

Securing Your Hand-held Devices

By Dick Mackey, Jonathan Gossels and Brad C. Johnson

dick.mackey@systemexperts.com

jon.gossels@systemexperts.com

brad.johnson@systemexperts.com

Today, many organizations recognize that laptops are every bit as capable and vulnerable as desktop computers. Security policies requiring the use of security tools and governing how laptops are used and configured are commonplace. However, some organizations still consider hand-held computers in a different light, as if the historical limitations of those devices somehow eliminate the risks associated with their larger, laptop counterparts. Over the past few years, the processing power, system software and connectivity of these small computers have increased to the point where such a distinction no longer applies.

Because of their small size and use both inside and outside the office, hand-held computers are far more likely to be stolen or simply left behind in taxis, hotels and airports. In addition, they connect to networks outside the control of their parent organization. In fact, one of the most attractive features is that these devices provide multiple communication mechanisms including dial up, Ethernet, Bluetooth, infrared, serial, and wireless. This combination increases the risk that sensitive information will be exposed in transit across these outside networks.

Hand-held PDA type devices have evolved from simple note pad/calendar replacements into vital multifaceted productivity enhancement tools. In some businesses, they have become ubiquitous. Unfortunately, few organizations are properly securing these devices. Most are not yet thinking about hand-held security.

This article provides a starting point for understanding the broad topic of hand-held security. It outlines some of the business requirements that will drive your hand-held security program and discusses what you'll need to do to address those requirements.

Understanding Hand-held Security

There are two factors that make securing hand-held devices particularly difficult. These are lack of control and convergence of functionality.

Ownership and Control

In many cases, employees have bought their own hand-held computers and integrated them into both their home and work lives. These personally owned devices exist outside the control of the organization's administration. This means that the software, configuration and connections that

these machines make to internal systems and external services may be putting the organization at risk. Most organizations have programs in place to ensure the correct configuration of laptop and desktop systems, but hand-held computers have been overlooked both as a corporate resource and a security risk.

This lack of recognition and ownership of the devices have made it difficult for organizations to impose an appropriate security policy. How

can an organization tell an employee that he can't install software on his own machine? How can an organization require an employee to buy, at his own expense, additional security products for a personal machine? How can an organization restrict how an employee uses his own device (for example, prohibiting the use of the device at Internet cafes)? How can an organization develop an effective security program for hand-held devices that encom-

passes every brand and every model (with a wide range of capabilities) in the marketplace?

The simple answer to all of these questions is to recognize that companies cannot exercise the control necessary to protect their private information and internal infrastructure on devices that they do not own. For many organizations, however, hand-helds have become an integral part of the conduct of business. For these organizations, the time for employee ownership of hand-helds has passed.

Convergence of Functionality

Three technologies have evolved as significant forces in the hand-held market—PalmOS devices that have evolved from the original Palm Pilot; Blackberries, which originated with the two-way pager device; and PocketPC, Microsoft's Windows-based answer to the Palm and other hand-held devices. All three of these have been adapted to serve the functions of what used to be multiple devices. Now, all three provide contact managers and calendar support and other advanced services like wireless networking, Web browsing, mobile phone service, word processing, and spreadsheet functionality.

As these devices accumulate functions, users will become more selective about the devices they're willing to carry. In other words, pocket real estate has become a limiting resource, and hand-held users have become discerning consumers. It's likely that *convenience* will be the driving factor in determining which hand-held devices will win the battle for the pocket.

Because of their small size and use both inside and outside the office, hand-held computers are far more likely to be stolen or simply left behind in taxis, hotels and airports.

However, the features that will be most critical will be those that allow the user to integrate transparently with his office environment both inside the office and out. These critical services will include e-mail, file sharing, printing, mobile phone, paging service, and wireless networking.

Meeting Real Business Requirements

Your hand-held security program will be most effective if it is based on genuine business requirements. In the following section, we touch on key requirements that will likely drive your hand-held security efforts, the threats that you will need to address in meeting the requirements, and mechanisms that can be used to counter those threats.

Maintaining the Confidentiality of Data on the Device

The rich application functionality of modern hand-held devices has allowed many users to leave their laptops at home and rely solely on these small devices both in and out of the office. It is now possible to read e-mail, develop and deliver presentations, enter and store contacts, and edit and store word processing documents and spreadsheets on these systems. Given these capabilities, it's no wonder these devices are often chock full of organizations' most sensitive customer data, business plans, and internal communications. Furthermore, a hand-held device's portability makes it the most convenient place to store the myriad PINs and passwords a user needs to remember and use every day for his business and personal life. In a very real way, the combination of portability and functionality makes a handheld a richer target for attackers than many desktops that never leave the safety of your organization's premises. It is clearly a requirement that organizations must protect the confidentiality of sensitive data on these systems.

