[STRATEGIC SECURITY]

3G Safeguards: Incomplete, Getting Better

With more organizations using mobile broadband networks, IT managers should be very concerned about security. Safeguarding data as it travels the airwaves may be only part of a mobile security policy -- enterprises must secure their devices and the data they store -- but the airwaves are a good place to start

The good news about wireless security is that today's mobile broadband networks have some enhanced security functions built in. The latest 3G technologies, including WiMax, have robust encryption options. AT&T and T-Mobile provide High Speed Packet Access with a 128-bit Kasumi encryption algorithm. CDMA2000, offered by Sprint and Verizon, sports 128-bit Advanced Encryption Standard encryption. WiMax also uses AES.

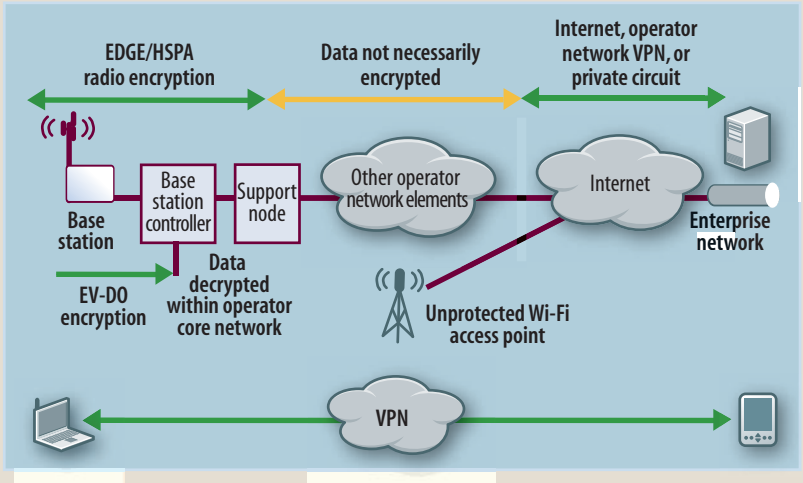
Encryption Not Guaranteed

The bad news is that there are major shortfalls with AES. One is that AES activation is largely optional on the part of operators. AT&T says its Kasumi encryption is always on, but Verizon wouldn't say whether that's the case for its encryption option. Moreover, even if your operator uses encryption, your users may roam onto a network that doesn't. And a 2G connection has much less robust encryption mechanisms than 3G, which are considered easy to defeat.

Finally, channel encryption only extends to an intermediate point within the cellular network. After that, data travels unencrypted until it reaches the far end of a connection, where most communication is again locked down.

Some operators offer network VPNs or private circuits, e.g., frame relay, for the unencrypted portion of your data's journey, so there are some options on the back end if you have a lot of data business with an operator. But these options can be complicated. Even if your radio link is reasonably secure, there's the problem of users connecting via other access networks, such as unprotected Wi-Fi hotspots. Wi-Fi capability is the norm for laptops and increasingly is available on smartphones.

Protection Varies As Data Travels



Radio encryption extends only from mobile devices to the support node within the operator network. Public Wi-Fi access points generally have no security at all. Enterprises will need to install VPNs for end-to-end wireless data protection.

End-To-End Security

One approach used by the security-conscious is to implement an end-to-end security system, either using mobile middleware or a VPN. Both of these address the airlink and protect the Internet connection.

In a white paper titled "Comparison Of Airlink Encryptions," Qualcomm states: "User data is best secured with a well tested end-to-end solution like VPN regardless of airlink encryption."

Your VPN choices are IP Security VPNs, Secure Sockets Layer VPNs, or mobile VPNs. Many companies already use IPsec or SSL VPNs for remote access, although an increasing number are turning to mobile VPNs, especially for workers who are often out of the office.

Mobile broadband networks are based on IP networking, so VPNs, even those designed for wireline networks, will work. As long as users operate de-

DIG DEEPER

Go Mobile Figuring out 3G/4G mobile broadband is worth the effort. Find out how at *informationweek.com/1185/report_global.htm*

See all our InformationWeek Reports at informationweekreports.com

vices while stationary -- i.e., not moving in a car -- existing business IPsec or SSL VPNs should work fairly well as long as signals are good. VPNs impose some tunneling overhead, but with typical throughput rates of 1 Mbps and large-bucket pricing plans, overhead isn't a big factor.

Some wireless networks issue private IP addresses unless your account provides for have a plan for public IP addresses. Private IP addresses do require IPsec to operate in what is called a Network Address Translation (NAT) traversal mode. Fortunately, NAT traversal mode is automatic for most modern IPsec VPNs.

