Preventing Mobile Mayhem

Securing Mobile Devices in the Enterprise

The Security Balance

Protecting sensitive information has been the concern of businesses for about as long as there have been businesses. Throughout history, artisans, artists, and athletes have sought to hide their techniques from the competition. In the modern era, trade secrets can make or break entire companies. For all of these audiences, and for any business in today's information economy, the common concern is the protection of information vital to success.

Of course, the strategies and techniques used today to protect critical data are much more involved than those of the past. Securing data and network traffic is a top priority for any business connected to the Internet, which by its very nature can increase the possibility for security breaches if the proper security measures are not put in place. Yet few would dispute the fact that the Internet has been instrumental in increasing productivity and creating new business opportunities.

A similar situation exists for mobile computing. In the last few years, handheld devices, lead by those based on the Palm OS® platform, have played an increasingly important role in the enterprise. Several million handheld devices have been deployed in enterprise environments, and a large percentage of these have a wireless connection to corporate networks. This widespread adoption of mobile devices has created a new set of concerns for security professionals in nearly all industries, and the growing tendency of these devices to connect to networks using wireless technologies compounds these security concerns even further. As with any business solution that accesses corporate data, the security of mobile devices must be assured.

Accordingly, companies face the dilemma of implementing security measures to protect their data and their assets without negatively impacting the rise in productivity derived from the use of mobile devices. For every security measure put in place, a company must evaluate the impact on the productivity and efficiency of its employees. In this regard, different businesses are likely to find one level of security more comfortable than another. Taken to extremes, security precautions that are too stringent may hinder productivity. For a business to be successful, it must strike the proper balance between strong security measures and worker productivity.

Companies therefore require a security platform that provides a high degree of flexibility and scalability. Only by being able to review a variety of options can an organization identify the right level of security for its needs and then determine which solution to deploy. As the needs of the organization change, a security platform must be able to scale to meet the new security requirements. With these considerations in mind, security professionals should ask themselves a number of questions concerning the deployment of a mobile platform:

- How flexible is this mobile platform?
- What security options are available for this platform?
- Does it provide a strong enough level of security, without sacrificing ease of use?
- Do the security measures incur any performance hit, or degradation in speed or battery life?
- How easily does it integrate into existing systems?
- Will it scale as the demands for stronger security measures increase?

Fortunately, there is a solution that offers both the strength and the flexibility required: Palm OS.

As the most widely deployed handheld platform for the enterprise, the Palm OS continues to deliver on the promise of providing a stable, scalable platform with the widest range of security options available for mobile computing. The introduction of Palm OS 5 raises the bar even higher, incorporating a suite of robust security options without sacrificing the Palm OS tradition of flexibility and ease of use.

In the following sections, this paper will discuss some of the key security concerns associated with mobile devices. For each of the three areas examined – data access, network communications, and systems administration – companies must evaluate not only the overall performance of the mobile platform but also the security options available and how well they integrate into existing systems. Addressing all of these concerns, the Palm OS delivers the strength and flexibility required to satisfy the needs of most organizations.

Securing Access

One of the greatest advantages of mobile devices, particularly those based on the Palm OS, is the ability to extend the reach of vital information to where it matters most. For a sales person visiting a customer, for a support team out in the field, or for employees in a meeting room at the office, having the right information at the right time is an invaluable asset. Instant access to crucial data can easily become a huge competitive advantage, increasing productivity, providing more effective customer service, and reducing time and cost restraints.

With mobile devices fast becoming essential tools for the modern-day workforce, companies need a reliable solution to secure the data on the device. For the security professional, the small form factor and mobile nature of these devices also create a set of new challenges. Some of these challenges include controlling access, preventing invasive activities, protecting data if the device is lost or stolen, ensuring data integrity, backing up data, and guarding against viruses and other malicious software.

Building upon a proven operating system, Palm OS 5 delivers a foundation for deploying a secure mobile platform that is both robust and versatile.

Access Control

Limiting access to a device through password protection is one of the most basic requirements in securing handheld devices. Often times, however, this basic protection may not be enough for an organization's security needs. Therefore, a viable mobile platform should offer both a reliable user verification method and security measures that encrypt the data and applications stored on the device.

User Verification

For some companies, a simple password challenge may be sufficient. For protecting more sensitive data, a more stringent authentication approach will be necessary. Even within an organization, some users may have different security needs than others. A mobile platform must therefore pro-

vide a choice of options for verifying the answers to two important questions: Who are you? and What level of permission do you have?

Requiring password entry to unlock the device has been a standard feature of the Palm OS for many years. Palm OS 5 extends this capability by adopting a much broader approach to access control. Palm OS 5 will encompass a system-wide authentication and authorization system that will allow businesses and developers to use any of a number of methods to restrict access.

The Authorization Manager built into Palm OS 5 will enable applications to specify a set of rules that must be met in order to access data on the device. With this capability, any managed resource can be protected, including stored data, application code, and kernel resources. The Authentication Manager in Palm OS 5 will manage any token used for verifying access, including such standard tokens as passwords, PINs, or pass-phrases. Featuring an extensible architecture, the Authentication Manager will also allow developers to incorporate such authentication methods as biometric verification (handwriting, voice recognition, fingerprints, etc.) and smart cards.

