Securing Wireless Access To Mobile Applications

Lisa Phifer

The key is to provide security in depth and lock down all possible weak points.

Wireless devices and applications have become a significant element in today's enterprise networks. According to Gartner, two-thirds of Global 2000 companies have either launched mobile data initiatives or plan to do so by the end of 2004. These initiatives demand faster, better-connected mobile devices. By 2007, In-Stat predicts that three out of four PDAs and nine out of 10 laptops will ship with embedded wireless.

For years, mobile applications have been impeded by low-speed wireless connectivity, but Wi-Fi LANs and 3G WANs are changing that. Gartner projects that Wi-Fi client shipments will top 50 million by 2006, creating an enormous base of high-speed wireless nodes. A 2002 Jupiter Research study found that email, intranet access and instant messaging are the dominant mobile applications. But wireless-enabled applications like customer relationship management (CRM), enterprise resource planning (ERP) and sales-force automation were also present in 15–25 percent of surveyed companies.

Mobile applications improve business efficiency by making networked company assets more readily available, anytime, anywhere. Adoption has been particularly strong in education, health care, financial, manufacturing and retail markets—environments where mobility clearly increases productivity. For example, when Nabisco rolled out its wireless warehousing application, speed and quality increased 12 percent. An enterprise WLAN study commissioned by Cisco found annual productivity improvements averaging $7,000 *per user*.

However, all network extensions increase risk, and mobile applications are no exception. Before adding wireless access to your business applications, you'll want to take steps to secure mobile devices, wireless connections and all points of entry into your private network and services.

Understanding The Risks

Studies show that one in five company networks have been infiltrated by unauthorized WLANs, and three in four personal digital assistant (PDA) owners use personal devices for business. Without corporate oversight, these unmanaged devices are security accidents waiting to happen. The first step for network/security managers is to identify the threats associated with permitting mobile access to company resources.

■ **Lost or stolen mobile devices:** Laptops, PDAs and smartphones are compact and portable, increasing risk of loss and theft. A Pointsec study reported that 40 percent of mobile device users have lost phones and 25 percent have lost laptops or PDAs—often in a cab or restaurant/bar. Since loss occurs in public places, the odds are against recovery. According to Gartner, of the 350,000 laptops, 232,000 phones and 35,000 PDAs lost or stolen in the U.S. during 2001, fewer than one-third were returned to their owners.

Misplaced devices may dent your pocketbook, but theft adds insult to injury. According to Pointsec, 57 percent of employees using PDAs for business don't encrypt stored data, and one-quarter disable password protection that might otherwise deter abuse of stolen PDAs. Business risks include disclosure of proprietary data, unauthorized wireless usage costs and denial of service attacks against your mobile application servers. Passwords stored on a stolen device can also help attackers gain access to corporate email or ride an otherwise secure VPN tunnel right into the company network.

■ **Device compromise:** According to a TechRepublic study, system failure, virus infection and corruption/damage are the most frequent causes of mobile device compromise. Virus-laden websites or email can crash mobile devices and overwrite files stored on them. Games and shareware downloaded onto mobile devices can carry Trojan horses, keystroke loggers and distributed denial-of-service (DDoS) zombies. Wireless peers at hotspots can abuse open fileshares and exploit operating system (OS) vulnerabilities. Associated business risks include data loss, down time and security threats to company resources.

We often associate these risks with mobile laptops, but PDAs and smartphones are easier to compromise because they use light-weight operating systems and are less likely to run security software. For example, the Information Assurance Advisory Council (IAAC) reports that a variant of the LoveBug worm infected smartphones in

Lisa Phifer is the vice president of Core Competence, Inc., a network security consulting firm based in Chester Springs, PA. Phifer has been using wireless and VPN products for secure mobile access since the late '90s, and frequently consults and teaches about these topics

Spain, propagating itself by using the phone's address book.

■ **Attacks against data in transit:** Mobile application data carried by wireless may be vulnerable to eavesdropping, forgery, replay and man-in-the-middle attacks. Wireless traffic is easily captured by anyone within proximity of the sender. Because mobile devices are used in public places filled with strangers, ample opportunity exists for traffic analysis. Anyone can record confidential data, addresses and logins sent as cleartext. Attackers can derive passwords or encryption keys, and malicious "rogue" access points (APs) can intercept and modify traffic without the sender or receiver noticing.

According to Jupiter Research, more than half of the companies using Wi-Fi experienced security incidents during the past year, including rogue APs, clients connecting to the wrong AP, and "war driver" snooping. Loss of confidential data, forgery and replay occurred less often, but may be under-reported, since these incidents are more difficult to detect. In fact, passive eavesdropping is nearly impossible to prevent—therefore, encryption should be applied so that captured traffic is less meaningful.

