprehensive, end-to-end encryption. Since handhelds tend to be more accessible to intruders than servers or desktops, it is prudent to be even more vigilant when protecting handheld data.

Multiple data encryption solutions are available for the Palm platform. Managed security solutions from Palm Solution Providers allows the IT administrator to control what data must be encrypted and offers the option of protecting individual databases with an additional level of password protection. A variety of encryption algorithms are available including AES, TDES, and Blowfish. For example, IT can enforce the rule that all users in the sales group will encrypt their customer relationship management (CRM) data, while all users in the engineering group must encrypt their Memo Pad database. Since sensitive data can reside not only on the handheld but also on expansion cards, many applications extend encryption to SD and MMC cards.

Palm Solution Providers also offer a wide selection of applications for handheld data encryption. This functionality is typically combined with advanced password protection and other features. See the Appendix for more information.

Communications Encryption
Palm handhelds typically send and receive data using either wireline communications (via synchronization cradle) or wireless communications. Since cradle synchronization is inherently private, this discussion focuses on the privacy of wireless communications.

One way to ensure privacy is to use a virtual private network (VPN). An IPSec VPN client performs encryption as well as authentication and data integrity checking. The selection of encryption algorithms allows an organization to choose a level of encryption that balances requirements for privacy and performance.

PPTP VPNs are easy to configure and are supported by most Microsoft servers, as well as many Cisco gateways.

In addition, there are many cryptographic toolkits, Public Key Infrastructure (PKI) toolkits and cryptographic libraries available for the Palm platform via Palm Solution Partners and open source code. A sampling of such toolkits is listed in the Appendix.

Malicious Code Protection

To date, there have been no successful virus attacks on the Palm platform. Since viruses are platform specific, Palm™ handhelds are not susceptible to the thousands of viruses developed for the Windows platform and cannot pass viruses back to the desktop during synchronization. But when it comes to security, it is best not to be complacent. Any connected system can be at risk for malicious code, and IT organizations need to be prepared.

Protection from malicious code begins with good anti-virus software. Best practices include frequent updates for the latest virus signatures and scanning of files immediately after receiving data. Best-in-class anti-virus software vendors such as Symantec, McAfee, TrendMicro and Computer Associates create anti-virus applications for Palm handhelds. See the Appendix for more details

Using code signing, organizations will be able to control more effectively what applications are run on the Palm devices. They can choose to only allow programs that have been signed by a trusted party to be installed and run; digital code signing will ensure the authenticity and integrity of the code, thus preventing malicious applications to compromise critical data and resources of the handheld. Digital code signing is a planned feature for Palm OS®.

Securing Wireless LAN and PAN Networks

Palm handhelds support a variety of connectivity options, available today, from WANs to WLANs and PANs (personal area networks). Palm supports both the Bluetooth and 802.11b protocols. Palm is focusing on optimizing next generation 802.11b solutions for handhelds. In addition, every Palm handheld has a built-in IR port that allows simple, fast data transfer.

802.11b
802.11 is a widely deployed and immensely popular WLAN standard. The built-in security available with today's 802.11 products has received a great deal of negative publicity due to Wired Equivalent Privacy (WEP) encryption vulnerabilities and poor authentication. IEEE is working hard to ratify new standards for authentication, privacy and interoperability such as WPA and 802.11i.

By August 2003, WPA and Temporary Key Integrity Protocol (TKIP) is expected to ship with many 802.11 products. TKIP is a temporary fix to WEP encryption problems, and can be applied to existing hardware through driver and firmware upgrades. Simultaneously, a long-term, AES-based solution is in the works. This solution will need to be incorporated in new hardware designs. The 802.1x standard is meant to improve authentication. Although the standard has not yet been ratified, solutions based on 802.1x have begun appearing in the marketplace.

Cisco's LEAP (Lightweight Extensible Authentication Protocol) is based on the 802.1x standard. LEAP provides mutual authentication based on password challenge-response. Since it was specifically designed to be"Lightweight", LEAP is well suited to mobile devices.

What can today's users of handhelds with 802.11 do to protect their data and networks? Solutions such as RADIUS, RSA SecurID and VPN can be deployed today to provide strong authentication. If an IPSec VPN is used, the data will also be protected with enterprise-class encryption and data integrity checking. In addition, many enterprise applications provide encryption and authentication as part of the base product. When building custom applications, organizations should consider incorporating encryption modules to protect data privacy during transmission.

