Defeating Malicious Mobiles

Lisa Phifer

The threat will only grow. Here are some ways to mitigate it.

Business use of mobile devices has surged, spurred by improvements in processing, storage and connectivity. Smart phone sales tripled in 2005, doubling again just six months later. By November 2006, 49 percent of surveyed companies reported significant use of mobile devices to transmit business-critical data. IDC expects this trend to continue through 2009, when one-quarter of the global workforce will depend on mobile devices to conduct business.

These new devices increase both business productivity and risk exposure. Yesterday's handhelds were limited to contact management and short messaging. But today's PDAs and smart phones are true mobile computers, connected with growing regularity and speed to corporate networks. Many run business applications like field service or sales force automation, while most routinely transmit business data, ranging from regulated customer records to intellectual property.

Companies that fail to recognize this paradigm shift and assert IT control over mobile devices may be in for a nasty surprise. When it comes to gaining back-door access to corporate networks, unprotected PDAs and smart phones are low-hanging fruit, ripe for the picking.

Mobile Threats

Although mobile operating systems have grown more sophisticated, factory-fresh PDAs and smart phones still lack the security staples that businesses commonly require on network-connected laptops. As a result, many workers underestimate the security risks.

- **Loss and theft**—Small devices designed for frequent brief use by on-the-go workers are extremely vulnerable to loss and theft. In a recent six-month study, Washington DC-area cabbies found 8,362 lost PDAs and phones—25 times the number of laptops found during the same study. And while most corporate laptops are password-protected, few users PIN-lock their PDAs and smart phones. Together, these factors create significant risk that a mobile device will be misused at some point during its lifetime.

- **Data disclosure**—When a mobile falls into the wrong hands, so does any data stored on that device. According to Credant Technologies, 88 percent of mobile devices carry valuable information—from patient, customer and employee records to intellectual property, financial information and passwords. Yet less than 20 percent of that data is encrypted to prevent disclosure.

  Of course, many laptop users also fail to enable file encryption. However, except for BlackBerry, mobile operating systems do not even include a content encryption option. Those who use personal mobiles for business often put their employer's data at risk.

- **Network compromise**—High-speed EV-DO and HSDPA wireless interfaces have increased the utility of PDAs and smart phones by enabling anytime/anywhere access to enterprise mail and other business services. To support voice over IP (VOIP) and fixed mobile convergence, Wi-Fi will soon grow common as well.

  Unfortunately, on a lost or stolen mobile device, these wireless interfaces are easily abused. Even where SSL or IPSec protects data in transit, mobile users tend to save passwords to avoid frequent re-entry. In short, misplaced mobiles are ready-to-use platforms for what Gartner calls "credentialed external attacks."

- **Mobile malware**—Users who would never touch a PC without firewall and virus protection often use the Internet from completely defenseless PDAs and smart phones. Mobile operating systems lack these common security measures, leaving them vulnerable to a new generation of viruses, worms and trojans.

  For example, Doomboot spreads to Symbian smart phones over MMS and Bluetooth, causing device failure on next reboot. Cardtrap not only disables its mobile host, but installs a Win32 trojan on removable memory to spread to desktops.

