Policing the Airwaves

May 07, 2004

Time to secure those runaway mobile devices

By Peter Rysavy for Secure Enterprise Magazine (CMP Publication)

If you're already overwhelmed by the security demands of your IT infrastructure, just wait. The proliferation of wireless PDAs, smart phones and other mobile devices will soon give you many more reasons to worry.

Until recently, PDAs and mobile phones posed only a limited security threat. That's changing as the devices gain capabilities and more widespread use. Today's handheld devices boast serious computing power. Some come with a 400-MHz processor and up to 5 GB of removable storage. What's more, cellular and Wi-Fi capabilities make these devices full network nodes supporting TCP/IP communications and application protocols for e-mail, Web access and database transactions.

As network nodes, these devices can inject viruses into your network. They're also easier to misplace than laptop computers, potentially giving unauthorized users access to confidential information. Even data stored locally on these devices--contracts and calendars, for instance--can be damaging or embarrassing in the wrong hands. The potential for misuse becomes far worse if the devices are set to access data stored on your corporate servers automatically.

You can no longer pretend these devices don't exist in your enterprise. If your company isn't buying them, employees are bringing them in through the back door. Their numbers are exploding, with tens of millions expected to be sold this year. Sales are growing at an 86 percent compound rate annually, IDC says. And everyone is battling for market share: Microsoft, with its Pocket PC and Windows SmartPhone; PalmSource; Research in Motion, with its Blackberry; and Symbian, a joint venture of Nokia, Psion, Samsung, Siemens and Sony Ericsson.

The good news is that comprehensive security mechanisms and tools are available for all these platforms, though they're not always the same ones you use for other mobile platforms.

The Same but Different

Here's something that may surprise you: There are many similarities between handheld wireless platforms and notebook computers. That means many of your notebook security tactics apply equally well to handhelds.

To begin with, handhelds can access the same kinds of wireless networks, including Wi-Fi, CDMA2000 packet data and GPRS/EDGE/UMTS. They also employ IP networking and can use many of the same VPN technologies you may have running in your shop. Most have browsers that include support for SSL and TLS (Transport Layer Security). They often access the same enterprise servers, and many support the same primary enterprise applications, such as e-mail, group calendaring, instant messaging and database access.

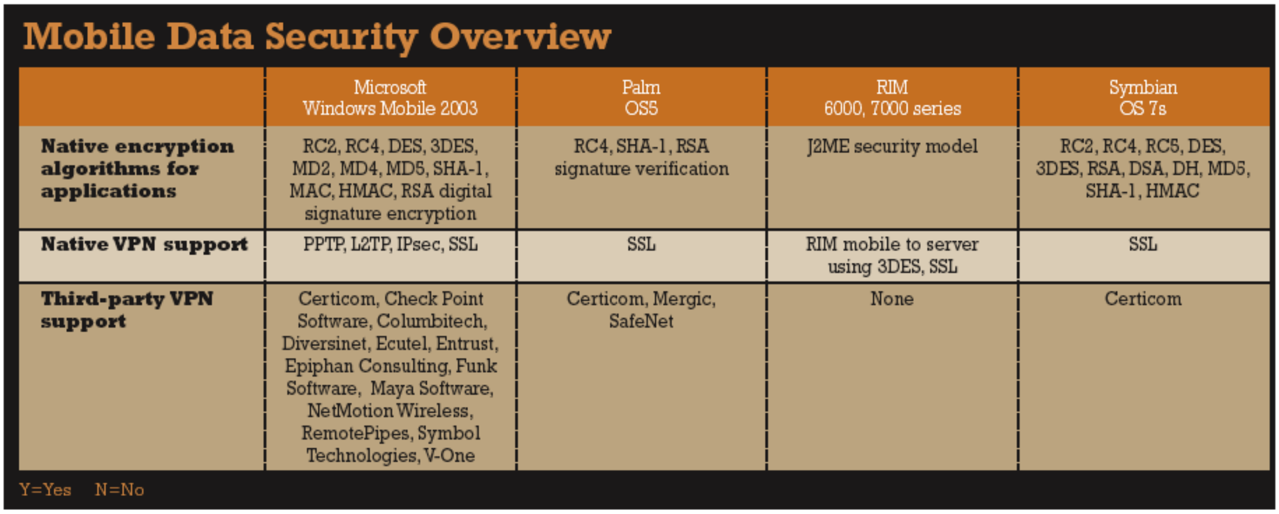
The biggest difference is in perception. Ironically, handheld devices are more dangerous in the enterprise because IT managers tend to underestimate the appliances' security risk. Raising less concern than notebooks, the devices aren't necessarily made an integral part of IT security plans and policies.

Another difference is diversity of platforms. Whereas most enterprises have standardized their desktop platforms, few have done so with PDAs or smart phones. The result is a smorgasbord of devices, each potentially connecting in a different fashion. There also are communications applications unique to these platforms, such as SMS (short message service), MMS (multimedia messaging service) and WIM (wireless instant messaging). These may be new avenues for spam in the short term and for viruses in the long run.

And the connections don't always look like client-server. Many handheld vendors and third-party software providers make mobile gateways that act as mobile proxies, fetching information for mobile devices and delivering them using wireless-optimized protocols. The centralized gateway also can perform security functions, such as encrypting communications with the mobile device.