Bluetooth

Bluetooth is an emerging wireless technology intended primarily for use in PANs. Bluetooth links devices within close proximity to one another (about 30 feet), using wireless communications to replace USB cables. PANs are spontaneous, or "ad-hoc," and require no infrastructure. Palm believes that Bluetooth is the optimal technology for PANs because of its small chipset and low power consumption.

While the Bluetooth specification does a respectable job in considering security factors, potential security risks in Bluetooth networks include man-in-the-middle attacks, as well as the possibility that other devices could try to access sensitive data by masquerading as connection-accepting or connection-seeking devices on the Bluetooth network.

The following built-in features of Bluetooth make it relatively secure against these types of attacks:

- User authorization required for data transmission. Bluetooth devices that accept user input, such as handheld devices, require user permission before transmitting or receiving data.
- Frequency hopping algorithm. Bluetooth transmits signals using short bursts on a pseudo-random sequence of different frequencies. Thus, a receiver cannot simply be tuned to a given frequency to intercept Bluetooth traffic—it must use the same frequency hopping pattern as the transmitter.
- Encryption algorithm based on SAFER+. The E1 encryption algorithm used by Bluetooth is based on SAFER+, an algorithm that has been in the public domain since 1998 and was a thoroughly reviewed AES candidate.
- New encryption key for each session. Bluetooth transmissions use separate keys for authentication and encryption. The encryption key is regenerated for every session, further limiting damage that can be done through man-in-the-middle attacks.
- Combination keys. The Bluetooth SIG recommends using combination keys whenever possible instead of unit keys. Combination keys use information from both the master and slave to authenticate users and to encrypt data. This ensures that devices in a valid piconet cannot masquerade as other devices to gain unintended access.
- Secret PIN and device address required for authentication. For any device accepting user input, authentication requires both a secret PIN known by the user and a correct device address. This means that fraudulent device cannot simply guess PIN numbers to gain access to other Bluetooth devices.

Additional security solutions can be used with Bluetooth to achieve excellent security. For example, PKI can be used to add strong authentication, encryption, digital signing and non-repudiation. RSA Security and others make PKI toolkits that work on Palm™ handhelds. For more information about Bluetooth, please see the white paper at http://www.palmos.com/dev/tech/bluetooth/palm_bluetooth_mwp_r1.pdf.

Infrared (IR)

The IR port is a relatively secure means of communication. It requires close physical proximity (4 feet or less) to the beaming device. The recipient is prompted when a beam is sent and must tap on the screen to accept incoming data. Palm handhelds also have built-in "sleep" thresholds (typically 1-3 minutes), and when sleeping the handheld cannot accept an incoming infrared beam. This means that the user controls what he or she receives. For those organizations that need to deactivate the beaming feature, Security Plus and other security applications include functionality to disable the IR port.

Backup and Recovery

When the worst happens, proper backup and recovery procedures can be the key to quickly restoring users to productivity. Limiting and containing the impact of a security breach is critical. If an employee's handheld is lost or stolen, their account should be quickly disabled on all systems, and their handheld segregated from the network.

To get the enterprise user back up and running, their data needs to be restored to another handheld. If backups are performed regularly, the data is safely within the corporate firewall and can be quickly restored to another handheld. Data backups can be performed via a PC-based HotSync® operation, network HotSync operation, server-based synchronization or Secure Digital Input/Output (SDIO) backup cards, which use the expansion slot available on most Palm handhelds.

Management solutions from Palm Solution Partners help companies manage handhelds, applications, and content from a central location. For example, IT administrators can deploy applications for use in the field; manage, exchange and deliver content; capture and store hardware and software information, automatically track handhelds and their health; and provide automated system and data backup and restore capability—all from a central location.

The Future of Security in an Insecure World

Security has become a top priority for business and government organizations, and many exciting new developments are expected to be available for widespread deployment in the not-too-distant future. A number of fascinating security products are in various phases of evolution, with such possible applications as biometrics, smartcards and location-based systems.

Biometric systems analyze unique physiological traits such as fingerprints, hands, voices and facial patterns. What makes biometric systems so effective is that physical characteristics such as these are unique and very difficult to counterfeit. Voiceprint matching, fingerprint recognition, facial and hand geometry patterning, iris scanning and thermal detection are all possibilities for handheld security. The beauty of biometric authentication is that it merges strength with convenience. Users can gain access simply by uttering a passphrase, touching a screen or scrawling their signature.

