Portable Security: Safeguarding PDAs And Smartphones

Lisa Phifer

Will you be prepared to defend your enterprise when the mobile devices turn on you?

Much has changed since the first generation of handheld computers and personal information managers emerged nearly a decade ago, led by Palm Pilot back in 1996. Today's PDAs are considerably smaller, faster, better connected, and capable of running many of the same business applications found on laptops and desktops. Smartphones, once a hard-to-use novelty for technophiles, have become the hottest handheld market segment, outselling traditional PDAs this year for the first time.

And yet, some things haven't changed. Although three out of four workers use their PDAs and smartphones at least partly for business, the vast majority of these devices are still purchased by individuals. According to Gartner, fewer than 30 percent of these handhelds are officially sanctioned or administered by IT. As a result, today's PDAs and smartphones—and the business data and applications they house—remain largely unsecured.

Increased business use of more capable devices, combined with general disregard for business risk and countermeasures, have created a potent breeding ground for compromised security. When a major PDA/smartphone virus outbreak or code exploit arrives, will your company be ready to defend its data and systems from good handhelds gone bad?

Caution: Curves Ahead

To date we've been lucky. Three Palm-based viruses were released in 2000, followed by cellphone 911 denial-of-service outbreaks in Spain and Japan. Since then, new virus activity has been focused elsewhere, exploiting Win32 PC vulnerabilities in RPC, SQL, IIS and Internet Explorer. Although handhelds have long served as vectors for desktop infection—for example, by synchronizing infected email attachments—they have not themselves been the target of malware.

Until now. That quiet period ended this summer with the introduction of several new exploits aimed squarely at handhelds running Symbian OS and Pocket PC.

In June, the hacker group 29A released Cabir, a proof-of-concept worm written for Nokia Series 60 phones running Symbian OS. Cabir propagates over Bluetooth wireless, beaming itself to nearby Bluetooth-enabled phones whenever the infected phone is powered on. Fortunately, Cabir doesn't carry malicious payload—it is more nuisance than harmful. But the Cabir worm effectively illustrated that many handhelds could be easily compromised by malware spread over unprotected Bluetooth interfaces.

In July came Duts, a similar proof-of-concept worm for ARM-based Pocket PCs. Duts inserts itself into every Windows CE executable larger than 4,096 bytes on infected handhelds. Unlike Cabir, Duts is spread by an infected executable that's been copied from another source—for example, beamed between Pocket PCs. But, like Cabir, Duts is benign and can only propagate if a naïve user responds to prompts. In other words, Duts is mostly a wake-up call, intended to showcase potential consequences of risky PDA user behavior.

In August, a "cracked" version of the Symbian game Mosquitos was posted on several websites for free download. The cracked version operates as a trojan, sending a stream of text messages from an infected smartphone, racking up premium rate charges to be paid by the phone's owner. To fall victim, the user must engage in unsafe practices—in this case, that means downloading a game from an unknown source and ignoring warning messages displayed during game installation and execution.

Also in August, Bradoor became the first Windows Mobile trojan seen in the wild. Bradoor infects ARM-based Pocket PCs by inserting itself into SVCHOST.EXE to launch automatically whenever the handheld is turned on. Bradoor repeatedly sends email with the infected

Lisa Phifer is vice president of Core Competence, Inc., a network security consulting firm based in Chester Springs, PA.

High-level execs (with high-value data) are the biggest users of mobile devices

handheld's IP address to the attacker, listening on port 2989 for further instructions. Using Bradoor, an attacker can get or put handheld files, display messages on the handheld, and run commands on the handheld. A Pocket PC compromised by Bradoor therefore represents a back door with open-ended potential.

A few common themes can be seen in these new attacks:

- The exploited handhelds are among the most popular on the market today, maximizing the at-risk population.
- The platforms are largely hybrid phone-PDA devices that are relatively well-connected to wireless networks.
- These attacks leverage unsecured or under-secured network interfaces to accomplish their objectives.
- These attacks largely depend upon high-risk user behavior, ranging from discoverable Bluetooth interfaces to downloading code of unknown origin.
- Had these programs been malicious exploits rather than simply benign proofs-of-concept, they could have executed silently, wreaking havoc.