■ **Attacks against networked company assets:** Permitting remote access to corporate networks, servers and applications always carries risk of unauthorized access and abuse. Without suitable authentication and access control measures, outsiders can connect to mobile application portals and gateways, retrieve confidential data, attempt to modify or destroy stored data and perform denial-of-service attacks against mission-critical resources.

These threats are certainly not unique to wireless, but wireless access opens the door somewhat wider. For example, because mobile devices are so often lost, two-factor authentication becomes more important. Because wireless traffic is so easily sniffed, source addresses cannot be relied upon for access control. Because anyone within proximity can transmit, DoS attacks against gateways and peers are more likely. Because fewer PDAs run anti-virus software, these devices may synchronize "malware" (malicious software) onto desktops or could open Trojan backdoors into your company network.

Policy-Driven Defense

Mobile application security means reducing these inherent risks to acceptable levels. Start by identifying business needs: Who needs access, when, where, to what, from what. Enumerate the business assets that are put at risk by adding wireless access, including mobile devices, confidential data, network gateways and intranet servers. Use the value of these assets and the probability of attack to determine the highest-priority threats for your business. Then identify appropriate counter-measures to neutralize those threats.

Document these conclusions in a security policy that will govern your mobile application deployment. According to Pointsec, 73 percent of companies lack formal policies for mobile device usage. Without policies, employees may be unaware of security risks or how to use mobile applications safely. Without policies, security measures may be absent or applied ineffectively.

Every mobile data initiative should define Acceptable Use Policies (AUPs) that identify permissible use, required security measures and compliance enforcement. AUPs should cover all scenarios—mobile devices using the office WLAN, residential WLANs at home and public hotspots—so everyone will understand what is and is not allowed, and the appropriate security measures can be deployed for each scenario.

Locking Down Mobile Devices

Selecting and deploying the right counter-measures can be tricky. Once your organization has identified the mobile device hardware and software platforms that must be supported, steps can be taken to secure those devices. If the endpoint isn't secure, nothing else you do really matters. Measures essential to nearly any mobile data initiative include:

■ **Device access authentication:** Your first line of defense is to deny access to lost or stolen devices. Most mobile device operating systems can be configured to require a simple login or access PIN. Many third-party products support more robust access policies, like requiring reset after password-guessing and enforcing password strength. Stronger authentication methods are also available, such as handwritten signatures or two-factor SecurID tokens. For example, Visual Key locks Win32 PCs, Palm PDAs and Pocket PCs by displaying an image; spots must be clicked in a pre-defined order to gain device access.

■ **Stored data encryption:** Should an attacker breach the device password, stored data encryption will prevent further disclosure. Password safes can be used to selectively encrypt sensitive values (e.g., passwords, account numbers)—an example of such a product is Ilium Software's eWallet for Win32, Palm and Pocket PC devices. A number of PDA programs automatically encrypt files used by sensitive applications—such programs include PDA Defense for Palm, Pocket PC, RIM Blackberry and some smartphones.

Finally, file/folder encryption is a built-in option on many laptops—for example, Win32 NTFS file systems. Of course, to prevent loss of stored data when a mobile device is misplaced or compromised, routine backups are a good idea.

■ **Anti-virus scanners:** Few companies would consider using laptops without anti-virus, but many firms leave PDAs unprotected. Don't make this mistake.

Third-party PDA products can continuously monitor the device for viruses, or scan uploaded

content only during PDA synchronization—for example, TrendMicro's PC-cillin for Wireless and McAfee's VirusScan for Handhelds. Both of these packages are available for Palm, Pocket PC and Symbian PDAs.

Also look for intrusion prevention tools that monitor mobile devices for malicious activity—for example, stopping malware that tries to delete or overwrite system files.

■ **Disabling and firewalling wireless interfaces:** Disabling unused network interfaces to avoid unnecessary risk is just good old-fashioned common sense. Turn off integrated Wi-Fi adapters and infra-red (IR) ports on laptops and PDAs when not in use. Windows laptops used at Wi-Fi hotspots may use the built-in Internet Connection Firewall and disable network file sharing to deter wireless peer attack. More robust third-party personal firewall software is widely available for Win32 laptops and even some PDAs—for example, Bluefire Mobile Firewall Plus for Pocket PCs.