Smartcards contain integrated circuits that provide tamper-proof storage of user and account identity and protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Smartcards can work with Palm handhelds via the expansion slot or a USB attachment and can be used for a wide variety of applications including digital signing, strong authentication, and secure ewallet solutions.

For example, fingerprint and voice recognition technology could be combined with a public key cryptography system on a smartcard. Each smartcard would hold a bio-template of the user's fingerprint and voice, both secured using biometric verification software. The user would access the system by speaking a previously recorded password and placing a finger in the reader. Systems such as this are already in pilot.

Location-based technologies, used today in consumer applications such as navigation systems, enable interesting security applications such as location-based access control and fraud detection. Global Positioning System (GPS) applications for handhelds are becoming increasingly popular. GPS uses a system of satellites that continuously broadcast their exact location in space and the precise time. By tracking the signals from four of these satellites, a GPS receiver on earth can determine its current latitude, longitude and altitude to within 20 meters. Technologies such as 802.11 and Bluetooth access points can be used for even finer-grained proximity control.

Conclusion

Today, handhelds have evolved into indispensable enterprise tools that enable an increasingly mobile workforce to remain connected and productive. As handhelds proliferate and become an integral part of the corporate technology infrastructure, handheld security must become a serious concern for every IT manager as well as for corporate handheld users. Protecting corporate information is essential to business survival and growth, and end-users must be trained to safeguard the resources that are carried or accessed on handhelds.

A clear understanding of the challenges posed by handhelds in a particular environment provides the basis for developing sound security policies, standards and practices. A security strategy must strike a balance between what is possible and what is feasible, basing decisions on industry best practices and clearly articulating guidelines and procedures. Encryption programs, anti-virus software, effective password use, training and awareness are all components of an effective enterprise security program.

The Palm™ Solutions Group and its Solution Providers are committed to addressing the security needs of enterprises by developing products and solutions that enable organizations to adopt security best practices and minimize the risks involved in mobilizing their workforce. The Palm philosophy of open standards and inter operability ensure that these solutions will evolve with our customers' security requirements.

Appendix: Applications from Palm Solution Providers

The following are additional security solutions from Palm Solution Providers.

Handheld Authentication and Encryption Solutions

Product	Features
Asynchrony PDA Defense Enterprise	PDADefense Enterprise provides enhanced password protection, 128-bit or 512-bit Blowfish encryption and hardware button password entry. IT managers can enforce password, encryption and beaming policies and set restrictions on application usage.
Certicom movianCrypt	movianCrypt uses 128-bit AES to encrypt handheld data , provides advanced password security and auto-lock functionality.
Communication Intelligence Corporation Sign-On	Sign-On uses biometric signature verification to safeguard data on a device. Users simply sign their name or create a personalized drawing or design and Sign-On verifies it to unlock the device.
Credant Technologies Mobile Guardian	Mobile Guardian addresses mobile security issues with centrally managed, policy administration and strong on-device user authentication and policy enforcement.
IS/Complete PDA Restrictor	Restrictor allows an administrator to create profile categories for different users on a single Palm handheld and enables users to automatically lock their Palm and hide records.
Kasten Chase Assurency SecureData for Palm OS®	Assurency SecureData provides record-level encryption for all data stored on the handheld and decrypts only as required, ensuring a fast user experience. An enterprise version empowers the IT Administrator.
TealPoint Software Corporate TealLock	Corporate TealLock is a secure automatic locking program. Features include serial and infrared lockout, data encryption, administrator password, remote-unlocking, and password controls.
Trust Digital PDASecure	PDASecure encrypts data on the handheld using AES. It features universal integration with all applications installed on the handheld and allows administrators to define security policies.

Authentication

Product	Features
RSA Security SecurID	SecurID software, used in conjunction with RSA ACE/Server software, generates a random, one-time-use access code that automatically changes every 60 seconds.
Secure Computing e.iD for Palm	From the maker of SafeWord authenticators, e.iD for Palm is a software authenticator for the Palm Computing platform. It allows any device running Palm OS v2.04 (and higher) to become a PremierAccess enabled authenticator.
Trio Security Trio VAULT™	Trio VAULT combines 3-factor user authentication, a single-sign-on solution, and access management into a single, integrated Palm OS® application that interfaces seamlessly with the existing network security infrastructure and eliminates the need for authentication and single-sign-on servers.