One parameter to consider changing is keep-alive messages. These messages allow VPN concentrators to terminate sessions with clients that are no longer connected. But if a user is temporarily out of coverage (while driving through a tunnel, for example), you can achieve better connection resiliency by disabling keep-alive messages. If the VPN employs a more sophisticated keep-alive method called Dead Peer Detection, you should adjust this to the largest permissible value.

Although these changes can make VPNs more stable, it's important to understand that maintaining sessions for phantom clients results in a higher concentrator load. At 3G speeds, VPN data compression options usually are a net gain. You may not want to turn on compression for high-speed wireline broadband users -- at some point, the time necessary to decompress data is greater than the time saved by sending less of it -- so you may want to have VPN profiles for mobile users that differ from those for wireline users. Your keep-alive management can also be handled in these profiles.

Another problem you may run into is that your VPN provider may not offer clients for your particular platform. For example, Cisco doesn't have Symbian or Windows Mobile clients that interoperate with Cisco VPN concentrators. These are available from third parties such as NCP Engineering, which may also provide concentrators, enabling IT managers to enforce endpoint policy, such as checking for up-to-date antivirus protection and correct versions of software. Noncompliant devices can be directed to a specific subnet to download needed files.

Many concentrators support both SSL and IPsec. SSL VPNs have one advantage for mobile users: They can support almost any phone for browser-based applications, thus supporting more mobile platforms. SSL VPN vendors, among them SonicWall (via its Aventail acquisition), support mobile-specific Web portals that direct mobile users to appropriate resources.

Supporting nonbrowser applications with SSL VPNs typically requires additional client code, so enterprises that need to support a wide range of applications on handheld devices still have to consider platforms for which SSL VPN client code is available.

The Essentials: 3G WIRELESS VPN SECURITY: TRADE-OFFS

	Strengths	Weaknesses
IPsec VPNs	Many organizations are already using these for site-to-site and for remote access Compatible with 3G, and works well for stationary users with a good signal	Not well suited for demanding mobile environments Limited features for controlling end point
SSL VPNs	Compatible with 3G Allows support for wider range of handheld devices in clientless modes Vendors provide mobile-specific features	Like IPsec, not well suited for demanding mobile environments
Mobile VPNs	Wide range of features provided for mobile use, including security, policy management, ability to roam across different networks	Requires additional VPN infrastructure for organizations already using other VPNs, such as IPsec

Go Configure

Beyond securing connections, companies might want to control what's allowed on the corporate mobile device fleet. Configuration management systems from companies like Trellis and others make this possible. These products can control settings such as enforcement of corporate VPN restrictions, preventing network bridging (e.g., 3G to corporate LAN) and ensuring proper proxy configuration.

Mobile VPNs, designed from the ground up for mobile usage, can maintain sessions while disconnected and provide seamless roaming across network types (e.g., Wi-Fi to 3G), and can optimize data traffic. Dealing with disconnects and IP address changes are

major challenges with IPsec VPNs. Beyond connectivity, new features found in NetMotion Wireless' Mobility XE, for example, emphasize capabilities such as policy management, endpoint control, network access control, and support for two-factor authentication.

If you need to develop applications for handheld platforms, consider mobile middleware with complete development environments, letting you target multiple mobile platforms with the same application code. These systems, from Antenna Software, Dexterra, MobileAware, Sybase, and others, have comprehensive management capabilities, robust security options such as communications encryption, storage encryption, access policies, and the ability to disable lost or stolen devices.

Turnkey e-mail and synchronization products like Research In Motion's BlackBerry and Microsoft Exchange Direct Push also have similar robust security features.

All In One

Alcatel Lucent's approach to mobile security is to put security functions directly in the modem card. The card actually implements the VPN client, as well as a policy management client. And requires an Alcatel Lucent VPN concentrator. Even with the laptop off, the card stays on with a battery, and can receive software patches, which it can then install on the laptop once the laptop is turned back on. When connecting via Wi-Fi or Ethernet, packets are still processed on the card to implement the VPN function. The card also implements smart-card functions for two-factor authentication (with a password as the other factor).

The bottom line is this: Today's mobile broadband networks have some enhanced security functions built in, but most companies should take responsibility for both the security of their devices and how those devices communicate. Fortunately, a rich set of options is now available.

Peter Rysavy is the president of Rysavy Research (www.rysavy.com), a company specializing in wireless technology. Write to us at iweekletters@techweb.com.