Protecting Wireless Traffic

Networks used for mobile application access fall into three broad categories: wireless wide-area networks (WANs), wireless personal-area networks (PANs) and wireless local-area networks (LANs). Each has its own security properties. To understand your risks and options, start by considering built-in airlink security for the kind(s) of wireless you will use.

■ **Wireless WANs:** WANs span large outdoor distances, and are operated by carriers like AT&T and Sprint. Second generation WANs based on standards such as CDPD and GSM were limited to 19.2 kbps, but 3G WANs like GPRS and CDMA2000/1XRTT offer speeds comparable to landline dialup today (i.e., 56 kbps), with higher speed on the way. WANs are primarily used by (smart)phones, but field service terminal, tablet PC and PDA usage is growing as bandwidth increases.

WAN security helps carriers control and account for network use, encrypting on the airlink only. Once data hits the interior of the carrier's network or the Internet, you're on your own.

For example, GSM authenticates mobile stations using secret device keys to ensure that only subscribers use the carrier's network. GSM optionally encrypts everything over the air between the device and the carrier's base station. Known GSM vulnerabilities have been addressed in GPRS. The GPRS Tunneling Protocol (GTP) also can relay data from serving nodes to gateway nodes. GTP authenticates roaming partners but provides no confidentiality or integrity.

■ **Wireless PANs:** Bluetooth PANs replace cables that would otherwise tether peripherals to nearby devices (PDAs to PCs, headsets to phones). Bluetooth devices optionally authenticate using challenge-response messages based on a static device PIN. During authentication, an encryption key is derived to scramble data sent over the airlink.

However, minimum-length device PIN and encryption keys are too short to prevent cracking. Static PINs and key inputs mean that compromised values may be used for a long time. Bluetooth connections can be hijacked when one-way authentication is used, such as when a PDA authenticates itself, but the connected PC does not. Nonetheless, Bluetooth security deters casual eavesdropping.

■ **Wireless LANs:** 802.11 (Wi-Fi) LANs deliver up to 54 Mbps at indoor distances up to 300 feet. LANs typically connect wireless stations (laptops and PDAs) to access points. Wi-Fi includes two built-in security options: Shared Key Authentication and the Wired Equivalent Privacy (WEP) protocol.

When authentication is required, only stations with the shared key (group password) can connect. Stations are not individually authenticated, and if the shared key becomes known to outsiders, all bets are off. WEP uses the same key to encrypt traffic over the air. Any station that has the key can decrypt traffic. Unfortunately, serious flaws make it possible for eavesdroppers to crack the WEP key. Once the key is compromised, authentication and encryption are defeated until all stations are rekeyed.

Fortunately, a near-term fix is available. Wi-Fi Protected Access (WPA) uses the emerging 802.11i Temporal Key Integrity Protocol (TKIP) and 802.1X Port Access Control (see *BCR*, May 2003, pp. 42–46). TKIP is a WEP replacement that uses stronger dynamic keys to defeat WEP crackers and a message integrity check to detect forgery and replay. SOHO LANs can use a secret pass phrase to initialize TKIP; corporate LANs can use 802.1x port access control. 802.1x uses RADIUS with a variety of methods (certificates, passwords) to determine which stations can access the wired network on the other side of the AP.

WEP and WPA tend to be used in privately-operated LANs, where one organization has control over stations and access points. They are not often used in public Wi-Fi hotspots, because that would require station reconfiguration, and giving shared keys to strangers has little practical value. Instead, hotspot providers use secure login portals to authenticate subscribers and control network access. The portal prevents login/password sniffing, but data sent thereafter is not protected. As a result, hotspot visitors usually require additional measures for secure mobile application access.
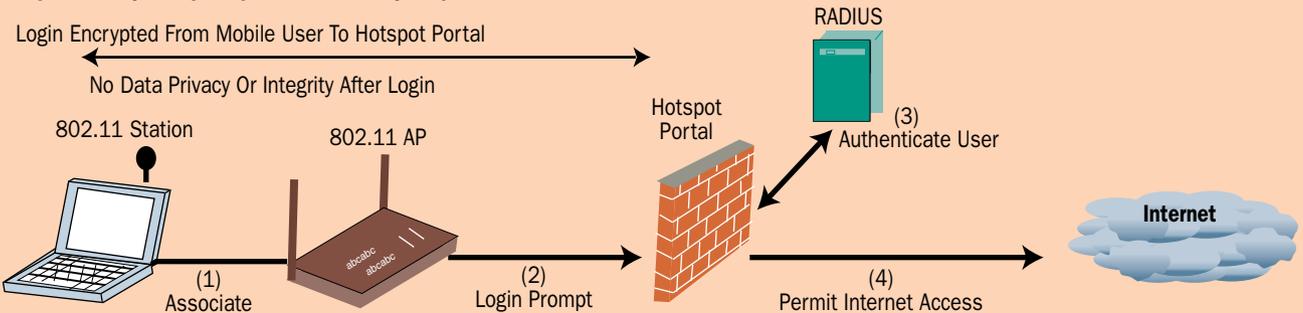
Securing Network Access