Additionally, the Authentication Manager will include support for signed code, so that only applications that have a valid digital signature may access certain data and resources. Among other benefits, this feature will assist businesses and developers in managing the installation and upkeep of approved software programs, while also ensuring that malicious programs cannot tamper with data stored on the device.

Data Encryption

Losing a handheld device – or worse, having it stolen – can have dire consequences for a company. Not only is there a loss of productivity, but there is also the very serious threat of the data on the device falling into the hands of a competitor. Even if the device is protected by a password, the data may not be completely secure, as a determined programmer may succeed in bypassing the access control layer. In order to protect data in situations such as these, the ability to encrypt the data on the device provides an additional layer of security.

Software developers for the Palm OS have been providing encryption solutions to enterprise customers for about as long as there has been a Palm OS. With the introduction of Palm OS 5, the Palm OS platform takes data encryption to a new level. On Palm OS 5, system-wide strong encryption (128-bit) is a standard feature of the operating system. Based upon the de facto standard RC4 encryption algorithm from RSA Security, the encryption features on Palm OS 5 can be applied to the entire device or to only selected data and resources.

Additionally, Palm OS 5 is built upon a 32-bit architecture and fully supports ARM®-compliant processors, enabling businesses and developers to activate these encryption features while maintaining the high level of performance expected from the Palm OS. Palm OS 5 will also allow businesses and developers to incorporate other encryption algorithms, such as Advanced Encryption Standard (AES), through a suite of APIs. With these capabilities, the Palm OS platform not only provides one of the world's most trusted encryption schemes as a standard feature, but it also delivers the flexibility to encompass future algorithms as they become available.

Data Integrity

Safeguarding corporate data involves more than merely prohibiting access to unauthorized parties. The security of data and resources also involves ensuring that no data is lost. Not having a device – specifically, not having the information on that device – could negatively impact productivity or severely impair a business deal or project. In the event of a handheld device failing or being misplaced, security professionals require the ability to restore the data so that normal business operations are affected as little as possible. Replicating the data on the device to a desktop computer or server is therefore a key attribute for any mobile platform.

Another important consideration with regard to data integrity is ensuring that the information on the device is current. In certain situations, having outdated or obsolete information can significantly hinder the success of a project or sale. Organizations therefore require the ability to synchronize data on a handheld device with information stored in a personal computer or central database, thereby ensuring that the user has accurate data.

The synchronization and redundancy of data are an inherent quality of the Palm OS platform. Indeed, data synchronization and back up to a desktop computer have been a staple of the Palm OS since its inception. Seeking to deliver a synchronization platform that is both powerful and versatile, the Palm OS features a mature suite of conduit APIs, allowing businesses and developers to customize the manner in which the mobile device communicates with the synchronization target.

Additionally, there are a number of server synchronization and back up solutions available from software developers for the Palm OS. Each of these extends the synchronization architecture of the Palm OS platform to include back-end servers that can centrally manage and distribute the appropriate information to the appropriate individuals in an organization. (Please refer to the appendix for a list of synchronization and back-up applications available on the Palm OS platform.)

Virus Protection

Thus far, mobile computing platforms have been relatively safe from virus attacks, but there is certainly no guarantee that a mischievous programmer will not create a destructive virus in the future. A virus attack can, under certain circumstances, deal a crippling blow to any organization, regardless of the source of infiltration. A virus may not only attack the handheld device itself, but it may also endanger the desktop computer to which it is attached. Some software may appear to be a legitimate application, only to turn into a Trojan horse that wreaks havoc over a network. Others may have a more damaging result, corrupting or deleting files or rendering a device inoperable. As with any computing platform, mobile devices can be susceptible to virus attacks, and security organizations need to be prepared. This is particularly true as more and more mobile devices directly access the Internet over wireless connections.

To date, the Palm OS platform has been remarkably safe from virus attack, and several solutions exist to provide additional assurance into the future. With solutions from numerous developers, the Palm OS platform is protected by an extensive array of anti-virus software. (Please refer to the appendix for a list of anti-virus applications available on the Palm OS platform.) This broad range of anti-virus solutions makes the Palm OS platform one of the safest mobile computing environments today.

Securing Communications

The use of mobile devices has grown far beyond the initial functions of a personal digital assistant (PDA). Certainly, managing personal information such as an address book or calendar remains an integral task for any mobile computing platform and will continue to do so for the foreseeable future. As mobile devices have evolved, the capacity to access information remotely – to deliver the right information at the right time – has become an increasingly important function for these devices.

Accordingly, the market has not failed to recognize the advantages of a wireless connection on a mobile device. Manufacturers have introduced several new products, mostly based on the Palm OS, that integrate PDA features with a mobile phone and Internet access, and businesses have begun to adopt these new technologies at an escalating rate. A recent study from IDC has shown that this "convergence" trend will grow significantly over the next few years, reaching a level of almost 80 million wireless communicators and smart phones sold in the year 2005.