Virtual Private Network (VPN) Solutions

VPNs are used to provide secure access to intranet and extranet resources and data. VPN technology is in wide use today, enabling mobile laptops and home office users to gain remote access to corporate data.

Product	Features
Certicom movianVPN	movianVPN is an IPSec VPN client that provides strong authentication, encryption and data integrity checking to secure remote access to email and data. movianVPN supports a wide variety of popular gateways, including Cisco, Lucent and Nortel
Mergic VPN for Palm OS	Mergic VPN is a PPTP (Point-to-Point Tunneling Protocol) VPN client for securing remote access.

SafeNet SoftRemotePDA™	SoftRemotePDA is an IPSec VPN client that. offers secure client-to-gateway communications over wireless networks and works with many popular gateways.
V-ONE Corp. SmartPass for Palm	SmartPass is a VPN client that provides secure remote access. SmartPass connects to V-One's SmartGate VPN server.

Cryptographic and PKI Toolkits

Product	Features
Blueice Research Multipass Client	Multipass Client is based on open Public Key Infrastructure (PKI) standards. This multi-platform client provides strong encryption functionality and the ability to perform secure digital transactions.
Certicom Trustpoint Client	Trustpoint Client adds PKI security to client-side applications running on Palm OS. Supporting both X.509 and WTLS digital certificates, Trustpoint Client allows developers to add digital signature and strong encryption to applications to support trust, authentication, confidentiality, privacy, and message integrity.
Diversinet Corp Passport	Passport client/server security software facilitates digital signatures, authentication and encryption with PKI products specifically optimized for wireless environments and devices
Ntru Cryptosystems Inc. Security Toolkit for Palm	Ntru offers a full range of public and symmetric key functionality, including encryption, decryption, signing and verification.

Anti-virus Applications

Product	Features
Computer Associates InoculateIT	InoculateIT is specifically designed to provide immediate and complete protection against all current known malicious attacks targeted at the Palm OS platform.
F-Secure Anti-Virus™ for Palm OS	Anti-Virus features resides on the handheld to provide always available protection, auto scanning after HotSync and automatic antivirus database updates.
McAfee Anti-Virus Resident Scanner	Resides on the handheld and can be used anytime for scanning. End-users can scan immediately after receiving data via IR, synchronization or wireless transmission. If a virus is discovered, the user is alerted, and synchronization is blocked until the destructive code has been deleted.
McAfee VirusScan Wireless	Scans handheld for PC viruses each time synchronization is attempted.
Symantec AntiVirus for Palm OS	Scans Palm files looking for signatures of viruses, Trojan horses and worms, and prompts the user if malicious code is detected. In addition, AntiVirus for Palm OS automatically updates virus definitions to the handheld during synchronization with the PC.
Trend Micro PC-cillin for Wireless Version 2.0 for Palm OS	Provides automatic real-time launch scanning to prevent viruses that enter the handheld from every possible entry point: beaming, synching, email and Internet downloading. Real-time launch scanning activates whenever applications on the handheld are launched and prevents viruses from activating on the handheld.

Glossary

3DES or TDES: Triple DES, a stronger version of DES encryption in which the input data is, in effect, encrypted three times.

802.11: A family of specifications developed by the IEEE for wireless LAN technology. The most commonly deployed 802.11 specification is 802.11b, also called Wi-Fi.

802.1X: An IEEE standard based on Extensible Authentication Protocol that provides an authentication framework for 802-based LANs.

AES: Advanced Encryption Standard, an industry-standard cryptographic algorithm. Also called the Rijndaal Algorithm.

Algorithm: A specific mathematical formula to perform a function (like encryption and decryption). Some algorithms are more secure than others, while some are faster than others.

Asymmetric Encryption: Any encryption scheme where the sender and receiver use a pair of different but related keys that cannot be derived from one another. Data is encrypted with one of the keys and decrypted with the other key.

Biometric Authentication: Any method for verifying identity that relies on a unique personal attribute, such as fingerprints or the blood vessel pattern around a retina.

Bluetooth SIG: Bluetooth Special Interest Group, the trade association of wireless company representatives and other experts who define and maintain the Bluetooth specification for short-range wireless transmission.

Blowfish: A symmetric block cipher developed by Bruce Schneider in 1993. Blowfish has undergone considerable review and is gaining acceptance as a strong encryption algorithm.

Certificate: Usually, a public key digitally signed by some signing authority to guarantee its validity.