Hotspot visitors and others that access mobile applications over more than one network require end-to-end protection, no matter what the underlying link(s). As mobile users roam from one wireless LAN to another, or from wireless WAN to LAN, risk profiles really should not change.
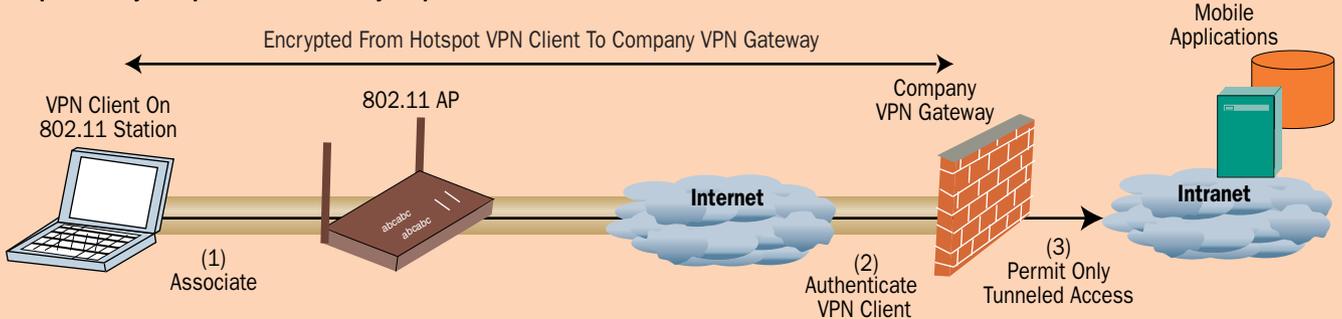
Hotspot visitors should use VPNs for security

Virtual private networks (VPNs) can provide this kind of uniform, network-independent security.

In a VPN, secure tunnels protect IP or TCP packets exchanged between clients (mobile devices) and gateways (firewalls or access concentrators) at the edge of your company's network. Unlike GPRS, Wi-Fi or Bluetooth security, Virtual private networks offer privacy and integrity over the entire path between the client and gateway. As each tunnel is established, your gateway and mobile device authenticate each other. The gateway is responsible for permitting authorized access to private networks, subnets, servers or individual applications, and of course keeping others out.

For this reason, VPNs are useful when using public hotspots (Figure 1). VPNs help hotspot visitors access mobile applications more securely. Hotspot providers employ lower-level measures like secure login authentication to meet their own business needs, and layering VPN tunnels on top will help you meet your own business needs—i.e., protecting corporate data from eavesdropping by hotspot peers, and preventing unauthorized access to mobile applications. Products that provide seamless integration between these two are emerging—for example, the iPassConnect service interface can use one login for both hotspot and VPN access, and tear down the hotspot connection if the VPN fails.

VPN alternatives that are popular with enterprise wireless implementations include IPSec, Secure Sockets Layer (SSL), and mobile VPNs:

■ **IP Security (IPSec)** is widely used for traditional (wired) remote access by teleworkers and travelers. Windows XP, 2000, Mac OS X and Pocket PC 2003 all include embedded IPSec VPN client software, but using remote access extensions may require that you install your VPN gateway vendor's client software. Third-party IPSec clients are available for other mobile devices—for example, Certicom's movianVPN (for Palm, PPC 2002, Symbian), and AdmitOne from Funk Software (for PPC 2002).

Companies that already use IPSec on traveler laptops should consider reusing these clients to secure wireless access. However, beware of IPSec limitations—notably, problems associated with sustaining secure tunnels for devices that roam between networks. If roaming is a requirement or you don't already have IPSec, give additional consideration to other VPN alternatives.

■ **Secure Sockets Layer (SSL)** has long been used to secure Web traffic. Recently, some gateways have started to use SSL for general-purpose remote access. Some provide native access to Web applications (e.g., webmail); non-Web applications must be "webified." Other products use Java applets, ActiveX controls or download-on-demand thin clients to present native application interfaces or to tunnel non-Web protocols.