As these wireless mobile devices become more prevalent, security professionals require a solution that can both meet existing security needs and offer the flexibility to adapt to future needs. For most organizations, the ability to encrypt data transmission is a fundamental requirement. A mobile platform should therefore support end-to-end communication encryption schemes, such as Secure Sockets Layer (SSL) encryption. Additionally, the ability to extend a corporate network to remote devices in a secure manner is another leading concern. Such a deployment should include both data encryption and the employment of password authentication and challenge-response security protocols. Currently, a virtual private network (VPN) is the preferred method for providing secure access to intranet or extranet resources and data, so the mobile platform must support a reliable VPN solution.

With a rich heritage of providing secure data communications, the Palm OS platform offers a variety of solutions for protecting remote access, including support for unique device identification. For mobile devices based on the Palm OS, network administrators can use several methods to identify a unique device, including Flash ID, Mobile Access Number (MAN), and Electronic Serial Number (ESN). Any of these unique device IDs can be used to authenticate the device for network access. Moreover, these unique identifiers allow mobile devices based on the Palm OS to be used as a physical token for two-factor authentication. Palm OS also supports Microsoft's Challenge Handshake Authentication Protocol (CHAP), and there are several VPN clients available for the Palm OS. (Please refer to the appendix for a list of remote access applications available on the Palm OS platform.)

The introduction of Palm OS 5 greatly enhances the security of mobile communications. The addition of SSL strong encryption (128-bit) enables software applications for the Palm OS to secure any data transmitted via an Internet connection. By incorporating the RC4 encryption algorithm as a system-wide capability, Palm OS 5 provides as a standard feature the world's most commonly used and trusted encryption protocol for data transmission. As new transmission algorithms are developed, devices and applications for the Palm OS will be able to utilize these new encryption schemes through the plug-in encryption architecture of the Palm OS. With this set of capabilities, the Palm OS platform offers a complete solution for securing mobile communications.

Administering Mobile Devices

For security professionals, having the tools available to protect mobile devices is only half of the battle. The ability to manage these devices, including the distribution and upkeep of essential software applications on all devices, is equally vital to success. Administration and management solutions for the enterprise must fulfill a number of responsibilities, depending upon the needs of the organization. Some common tasks managed by these systems include new device discovery, software installation and removal, real-time inventory management, configuration management (including enforceable access control), data synchronization, backup and restore, application deployment, local or remote monitoring, activity logging, and virus protection.

Most organizations have already deployed enterprise and network management solutions. As such, any evaluation of a mobile computing platform should include an examination of how well this platform will integrate into existing systems, and how flexible this platform will be as the network evolves.

As a mobile platform not reliant upon any single back-end support system, the Palm OS platform offers the flexibility to fit into an existing infrastructure, and to support the infrastructure that best suits the organization's needs. Several key enterprise software partners for the Palm OS extend their security solutions and offer management solutions that easily inventory handheld devices and enforce security policy. (Please refer to the appendix for a list of administration and management solutions available for the Palm OS platform.) Featuring an extensive range of enterprise applications and network management solutions, the Palm OS platform allows businesses to deploy an effective solution that immediately addresses the current needs of the organization and that will adapt as these needs change.

The Palm OS Advantage

The security of mobile computing devices is a vital concern to any organization, particularly as wireless connectivity becomes more commonplace across the enterprise. With the world's largest installed base of handheld devices – over 20 million units – and the widest range of mobile enterprise software, the Palm OS platform provides the strength, depth, and flexibility of security solutions needed by businesses to address these concerns, without compromising ease of use.

Appendix

Note: This is not an exhaustive list of security solutions for the Palm OS but merely a small sample of the many applications available.

Synchronization and Back-Up

- BackupBuddy, from Blue Nomad **www.bluenomad.com**
- EasySync Pro, from IBM **www.lotus.com**
- Intellisync, from Puma Technologies **www.pumatech.com**
- Pocket Mirror, from Chapura **www.chapura.com**
- SyncWisePro, from Toffa **www.toffa.com**

Anti-Virus

- BackupBuddy, from Blue Nomad **www.bluenomad.com**
- F-Secure Antivirus, from F-Secure **www.f-secure.com**
- InoculateIT, from Computer Associates **www.computerassociates.com**
- Palm Scanner, from Symantec **www.symantec.com**
- VirusScan Wireless, from McAfee **www.mcafee.com**

Remote Access

- MovianVPN, from Certicom **www.certicom.com**
- SoftRemotePDA, from SafeNet **www.safenet-inc.com**

Administration and Management

- Afaria, from Xcellenet, Inc. **www.xcellenet.com**
- Asset Services Management, from Critical Devices **www.criticaldevices.com**
- Castanet, from Marimba **www.marimba.com**
- iMobile Suite, from Synchrologic **www.synchrologic.com**
- Mobile Automation 2000, from Mobile Automation **www.mobileautomation.com**
- ON Command CCM, from OnTechnology **www.on.com**
- Orbiter, from Callisto **www.calisto.com**
- Tivoli Smart Handheld Device Manager, from Tivoli **www.tivoli.com**
- Unicenter TNG, from Computer Associates **www.computerassociates.com**