Once an organization recognizes the requirement to protect the data, the challenge is to determine how. One simple but usually ineffective measure companies take is to establish a policy that sensitive data cannot be stored on these devices. This approach often encourages users to break policy or discourages users from taking advantage of these useful devices. Another approach is to use technology to reduce the risk of exposure. Unfortunately, there are issues that are unique to hand-held devices that make solving the problem slightly more complicated than solving the same problem on laptops and desktops. There are two sides of the problem—technology and user behavior. Technology is an easier problem to discuss, so let's tackle that first.

The most convenient and straightforward method for accessing the sensitive data on a hand-held device is directly through the device's user interface. So, the first line of defense should be to enable password protection. All hand-held devices support this feature. This simple measure, with an appropriately hard-to-guess password, will hamper many direct attacks. Furthermore, built-in password support can usually be configured to lock the device after multiple successive failures. Unfortunately, since hand-held devices allow data to be stored in external memory modules, password protection doesn't cover you completely. An attacker can often remove the card and read the removable memory with another device. To address this specific threat, handheld users should investigate encryption mechanisms that obscure data. This will help to protect the data in the event an attacker gained direct physical access to memory or through an external device acting as a debugger. One of the realities of dealing with encryption on today's hand-held devices is that it typically requires add-on products. The challenge is to find an encryption

product that provides needed capabilities, preserves the convenience of the device, and integrates well with your corporate environment without being too cumbersome.

We said earlier that protecting physical access was complicated by other issues, namely, user behavior. We have noted that many hand-held users are resistant to implementing common security controls on these devices. In fact, many users who would never think of disabling a password on a laptop or desktop are reluctant to accept the burden of a password on a hand-held device. It could be that users have not internalized the power these devices have and still view them as simple replacements for notepads. Whatever the reason, users must be educated regarding the importance of complying with corporate policy and maintaining the security of hand-held computers.

The solution to the user behavior problem is to implement policies and mechanisms that maintain the convenience of the device while still achieving your security goals. This may mean working with users to determine an acceptable solution and revising it over time.

Maintaining the Confidentiality of Data in Transit

One of the main reasons hand-held devices have caught on is their ability to connect to many different types of networks. They support hardwired networks, like Ethernet and serial lines, as well as wireless technologies like 802.11, Bluetooth and infrared. In addition, many hand-held devices are combination computer/mobile telephones. These devices provide even more options for connectivity of both voice and data. Given these communication capabilities, it is natural to assume that the same sensitive data that resides on the system would be communicated over the wire and over the air. After all, the devices regularly download e-mail, synchronize contacts, and download documents from corporate networks and the Web. We should also assume that due to the portability of these devices, it's likely the sensitive data will be traveling over public networks where it will be possible for outsiders to eavesdrop on transmissions. In view of sensitive data and the hostile network, it's clear that we have a requirement to protect the confidentiality of the data as it is communicated.

The solutions in this space are almost identical to those applied to laptops. Users can employ standard encrypted protocols like SSL when communicating with Web sites or use VPN products to encrypt all traffic. The problem with attempting to depend upon various encrypted application protocols is that it is likely that you'll need to use some protocol that is not available in encrypted form. When that happens, you're left unprotected. On the other hand, VPN support has its own drawbacks. You'll have to choose one that your corporate networking group will support, you'll probably have to have all traffic flow over the VPN, and you'll likely pay some performance penalty (if only because you need your traffic to flow back to your corporate network). These are the same problems faced by laptop users, but hand-held users may feel as if the solutions are overkill for such a small, portable device. Unfortunately, this same attitude is what makes securing these devices so difficult.

Protection of Internal Infrastructure

Once hand-held devices are used by an organization, a certain amount of infrastructure needs to be set up to support them. Synchronization, file sharing, software updates, virus protection, and e-mail downloads are examples of the kinds of services hand-held devices consume and corporate infrastructures provide. Some existing services (like e-mail) require very little modification to allow hand-held devices to participate in the net-

work, while others (like synchronization and software updates) can be unique to a particular hand-held platform. When an organization either deploys new services to support hand-held devices or opens existing services to new access paths, the corporate network inherits the vulnerabilities of those new devices or services. Organizations need to review new handheld services to ensure that the protocols these devices use won't be exploited to allow attackers access to sensitive data. Furthermore, organizations should be aware of the threat that physical loss of a device might represent to its internal infrastructure. If a poorly secured handheld device falls into the wrong hands, the handheld support services should be designed to limit the access an unauthorized user has to the corporate infrastructure. Typically, this is accomplished by multiple authentication steps and segregation of the systems and data supporting the hand-held devices from the rest of the infrastructure. Clearly, this type of segregation has a cost in multiple dimensions. Separate systems, additional administrative personnel, and layers of authentication all represent cost in terms of dollars and reduced convenience. The challenge is to balance the expense with the risk.