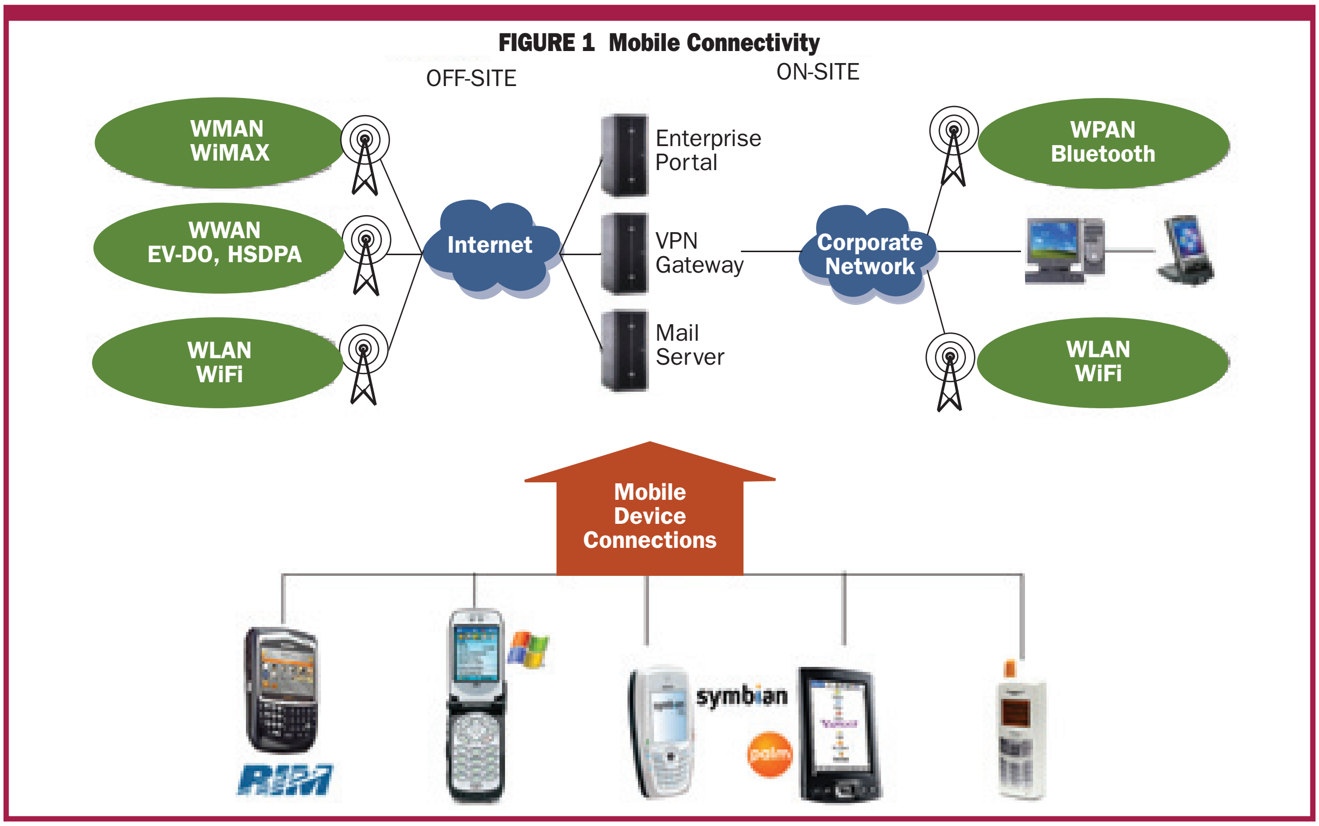
  Hundreds of programs like these have been reported since mid-2004; to date, none has caused widespread damage. However, Gartner expects more targeted mobile malware to become common by year-end 2007.

Corporate Network Exposure

Whether stolen or infected by malware, a malicious mobile can be exploited as a vector to compromise corporate network resources. Without the

Lisa Phifer is an owner and principal consultant at Core Competence, a network security technology consulting firm based in Chester Springs, PA. A 25-year veteran of the networking industry, Lisa has been involved in mobile security since 1997. She can be reached at lisa@corecom.com.

FIGURE 1 Mobile Connectivity



ability to monitor and secure these devices, companies are ill-prepared to assess their network's exposure, much less mitigate it.

PDAs and smart phones have been quietly creeping into corporate networks for years. Most have been purchased by individuals, without IT knowledge or official sanction. Smart phone retail sales are hot, and only within the past year have corporate PDA sales really grown. Thus, the average mobile device used for business is still employee-owned, unmanaged and largely unprotected against these mobile threats.