The type of authentication you use may not be supported on your mobile devices or may require additional software, too. For example, if you have Wi-Fi access and are using a particular 802.1X EAP (Extensible Authentication Protocol) method, your chosen EAP client may not be available on all the mobile platforms under your roof.

Most wireless platforms provide an option for requiring a user to enter a password when the device is turned on. Stronger authentication is available as well. For instance, some Hewlett-Packard iPaqs, based on Microsoft's Pocket PC, have a fingerprint reader built in. SDIO (Secure Digital Input/Output) slots are a common option on many of these devices, so you can consider a secure ID card. Wireless devices that incorporate GSM phone functionality for voice and/or data use a SIM card for network authentication, so you can optionally require a four-digit SIM PIN code for network communications.



Mobile Data Security Overview

	Microsoft Windows Mobile 2003	Palm OS5	RIM 6000, 7000 series	Symbian OS 7s
Native encryption algorithms for applications	RC2, RC4, DES, 3DES, MD2, MD4, MD5, SHA-1, MAC, HMAC, RSA digital signature encryption	RC4, SHA-1, RSA signature verification	J2ME security model	RC2, RC4, RC5, DES, 3DES, RSA, DSA, DH, MD5, SHA-1, HMAC
Native VPN support	PPTP, L2TP, IPsec, SSL	SSL	RIM mobile to server using 3DES, SSL	SSL
Third-party VPN support	Certicom, Check Point Software, Columbitech, Diversinet, Ecutel, Entrust, Epiphan Consulting, Funk Software, Maya Software, NetMotion Wireless, RemotePipes, Symbol Technologies, V-One	Certicom, Mergic, SafeNet	None	Certicom

Y=Yes N=No

The next area to consider is the protection of sensitive information on the device. Microsoft and Symbian offer flexible cryptographic libraries and application APIs with support for common algorithms, including DES, 3DES, RC2, RC4 and RC5. Palm supports encryption based on RC4, but also provides a plug-in architecture that allows incorporation of other encryption algorithms, such as AES (Advanced Encryption Standard). These cryptographic APIs let applications encrypt data, whether for storage or for communications. Of course, their presence doesn't guarantee that data is encrypted. Microsoft also offers a mechanism for storing encrypted information in a relational database using SQL Server CE, which offers 128-bit encryption and password support.

RIM's primary approach for third-party app support is via its JVM (Java Virtual Machine) using J2ME MIDP 1.0. Note that J2ME is also available as an application environment on PalmOS, Symbian and Windows Mobile. JVM has safeguards against run-time application errors to prevent memory leaks and subsequent crashes, and can provide a security sandbox for apps where the JVM security manager grants privileges based on a trust level. Security options are greater with J2ME MIDP 2.0 than with MIDP 1.0. Symbian has the best Java capabilities, with MIDP 2.0 support and Personal Java as an option using IBM software. Palm is beta-testing MIDP 2.0 now.

Just as important is securing communications between the device and your enterprise. The most common approach for notebook computers is to use an IP VPN, which lets users choose any ISP for secure communications. VPNs using IPsec or SSL also work for handheld wireless devices.

In this area, Microsoft leads in terms of the number of protocols (IPSec, L2TP, PPTP and SSL) and third-party solutions its platform supports. About a dozen vendors offer VPNs, most targeted for the Pocket PC platform as opposed to Windows Smartphone. Some of these--Ecutel and NetMotion Wireless, for example--offer VPN technologies designed specifically for wireless networks, featuring optimization and mobility enhancements. Palm supports SSL and offers third-party support from three vendors. Symbian also supports SSL and offers VPN support using a Certicom client. RIM has opted for a end-to-end solution between the client software on the mobile device and a RIM server you install on the enterprise network.

The VPN approach lets you use the same security architecture for all your remote access, whether handhelds or notebooks, so long as the necessary client code is available for your chosen platform. This is a big plus. However, VPN tunnels are initiated by the mobile user, complicating mobile applications that need to "push" data from the enterprise to the device. RIM's end-to-end solution functions better in this respect, as it has been designed to support push. Note that third-party solutions from the likes of Extended Systems can also offer push mail functionality over secure channels that operate between a mobile client portion and a server installed in the enterprise.

Although threats like viruses and Trojans aren't yet a major factor for mobile platforms, this is likely to change, so depending on the applications you run on your device, you may want to consider third-party software. Major antivirus-software vendors have started offering mobile platform versions of their products. Similarly, you'll need to consider firewalls on the device, or at least at some central gateway, to protect against compromised mobile devices.

Finally, your biggest headache may simply be keeping track of all the mobile devices for which you are responsible, and maintaining their configuration and software components. Here you'll have to decide whether to use management tools designed specifically for the platform or to look for mobile extensions to your existing management systems, if available. These management systems can track the inventory of devices, distribute software, perform backup-and-restore functions and handle data synchronization. In the event of a device's loss or theft, some of these systems can send a message to the device to execute a "kill pill" that erases data. Leading systems-management vendors that support mobile applications include HP/Novadigm, Mobile Automation, Novell and Xcellenet. In the data-synchronization area, vendors include Extended Systems and Intellisync. Over time, you can expect all these vendors to extend the security options of their offerings.

Modern wireless platforms promise huge productivity gains at modest cost for enterprises. In many cases, these can replace notebook platforms for mobile workers. But start preparing yourself for a whole new world of security considerations, all of which can be managed but none of which can be ignored.