Certificate Authority: A trusted third-party clearinghouse that issues digital certificates and digital signatures.

CHAP: 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. Encrypting the username and password before transmission protects your credentials from eavesdroppers.

Checksum: A technique whereby the individual binary values of a string of data are totaled before network transmission and after to verify that nothing has changed.

Cipher: The generic term used to describe a means of encrypting data. May also refer to the encryption algorithm.

CRM: Customer relationship management.

Encryption: Any method of scrambling data so that it cannot be read during storage or transmission. The data is then kept confidential until it is decrypted (unscrambled).

Flash ID: Unique serial number for the ROM in a Palm device.

FIPS (Federal Information Processing Standards): Standards and guidelines for federal computer systems issued by NIST.

GPS: Global Positioning System, a worldwide radio navigation system.

HIPAA (Health Insurance Portability and Accountability Act): U.S. legislation that, among other things, sets standards for the security of medical records in electronic format.

HMAC: Hashed Message Authentication Code, a message digest function and secret key used to create authentication codes using MD5 or Secure Hash Algorithm (SHA).

HSN: Hardware Serial Number.

IEEE: Institute of Electrical and Electronics Engineers. A large, international, non-profit, technical professional association that establishes consensus-based open standards.

IETF: Internet Engineering Task Force. A large open international community of professionals concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

IPSec: IPSecurity, a tunneling protocol developed by IETF and used to implement VPNs.

IR port: An infrared port, a port built into many models of handhelds for transfer of data between devices.

ISO: International Organization for Standardization, a worldwide federation of national standards bodies from more than 140 countries.

ISP: Internet service provider.

Key: Usually, an alphanumeric string used for encryption and/or decryption.

LAN: Local area network.

LDAP: Lightweight Directory Access Protocol. An open standard protocol for directory lookups which uses a hierarchical naming structure.

MAN: Mobitex Access Number.

MD5: A one-way hash algorithm used to create a message digest for digital signatures.

MMC: MultiMediaCard cards, a non-secure, removable storage media for Palm handhelds.

NIST: National Institute of Standards and Technology, a non-regulatory agency within the U.S. Commerce Department that develops and promotes measurements, standards, and technology.

PAN: Personal area network. A wireless network that enables handhelds, cell phones, and other mobile devices to communicate over short distances.

PKI: Public key infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate each party in an Internet transaction.

PPTP: Point-to-Point Tunneling Protocol. A protocol developed by Microsoft and others to enable VPNs.

Public Key Encryption: An asymmetric encryption scheme such as RSA, Diffie-Hellman-Elgamal, and elliptic algorithms.

RADIUS: Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet service providers. The specification is maintained by IETF.

SAFER+: An encryption algorithm submitted by Cylink Corporation as an AES candidate. SAFER+ provides slightly less than the suggested 2128-order protection, given 128-bit keys, which is why it was not chosen for AES. Experts agree, however, that this academic imperfection does not allow it to be broken in practice.

SET: Secure Electronic Transaction. An open industry standard protocol developed for the secure transmission of payment information over the Internet and other electronic networks.

SD: Secure Digital cards, a secure removable storage media for Palm handhelds. Uses the same form factor as MMC.

SDIO: Secure Digital Input/Output.

SHA1: Secure Hash Algorithm. A popular algorithm for computing cryptographic checksums.

SMS: Microsoft Systems Management Server, a product that provides tools for software distribution, asset management, and remote troubleshooting for Windows–based desktop and server systems.

SNMP: Simple Network Management Protocol.

SSL: Secure Socket Layer, a commonly-used protocol for managing the security of a message transmission on the Internet.

Symmetric Encryption: Any encryption scheme where the sender and receiver share the same key.

TKIP: Temporary Key Integrity Protocol, a temporary fix to WEP encryption problems, which can be applied to existing hardware through driver and firmware upgrades.

USB: Universal Serial Bus, a plug-and-play interface between a computer and add-on devices.

VPN: Virtual private network. A network which emulates a private network, although running over a public network. The use of encryption and a tunneling protocol maintains privacy.

WAN: Wide area network.

WEP: Wired Equivalent Privacy. A security protocol for wireless local area networks defined in the 802.11b specification.

WLAN: Wireless local area network.

WTLS: Wireless Transport Layer Security.

Palm Solutions Group
400 N. McCarthy Blvd.
Milpitas, CA 95035
1-888-223-4817
www.palm.com/enterprise

P582 01