Many of these "bring your own" mobiles spend more time off-site than on; some may never enter company premises. But today's well-connected PDAs and smart phones are still capable of reaching business servers and networks from a distance, using an array of wireless technologies (Figure 1).

On the surface, these mobile connections resemble conventional laptop remote access. Indeed, it can be difficult to determine whether the client accessing an Exchange server or SharePoint portal is a laptop or a PDA. Given similar connectivity and applications, a compromised mobile exposes the corporate network to the very same threats as a compromised laptop. Such mobile devices merit the same degree of IT attention to assess and mitigate their vulnerabilities.

However, mobile device connections differ in several important ways.

- Connections tend to be far more intermittent and difficult to predict. For example, a smart phone may move from WiFi at home to EV-DO on the road to desktop cradle at the office in the space of one hour. That device's WiFi interface may rapidly alternate between internal and external access points throughout the business day.
- Mobile connections are shorter but far more frequent. Instead of reading email for an hour, twice a day, mobile users tend to receive messages in near-real-time, wherever they have coverage. Login sequences that are considered brief on a laptop may take far too long on a mobile device.
- Mobile transactions must continue in the face of limited network and processing resources. Housekeeping tasks performed in the background on a broadband-connected laptop could easily render a PDA unusable in a weak coverage area, preventing a mobile worker from doing his or her job.

These differences make it impractical to simply re-apply laptop remote access policies and measures to PDAs and smart phones. Even if you did have a complete inventory of mobile devices, and your corporate antivirus solution did run on all those devices, you would be challenged to provision, update and enforce its use.

Managing Mobile Risk

Securing PDAs and smart phones will not be easy, and it will not be accomplished overnight. However, companies can take incremental steps to evaluate and reduce their mobile risk exposure:

Detection—The first step is to find those "bring your own" mobile devices that touch your corporate network. Quantifying the number and type of mobile devices already accessing your network,

Embedding mobile malware defenses “in the cloud” may be more scalable and effective

and the interfaces used to do so, can be enlightening. Not only does this provide the foundation for security policy development—it defines your risk exposure and establishes a business case for taking additional steps.

Start by turning the threat posed by mobile network access into a platform for mobile risk management. Identify every vector used to reach business systems, from laptops and desktops to application servers and network access points. Each access vector represents an opportunity to monitor connections and spot mobile usage.

Common mobile access vectors include enterprise mail servers (reached directly or through message forwarding to an external POP account), data synchronization services (conveyed by USB cable or Bluetooth/WiFi/3G over-the-air interfaces), business application portals (accessed via Web front ends or mobile communication application gateways), and wireless LAN access points.

Logging access is one thing; spotting and correlating mobile device usage is quite another. A single PDA may have several physical identifiers (WiFi MAC, GSM SIM, handset IMEI) and use numerous dynamic IP addresses. Over time, it may log into many accounts, applying different user identities and credentials. In some cases, the only way to actually spot an unknown mobile device is to examine client hardware and software identifiers (e.g., HTTP User-Agent, unusual MAC address prefixes).

Depending upon network size and topology, detecting and “fingerprinting” mobile devices may require automation. Start by leveraging the filtering and correlation capabilities of existing network/security systems, like Wireless Intrusion Prevention System (WIPS) rogue client alerts and Network Admission Control (NAC) unknown host results. If that proves insufficient, consider using a mobile security suite (e.g., TrustDigital, Credant, Bluefire) that detects unknown mobiles whenever they try to sync with a desktop or connect to a server. Such tools can be used to simply report on mobile activities, to actively block desktop/network access, or even to automate registration and provisioning (see “Enforcement” below).

Mitigation—Mobile device inventory is both an ongoing task and a means to an end, and that end is mobile threat mitigation, accomplished through risk assessment, policy definition and security implementation.