Precious Cargo On Board

Still, why worry about a handful of low-impact attacks against PDAs and smartphones?

Certainly, most IT departments have bigger fish to fry, like fighting spyware on corporate desktops and preventing compromise of mission-critical servers. During the same two-month period this summer, Netsky alone infected more than 1 million Win32 PCs. While today's handheld attacks may not present the same kind of immediate threat, the PDA and smartphone risk profile appears to be changing.

- **Business Use Is Increasing.** According to IDC, nearly all enterprise employees now own mobile phones or handheld devices. In fact, a stalled traditional PDA market has now given way to a fast-growing converged phone-PDA and smartphone market. More than 22 million smartphones capable of running enterprise applications will ship in 2004, with this figure reaching 100 million by 2008. As the installed base grows, these new handheld devices will become a much more attractive target.
- **Asset Value Is Growing.** According to Frost & Sullivan, mobile professionals and mobile sales staff now represent three-fourths of mobile data users in the U.S. The value of business data and credentials stored on these devices has grown in lock-step with their ability to run true business applications, ranging from horizontal applications like email and instant/text messaging to vertical applications like field support and sales force automation. Furthermore, high-level executives (with high-value data) are among those most likely to make extensive business use of today's well-connected smartphones.
- **More Data Is Now At Risk.** Handheld storage, once limited to a few kilobytes of RAM, is now measured in megabytes. Tiny removable compact flash (CF), secure digital input/output (SDIO) and multimedia cards (MMC) have further expanded storage capacity. Today, a handheld device or memory card that falls into the wrong hands is likely to house a significant quantity of business data, including customer lists, corporate mailboxes, schedules, company-proprietary documents and presentations. For example, in a well-publicized August 2003 incident, a Blackberry sold on eBay by a Morgan Stanley executive still held dozens of corporate email messages and attachments.
- **Compromise Is Getting Easier.** Newer PDAs and smartphones offer more attack vectors, including built-in cameras, text and multimedia messaging, Bluetooth, Wi-Fi and 3G wireless network interfaces. Faster WCDMA and EV-DO carrier networks make mobile applications more usable, but also make it easier to download ringtones, images, games and shareware of questionable origin. Smartphones that offer convenient headset-handset Bluetooth connections can fall victim to Bluesnarfing—remotely reading/writing the phone's address book, initiating calls, sending text messages, etc. Users who take advantage of new interfaces without understanding associated risks invite compromise.
- **Loss Is (Still) A Major Threat.** In a recent FusionOne poll, 43 percent of mobile users had experienced handheld damage, loss or theft. According to IDC, characteristics that make these devices inherently vulnerable include modest price and compact size. Users are thus likely to view their handhelds as easily replaceable and thus feel little incentive to guard them closely. However, despite the prevalence of loss/theft, Gartner estimates that 90 percent of mobile devices storing enterprise data lack the power-on protection and encryption to withstand casual-to-moderate efforts to access their content.
- **Stakes Are Getting Higher.** Privacy regulations like Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA and Japanese and EU Data Protection Directives now require many companies to protect private data from unauthorized access (and, in some cases, alteration). But companies scrambling to comply by safeguarding confidential data on servers, desktops and laptops often give little thought to the same data stored on PDAs and smartphones. A lost, stolen or hacked handheld that leads to breach of privacy can have significant regulatory, legal or financial consequences, no matter what kind of device stores the data, or even who owns that device.

Navigating The Road

In fact, IDC's Alex Slawsby argues, "In many enterprises the greatest security threat comes not from devices purchased and deployed by the com-

pany but from the mobile phones and handheld devices owned by enterprise employees." In the long run, bringing PDAs and smartphones under IT supervision and control is undeniably the safest path. "Centralizing device management and protection by removing the end-user variable and ensuring full compliance is one of the most significant steps that enterprises can take," wrote Slawsby in his paper, *Extending the Corporate Security Infrastructure to Mobile Devices*.

But companies that have little or no policy today regarding business use of handheld devices have quite a long way to go before achieving in-house handheld ownership, administration and enforcement. Getting from here to there will require time, financial investment and cultural change. Nonetheless, there are many incremental steps that companies can take to move in that direction.