Recoverability of Information on the Device

In the same way laptops and desktops require backup and recovery services, hand-held devices do as well. In many industries, regulatory agencies require that documents and correspondence be provided on request in the event of an investigation. This means that it must be possible to extract information stored on handheld devices. In addition, the converse of this situation must be addressed as well. That is, it also is a requirement that confidential information cannot be recovered under certain circumstances. For example, when an employee leaves a company, all data must be scrubbed from the device. In addition, organizations often decide to have a device scrub all its data after multiple successive login failures.

The requirements for recovering data and ensuring that data cannot be recovered appear to be diametrically opposed but really are not. Recovering data from a handheld is relatively straightforward within certain limits. Synchronization and backup programs are commonplace in even modest hand-held support infrastructures. All files on a hand-held can be automatically copied every time the device connects to the infrastructure either by the network or through its cradle. Changes made between synchronizations would be lost if the device were destroyed.

One of the problems that organizations face when considering how to deal with data recovery is the effect that other security mechanisms may have on recoverability. For example, some authentication products can be configured to erase all memory in the device after some number of successive login failures. While this feature will help to foil an attack aimed at reading data or using the device, the feature could be used intentionally to destroy evidence or deny service. Here again, an organization must consider which requirement is more important and address its most critical risk.

Convenience and Usability

As we mentioned earlier, users often buy hand-held devices themselves and use them for both personal and business purposes. If an organization eliminates personnel use of the devices altogether, it may make the device unattractive. If the user is forced to carry multiple hand-held devices, he may choose to carry his own and leave the organization-supplied device at the office. In this case, the corporation has likely increased risk and reduced its control.

It's better to at least consider the risks of striking a balance between convenience and security. This means that individuals should be encouraged to identify software they need to use so that it may be reviewed for vulnerabilities. Users should also identify the networks, systems and services they connect to, so the company can understand the risks associated with them. It may be that the company can advise the user regarding alternatives or dissuade the user from engaging in behavior that could put the company at risk.


The simplest rule to follow is that the hardware, software and policies implemented to secure the handheld must not render the device so difficult to use as to discourage users from complying with the policies or using the devices. For example, passwords should not be required to be excessively complicated, nor should they be required to be changed too often. Another usability issue is that screen lockouts should not be so short that users are required to constantly enter passwords or so long that it defeats the purpose of having a password. The approved software for the platform should include tools that users need and not arbitrarily rule out software that users have become accustomed to using.

Manageability

One of the challenges that organizations often face with hand-held devices is incorporating a large number of unmanaged individual devices into a manageable group. It is virtually impossible for even moderately sized organizations to manage software updates, security configurations, software installations, and backups without some kind of infrastructure. Leaving the job to individuals is a sure path to chaos. One of the challenges of central management is choosing a device or set of devices to manage. It is impractical to support every different type of hand-held device. The next challenge is determining what services you'll centralize. There are a variety of choices available in commercial products, and they offer an interesting combination of synchronization services and security features. The problem is trying to coordinate local device security with centralized management tools. Unfortunately, there's no easy answer here, either. You'll need to look at the authentication and encryption provided by the management infrastructure and determine whether it conflicts with your choice of VPN, mail service and local encryption products.

Last Word

Hand-held devices have succeeded in penetrating the business world because they are small, powerful and convenient. Organizations must now treat them as first-class members of their computing environments and include them in their security plans, processes and infrastructure.

Increasingly, businesses are deploying hand-helds in production applications. As this article has shown, these devices are susceptible to a wide range of threats, and companies are recognizing the very real business risk these devices pose. At the same time, the inherent value and convenience the devices offer is well recognized. By thinking through your specific business requirements and then deploying a combination of practices and tools, it is possible to take advantage of this technology without putting your enterprise at risk. 

All three authors are employed with SystemExperts Corporation. Dick Mackey is principal, Jonathan Gossels is president, and Brad C. Johnson is vice president.