

2003 "Pervasive Security Update" report. Encryption of files and disks and boot-up and network-access authentication are essential as are centralized backup and recovery strategies in the event of device loss.

Authentication, however, remains a weak link in the remote security chain. First, human nature leads some users to find ways to bypass inconvenient boot-up authentication. Second, authentication measures themselves still are primarily just IDs and passwords ("what you know") and, in fewer cases, include a second factor of security certificates and smart cards ("what you have"). Biometric devices ("who you are") still are uncommon, according to a consensus of sources in this article, and other measures—such as systems to alert of attempted access from unexpected physical locations ("where you are")—are rare. Further, the META report maintains almost all PDA operating system passwords are "completely insecure" because they are simple and not securely stored.

"For all major platforms, there are known mechanisms to circumvent user passwords. Palm and PocketPC systems both have had back doors that allow debuggers to access system files, completely bypassing the user password. Without rigorous password enforcement in combination with data encryption, device security is very low," says David Thompson, senior research analyst in META Group's Technology Research Services.

Lastly, if the endpoint device is lost, insurers need to have in place a way to shut off the access of that device to the network, assuming device authentication controls are compromised. Health insurer Lumenos, for instance, provides its sales force notebooks, and Lumenos CTO Chad Pomeroy reports the carrier's VPN can restrict network access at the device level if a notebook is lost. Also, user logon information is not cacheable.

Securing the Connection

Carriers, such as P&C insurer Country Insurance & Financial Services, whose auto-damage appraisers have been using notebook computers for more than five years in the field, contend with supporting and securing multiple remote connection methods. The primary use of the notebooks at Country Financial is for connection to the insurer's estimating partner, ADP, using the security built into the ADP estimating

program and a direct modem connection.

According to Brad Lockwood, support analyst at Country Financial, connection to ADP is made using wireless modems, built into Panasonic CF-28 Toughbooks, which access the Cingular Interactive (formerly Mobitex) network. The insurer has stayed with this direct connection method, rather than an Internet-based one, because the Cingular infrastructure is more established than wireless Internet currently is, and coverage is more important to appraisers than connection speed.

Additionally, field staff can make a direct-dial connection to the Country Financial network and also have a software-based VPN available for Internet-based connections, which ultimately will replace the current modem-based connection to ADP. Finally, the insurer augments its security technology with a policy that prohibits users from installing any additional software on their machines.

Because insurers have been providing remote access for some time, and since direct dial-in was the earliest means of access, modem-based firewalls are a key line of defense for many insurers. For Internet-based connections, establishing a VPN still remains the security method of choice, and among the various technologies—including IPsec (IP Security Protocol), SSL (Secure Sockets Layer), and Microsoft's PPTP (Point-to-Point Tunneling Protocol), IPsec VPNs currently are, by far, the most widely used among insurers.

However, as users demand access from more locations—including public hotspots—and from more devices—including kiosks and similar nonowned endpoints—the VPN equation becomes more complicated. The one drawback to IPsec VPNs, particularly in supporting mobile devices, is they require a client application running on the endpoint—meaning the user must control the endpoint—and these clients must be updated over time.

This has led to some current interest in purely Web-based versions of SSL VPNs, which rely on the SSL technology that is part of most browsers. The difference between SSL and an SSL VPN is SSL is designed to secure only the communication between the endpoint and connecting device, whereas an SSL VPN, by virtue of creating a private network, secures the environment for the applica-

TECH GUIDE: SECURITY

Accenture, Palo Alto, Calif.
650-213-2000, www.accenture.com

AdminForce Remote LLC, Philadelphia, Pa.
610-734-1900, www.adminforce.net

Aladdin Knowledge Systems, Arlington Heights, Ill.
800-562-2543, www.aladdin.com

BindView Corp., Houston, Texas
800-813-5869, www.bindview.com

Candle Corporation, El Segundo, Calif.
866-488-4246, www.candle.com

Computer Associates International, Islandia, N.Y.
631-342-6000, www.ca.com

CMS Peripherals, Costa Mesa, Calif.
714-424-5520, www.cmsperipheralsinc.com

Digital Sandbox, Reston, Va.
703-390-9770, www.dsbox.com

DynTek, Inc., Irvine, Calif.
949-798-7215, www.dynetek.com

Engedi Technologies, Inc., Fairfax, Va.
703-273-3389, www.engedi.net

Ernst & Young Security & Technology Solutions Practice, New York
212-773-3000, www.ey.com

FileNet, Costa Mesa, Calif.
800-345-3638, www.filenet.com

Financial Services Information Sharing and Analysis Center, Herndon, Va.
888-660-0134, www.fsisac.com

Global Technologies Group, Arlington, Va.
703-486-0500, www.gtgi.com

Group Technologies, Milford, Mass.
508-473-3332, www.group-technologies.com

Oblix, Cupertino, Calif.
408-861-6800, www.oblix.com

onClick Corporation, Houston, Texas
713-784-7600, www.onclickcorp.com

Ovum, Boston, Mass.
800-642-6886, www.ovum.com

RedSiren, Pittsburgh, Pa.
877-360-7602, www.redsiren.com

SmartPipes, Inc., Dublin, Ohio
614-923-5661, www.smartpipes.com

Sygate, Fremont, Calif.
510-742-2600, www.sygate.com

SysAdmin, Audit, Network, Security (SANS) Institute, Bethesda, Md.
866-570-9927, www.sans.org

Terrorism Research Center
877-635-0816, www.terrorism.com

Tumbleweed Communications, Redwood City, Calif.
650-216-2000, www.tumbleweed.com

Verizon Wireless, Alpharetta, Ga.
877-223-3337, www.verizon.com

Whale Communications, Fort Lee, N.J.
201-947-9177, www.whalecommunications.com

Worldwide Testing and Security Services, Inc., Clifton Park, N.Y.
518-371-8327, www.worldwidetest.com