Conduct a security assessment of existing handheld devices

Start by defining what "handheld business use" means for your company. Who uses PDAs and smartphones now, or will be likely to use them in the near future? What business applications and data are these handhelds being used with today, including contact lists, task lists, calendars, email, documents, remote access clients, and user credentials? Answering these questions will help you determine and document your business needs and at-risk resources.

Which PDAs and smartphones are your employees now using for business? Identify operating system/version, device vendor/model, and external/network interfaces so that you can get a handle on built-in security measures, known vulnerabilities and vectors that require protection. Eventually, you may specify company-standard devices, supported OSs, and required patches—the handheld equivalent of a standard desktop computing environment. For now, start by creating an inventory of personal handhelds used for business, and make sure to include PDA serial numbers and Smartphone Mobile Equipment Identity (IMEI) numbers.

Conduct a security assessment of existing handheld devices. Examine a representative sample that includes employees from several different organizations/levels/positions, and devices of each model and OS/version. By evaluating actual vulnerabilities and exposures, you can begin to develop a handheld security policy that concretely identifies the threats that must be mitigated, and the potential cost to your company should you fail to do so.

Use results to select necessary countermeasures. For example, handhelds used for business to any degree should block unauthorized access through power-on authentication. Handhelds that hold confidential business data should use some form of storage encryption. If only a few values need protection, a "password safe" may be sufficient. If sensitive documents and applications are compartmentalized, folder encryption may do the trick. If not, the cost of encrypting everything may be justified.

Further countermeasures to consider include automated backup/restore, virus scanners, intrusion detectors, handheld firewalls, secure remote access (VPN) clients, and interface-specific security (Table 1, p. 22). In short, the same "best practices" commonly applied to corporate laptops can (and should) be applied to PDAs and smartphones used for business.

Of course, PDAs and smartphones employ different CPUs and OSs—that means that they have different inherent weaknesses and limitations, and run different built-in and third-party security tools. This is where your handheld inventory comes into play. Search out known bugs for each handheld OS/version in your inventory to determine security patches/upgrades. For example, Blackberry handhelds have a denial of service (DoS) reset vulnerability fixed in RIM version 3.8; in July, Nokia released Series 60 upgrades to squelch Bluesnarfing. Like servers and desktops, handhelds can benefit from centrally-controlled patch management. But you can start by educating employees about known security holes and how/where to obtain related fixes.

Identify built-in security features provided by each device/version and interface, and document required device configurations and settings. For example, if you have no valid business use for IR or Bluetooth, teach employees to disable these interfaces—many handhelds are shipped with these enabled by default, and employees may not realize this. Or, if you want to permit safer use of Bluetooth, teach employees how to configure their PDAs and smartphones to disable discovery and require strong PIN authentication on every access. Here again, central policy configuration and enforcement is clearly more effective. But if that's not realistic for your company this year, recommending best practices can reduce risk while you work to plan, budget and deploy an IT-managed solution.

Where built-in security features provide insufficient defense, look for suitable third-party products to fill the gap. For example, most PDAs and smartphones ship with factory-installed but disabled PINs. Short numeric PINs are better than nothing after handheld loss/theft, but can be brute-forced with minimal effort. A wide variety of add-on products can be used to require long, complex

Pick a representative set of users to trial your security measures

passwords, signature or fingerprint authentication, or wipe stored data after repeated PIN-guessing.

When selecting tools, keep usability in mind. PDAs and smartphones tend to be used in brief sessions; many users find even simple PINs too much trouble to enter. Don't count on users to remember to lock their handhelds—use timeout and holster-based controls. And look for features like self-service challenge/response PIN recovery to make your security mandates usable. Remember, when users get locked out, they'll probably be in another city, country or time zone.

Create educational materials to teach employees about the adverse consequences of risky behavior and how to use their PDAs and smartphones safely. For example, instruct employees to exercise caution when downloading shareware and freeware onto handhelds. Code written for Symbian, Pocket PC and Palm OS can be digitally-signed to identify the author and prevent modification.

Once you've defined secure configurations and suitable countermeasures, test them to verify their effectiveness. Initiate a trial program where your IT department works with a representative set of users to review the educational material that you've compiled and follow instructions to install updates, reconfigure devices and add security programs, whether purchased individually or supplied by your company. Then repeat your vulnerability assessment on those safeguarded handhelds, and refine your practices until residual risk is acceptable. Consider ways to minimize IT cost and employee pain before rolling out your handheld security strategy on a broader scale.