To assess risk, start by identifying threats and business impacts associated with each discovered device type, user type and access vector. Some threats are associated with specific mobile operating systems (e.g., Symbian trojans) but risk can be reduced by upgrades (e.g., Symbian 9) and best practices (e.g., Symbian-signed program verification). Other threats are inherent to all mobile devices (e.g., loss/theft) but risk depends upon who carries the device and how they use it for business. Categorize devices into workgroups and use cases to evaluate risk exposure, establish acceptable use policies and assess the usability consequences of any potential countermeasure.

Once security needs have been established, select appropriate countermeasures. For pragmatic reasons, you may limit the mobile OSs, versions and vectors you support. However, your overall approach must allow for extension—if one thing is certain, it is the continuing evolution of mobile devices and wireless networks. C-level executives are the first to buy new smart phones, but can be very hard to deny access to.

Countermeasures can be applied to the mobile device itself, the corporate network, or the connections between them.

- Secure communication can be employed at several layers, including data link protection, network tunneling and secure application protocols. Take advantage of link security where available—for example, disable Bluetooth discovery and WiFi *ad hoc* mode to deter wireless-borne attacks. However, mobile devices that use multiple links really require a network-agnostic secure channel.

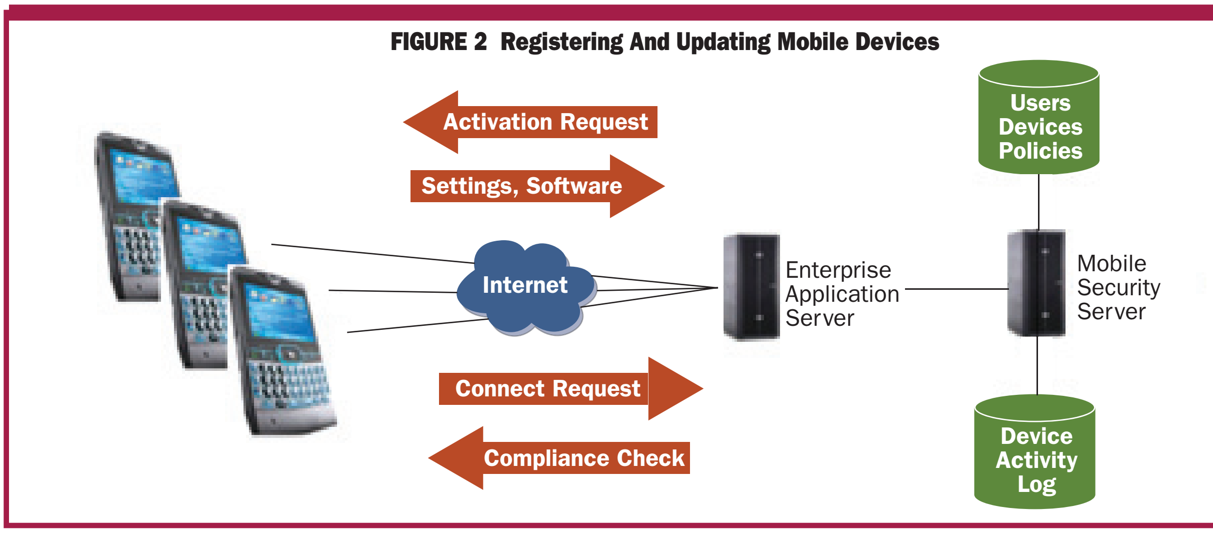
This means routing all traffic sent by a mobile device through server(s) at the corporate network edge. For example, all PDA messages might be directed through a BlackBerry Enterprise Server or a NetMotion Mobility Server, whether they originated inside or outside the network. When choosing a solution, consider mobile OSs and applications to be supported, administration costs and performance impacts. For example, conventional VPNs that require continuous connectivity and unlimited processor/battery do not fare well on mobile devices.