Because mobile devices usually come equipped with browsers that support SSL, you won't have to install and configure additional VPN client software. This is most attractive when your mobile applications are browser-based anyway and can be displayed effectively on your mobile device (e.g., PDAs with small screens). In addition, SSL VPNs that use applets and thin clients must support your specific mobile device

operating system—for example, Aventail's Java SSL VPN agent runs on PPC 2002.

■ **Mobile VPN** products use proprietary protocols or variations on standard protocols (e.g., Wireless Transport Layer Security—WTLS—and Mobile IP) to create general-purpose secure tunnels. Unlike SSL VPNs, mobile VPN products are not tied to Web applications or browsers. Instead, they use VPN client software to provide value-added functionality for wireless networks.

Mobile VPNs are often tailored to support secure roaming between different types of networks, without application interruption—in some cases, letting sessions persist when network connectivity is lost. Mobile VPNs may also include optimizations to improve efficiency for low-speed wireless networks or small-footprint mobile devices. A few examples include NetMotion, Ecutel and Columbitech. Mobile VPNs deserve extra attention if your mobile data initiative requires end-to-end security with WAN/LAN roaming.

Securing Individual Mobile Applications

If you just need secure wireless access to a single mobile application, a VPN may be overkill. VPNs create a secure infrastructure that can support multiple applications, but you may find simpler solutions to secure a single application.

■ **Outlook Web Access:** SSL-protected HTTP sessions are a popular security solution for Web-enabled mobile applications. For example, Outlook Web Access provides a secure Web interface to Microsoft Exchange Server. Exchange Server 2003 includes low-bandwidth optimizations, compression and wireless synchronization with Microsoft Pocket PCs and smartphones.

■ **Blackberry for Microsoft Exchange and Lotus Domino:** Companies that use Research In Motion (RIM) Blackberry devices can use the Blackberry Enterprise Server as secure mail gateway between wireless users and your "vanilla" Microsoft Exchange or Lotus Domino Server. The Blackberry Server encrypts email sent to the PDA's Inbox, and decrypts outgoing messages to the mail server. The Blackberry Server and RIM PDA use a secret key for encryption and message authentication. Frequently used with secure email and short messages, this server can also support access to corporate data over SSL connections between mobile Blackberries and back-end application servers.

■ **Oracle9iAS Wireless:** Companies that need to provide mobile access to enterprise databases may consider a wireless-aware platform like Oracle9iAS Wireless. The Oracle9iLITE relational database supports encrypted, authenticated Java or Web access by Win32, Pocket PC, Palm and Symbian devices. Oracle's Mobile Application Server synchronizes data with wireless devices. Ready-made applications that run on this platform include Oracle Mobile Field Service and Oracle Mobile Field Sales.

These are just a few examples of apps with built-in security that protects wireless data end-to-end. If your application needs are fairly narrow and likely to stay that way, these can be just the ticket. Instead of adding security to your mobile applications, you can use security features tailored to your application, provisioned and monitored through application-specific interfaces.

However, general-purpose VPNs are extensible to support applications that you may add in the future. That's important because managing authorizations for multiple applications through several interfaces can be challenging. When an employee leaves or loses his mobile device, you want to lock that door quickly. A general-purpose platform that secures all your mobile applications can make this task easier.

Conclusion

One Microsoft study cited security concerns as the top barrier to wireless deployment; factors like budget trailed far behind. You can tackle this barrier head-on by assessing your risks, developing a security policy and implementing that policy with appropriate counter-measures.

Most companies implement complementary measures at multiple layers to provide security in depth. Securing wireless access to mobile applications requires protecting every link in the chain: mobile devices, wireless links, network access and targeted mobile applications. Mobile data initiatives must carefully combine these security measures to match business needs with acceptable risk. Only then can your company fully reap the benefits promised by mobile applications□

One study cited security concerns as the top barrier to wireless deployment

Companies Mentioned In This Article
Aventail (www.aventail.com)
Bluefire (www.bluefiresecurity.com)
Certicom (www.certicom.com)
Columbitech (www.columbitech.com)
Ecutel (www.ecutel.com)
Funk Software (www.funk.com)
IBM/Lotus (www.lotus.com)
Ilium Software (www.iliumsoft.com)
iPass (www.ipass.com)
McAfee (www.mcafee.com)
Microsoft (www.microsoft.com)
NetMotion (www.netmotionwireless.com)
Oracle (www.oracle.com)
Palm (www.palm.com)
PDA Defense (www.pdadefense.com)
Research In Motion (www.rim.com)
Symbian (www.symbian.com)
Trend Micro (www.trendmicro.com)
Visual Key (www.viskey.com)