Finally, create safe business processes for responding to handheld device loss, theft, repair and retirement. If an employee loses a smartphone used to read enterprise email, you must have the ability to quickly disable that employee's accounts for the carrier network, internal mail server and desktop synchronization. If an employee damages a PDA, he or she should know how to submit that device for repair through your IT department rather than shipping the device back to the manufacturer. Even if the PDA or smartphone belongs

TABLE 1: Third Party Handheld Security Measures

Category	Examples	URL
Device Authentication	Bluefire Mobile Firewall Plus	www.bluefiresecurity.com
	CIC Sign-On	www.cic.com
	Credant Mobile Guardian	www.credant.com
	Softava PicturePassword	www.picturepassword.com
	Utimaco Safeguard PDA	www.utimaco.com
Stored Data Encryption	Certicom movianCrypt	www.certicom.com
	Ilium Software eWallet	www.iliumsoft.com
	JP Mobile PDA Defense	www.pdadefense.com
	Pointsec for Palm/PPC/Symbian	www.pointsec.com
	Trust Digital PDA Secure	www.trustdigital.com
Anti-Virus and IDS	Airscanner Mobile AntiVirus	www.airscanner.com
	Alwil Software Avast!	www.avast.com
	F-Secure Anti-Virus for PPC	www.f-secure.com
	McAfee VirusScan PDA	www.mcafeesecurity.com
	TrendMicro PC-cillin for Wireless	www.trendmicro.com
Firewalls	Bluefire Mobile Firewall Plus	www.bluefiresecurity.com
	Check Point VPN-1 SecureClient	www.checkpoint.com
	Credant Mobile Guardian	www.credant.com
	Mobile Armor Mobile Firewall	www.mobilearmor.com
Wireless VPNs	AppGate Mobile Client	www.appgate.com
	Aventail OnDemand	www.aventail.com
	Columbitech WVPN	www.columbitech.com
	NetMotion Wireless Mobility	www.netmotionwireless.com
	V-ONE SmartPass Client	www.v-one.com

to the employee, the business data stored on it belongs to you, and you have a right to define cradle-to-grave rules to ensure that data's privacy.

Keep On Rolling

Put a handheld security policy into place now—even if compliance is voluntary at first. Then use that foundation to develop a long-term strategy that increases effectiveness by transitioning to company-owned PDAs and smartphones, providing formal IT support for those devices, centrally monitoring and enforcing handheld security, and blocking company network/desktop interaction with unauthorized handheld devices.

For help in realizing these broader objectives, look to vendors like Blackberry, Bluefire, Credant, GoodLink, Mobile Armor, Pointsec, Trust Digital and XcelleNet. You may also want to consult a wireless carrier for business-grade secure mobile application services. If you've already invested in an enterprise desktop management suite from a company like IBM or CA, consider using that suite's mobile device management capabilities.

Immediate stop-loss steps and long-term strategies like these can help your company reduce its exposure to unsafe business use of PDAs and smartphones. When these devices are not company property, it's easy to look the other way, but don't make that mistake. When crackers tire of banging on well-protected desktops and laptops, they'll refocus on lower-hanging fruit, and today's wide-open handheld devices are ripe targets. Prepare yourself for the inevitable by putting a plan in place to safeguard your workforce's PDAs and smartphones.

As IDC's Slawsby warned, "Enterprises failing to consider the security threat associated with mobile devices stand to lose far more in the way of reputation, resources and competitive advantage than it would cost to implement protective security strategies."□

Companies Mentioned In This Article

Blackberry (www.blackberry.com
Bluefire (www.bluefiresecurity.com)
Computer Associates (www.ca.com)
Credant (www.credant.com)
Good Link (www.goodlink.com)
IBM (www.ibm.com)
Mobile Armor (www.mobilearmor.com)
Nokia (www.nokia.com)
Pointsec (www.pointsec.com)
Trust Digital (www.trustdigital.com)
XcelleNet (www.afaria.com)

Put a handheld security policy into place now—even if compliance is voluntary at first