- Add mobile defenses to your corporate infrastructure and bake them into all new mobile servers and applications. This is a logical extension of existing best practices, whereby intrusion prevention, antivirus, anti-spyware, anti-spam and content filtering are slowly being added to firewalls, mail servers, database servers and other systems. Centralizing these services can reduce TCO, stop malware from spreading, prevent sensitive data from leaving the network and reduce dependence on endpoint security.

To extend these practices to your mobile workforce, add mobile malware detection to platforms now used for network and server antivirus/anti-spyware scanning. Scan email message content at the server, tracking data copied onto mobile devices and blocking sensitive values that would pose unacceptable risk. Filter spam to eliminate phishing messages before they can be pushed to mobile devices. Measures like these can reduce both risk exposure and the workload imposed on individual mobile devices.

- Outfit all mobile devices used for business with a minimum required set of countermeasures, specifically designed to fit mobile user needs and mobile device capabilities. For example, mandate strong access controls to deter misuse of

FIGURE 2 Registering And Updating Mobile Devices



lost/stolen devices, but choose methods that provide easy access to frequent tasks like answering phone calls. Back up and encrypt sensitive data—if not the entire device, then at least the data used by business applications. Although mobile devices are gaining features, meeting your business needs may well require after-market security software.

Gartner analyst John Pescatore recommends that enterprises start requiring their PDA vendors to provide boot-up protection, personal firewall and antivirus capabilities. Insisting on these baseline measures would make mobile devices more resistant to malware and network-borne attacks.

But Pescatore considers client-side antivirus to be a last resort. After all, desktop antivirus has proven insufficient against Win32 malware, aimed at one homogenous target. Frequent, automated patch management has become necessary to fix new vulnerabilities. Using this approach to defend a large, diverse field of mobile devices with intermittent connectivity would be even harder. Embedding mobile malware defenses "in the cloud" may be more scalable and effective.

Enforcement—Ensuring that mobile devices comply with your defined security policy can be tough—especially for devices that may never even enter the office. Fortunately, the same tools that detect new, unauthorized mobiles can also activate and enforce security policies.

Many mobile security suites provide self-enrollment, over-the-air client installation, initial policy configuration and ongoing compliance checking. For example, whenever a PDA is synchronized with an office desktop, a PC-based agent could check the PDA's identity and state. If the PDA is new, a registration dialog would be launched. Windows ActiveDirectory and Group Policy Objects could determine whether this user is permitted to activate this type of device. If approved, mobile security software would be installed onto the new PDA, along with policy-defined credentials, keys and settings. A similar process could be used to activate the PDA over wireless, on first access to a mobile messaging server.

The same mechanism can verify compliance on subsequent connect attempts, and can update software and settings in the future (Figure 2). For example, a mobile user could use this workflow to restore a PDA that has undergone hard reset, without visiting the office. Alternatively, a lost PDA could be remotely-wiped when it tried to access the corporate network, or as soon as malicious traffic from that PDA is detected.

Mobile security suites can play an important role in security enforcement at approved network entry points. However, they must be complemented with systems that block unauthorized network access elsewhere. Often, the same existing network/security systems used to detect mobile devices can help deny unwanted connections and block unauthorized protocols. For example, desktop firewalls can be configured to block email forwarding and synchronization sessions to mobile devices, inside or outside the corporate network.

Conclusion

Effectively managing mobile threats will require time and effort, from log analysis and policy development to infrastructure upgrades and mobile security software purchases. However, that investment will eventually pay dividends by reducing risk exposure and total cost of operation as the mobile workforce grows. And those who fail to put mobile device detection into place today are setting themselves up for operational, financial and regulatory impacts tomorrow.

"The [mobile malware] hype has been ahead of the threats for several years," Gartner's John Pescatore wrote in a recent presentation on wireless security. "But mobile security architectures need to be in place before the tipping point." We appear to be nearing that point—if not this year, then certainly within the three-year period that organizations typically take to move from initial threat awareness to mastery□