

<b>Search</b>
<b>Issue Archives</b>
<b>Subscribe/ Change Address</b>
<b>Paid Subscriptions</b>
<b>Infosec Jobs</b>
<b>Editorial</b>
Editorial Calendar
Contact the Editors
Staff Biographies
<b>Vendor Links</b>
<b>Happenings</b>
<b>Advertising Info</b>
Rate Card
Editorial Calendar
Testimonials
Internet Opportunities
Contact a Sales Rep
BPA Statement
List Rental Info
Reprint Info
<b>Security Wire Daily</b>
<b>Wireless SWD</b>
<b>Back/Missing Issues</b>
<b>About/Contact Us</b>
Directions
<b>Privacy Statement</b>
<b>Security Wire Digest</b>
Read Current Issue
SWD Archives
Subscribe to SWD
<b>Home</b>

## FEATURES

April 2001

### AIRBORNE VIRUSES

The only thing standing in the way of a handheld virus epidemic may be limitations in the devices themselves.

BY EDMUND X. DEJESUS

Virtually every personal digital assistant (PDA) or Web-enabled cellular phone has a screen for storing its owner's personal information--the usual stuff, such as name, address, telephone number, etc. It's the kind of file that few users check after setting up. Some European users of Web phones running on the EPOC OS recently found their personal information had been replaced with four simple words, "Some fool owns this"--thanks to the BadInfo Trojan, one of a handful of malware targeted at handheld devices.

Affordable, feature-rich and easy to use, PDAs, Web phones and two-way pagers are quickly becoming indispensable mobile communications devices for businesses and consumers alike. With each successive generation, however, these handheld gadgets are taking on more and more of the functions and capabilities traditionally found on desktops and laptops.

The multifunctionality and increased 'Net accessibility of handhelds have also made them a bigger target for hackers and virus writers. Granted, there are fewer than a dozen handheld malware (see Table 1) in the wild, but this may only be a harbinger of emerging risks on the horizon. Moreover, even these few known nasties are much more dangerous than the innocuous "Hello" virus that initially infected desktops. They can wipe out settings, overwrite files and hijack applications for remote exploitation.

"The thing we all have to remember as we build these systems and technologies on open platforms is that somebody is going to eventually target them," says Robert Stout, VP for Eastern operations for F-Secure ([www.f-secure.com](http://www.f-secure.com)).

To date, handheld Trojans and viruses have been little more than an annoyance and inconvenience to users. For example, the Vapor Trojan, which targets the popular Palm OS, hides--but doesn't delete--installed applications. The Ghost Trojan infects EPOC-based Web phones, flashing insulting messages on the screen. Perhaps more damaging is the Liberty Trojan, also written for Palm OS, which deletes all applications on an infected PDA.

### Wireless Vectors

The infection vectors of wireless devices directly correlate to their connection points to the wired world.

- 1. Host PCs.** Since most users regularly synchronize their PDAs with a host desktop, the host is currently the prime conduit of infection. In most cases, a malicious code specific to handhelds lies dormant on the host, giving it a stealthy quality. It's able to float around desktops and networks undetected until it's uploaded to a handheld, where it executes its destructive payload.
- 2. Infrared transmitters.** PDAs, particularly of the Palm and Handspring variety, have the ability to convey information and files to other PDAs through infrared transmitters and receivers. It's also possible to transfer a virus this way. That means that each infected PDA has the potential to infect other PDAs with the exchange of something as benign as an electronic business card. While infrared beaming is a popular feature among users, it's not yet a common means for transmitting mobile viruses, according to Symantec ([www.symantec.com](http://www.symantec.com)), maker of the Norton antivirus line of products.
- 3. Wireless modems.** A far more common means of infection is wireless modems, which enable users to retrieve and send e-mail, surf the Web and make electronic data transfers from virtually anywhere. These over-the-air connections could also provide the means for rapidly spreading viruses to thousands of users, either overtly or covertly. The risk level of this vector is still unclear, since wireless connectivity is a relatively new feature. However, as the popularity of wireless modems catches on, AV experts expect to see a boom in malware transmitted by wireless modems--similar to the growth of infections that occurred with the advent of Internet connectivity.
- 4. Telephone.** Just as viruses can spread through information transfers via other media, they can also spread over telephone connections--especially through Web phones, which combine cellular telephone service with portable computing and Web browsers. This vector is of particular concern in Europe and Asia, where Web phones are more popular than in the United States. Already, there are six Trojans targeting the EPOC operating system, a platform developed by the Symbian consortium to provide a universal standard for Web phones. Symbian was formed by cell phone OEMs Ericsson,

Matsushita, Motorola, Nokia and Psion.

PDA vendors are actively partnering with mobile phone OEMs to produce devices that support both voice and data. Unfortunately, it's possible to transmit data--including Trojans--within the information stream. What happens on the user end depends on the device's processing architecture. If the device can automatically receive and process data, it can also automatically propagate viruses.

### Devices as Carriers

What good is a virus if it only infects one user's PDA? Sure, a virus writer can wipe out a Palm Pilot's OS or corrupt a user's calendar, but is that fun or practical for someone who has invested a lot of time and energy in writing a unique piece of malware? From a virus writer's perspective, a far better use of a wireless device is as a carrier for infecting desktops and networks. Viruses that are innocuous to handhelds, but infectious to desktops and networks, can be loaded onto PDAs and Web phones. Depending on the level of interaction--say, through wireless modems or hardware synchronization--handhelds could spread viruses faster and more covertly than current Internet-borne malware.

This scenario should seem familiar. It's virtually the same way malware was transmitted at the dawn of the virus age--via floppy disks. Industry veterans will recall how potentially dangerous "sneakernet" was to organizations, as diskettes with infected boot sectors would knock out systems as they were passed from user to user. Along the same lines, users synchronizing their handhelds with a desktop could infect the PC and its connected networks. The risk is compounded by the fact that many handheld users synchronize their PDAs with multiple PCs, usually their home and office desktops. "With floppies, there was not much effect on the corporation," says Bob Hansmann, a product technologist for AV vendor Trend Micro ([www.trendmicro.com](http://www.trendmicro.com)). "However, wireless devices can have a far greater impact, making this a corporate concern."

Further escalating the risk is carrier handhelds' ability to connect remotely to the Internet. It's possible for dormant viruses on wireless devices to spread attack tools, such as codes for causing a denial-of-service attack. On devices with telephone access, a virus could call everyone on a user's contact list, dial random long-distance phone numbers or use phone phreaking techniques to defraud telephone networks. Virus writers could even make money by having handhelds call their 900 numbers.

Doubt this could happen? Well, it already has in Japan. Hansmann says the "911" Trojan targets the popular Japanese i-mode device. Japanese users of NTT DoCoMo's i-mode got a nasty surprise last August when they participated in an online quiz on love. Answering "yes" to a certain question caused their phone to dial "110," the Japanese equivalent of 911 emergency assistance. In cities throughout Japan, police switchboards were swamped with bogus calls that prevented authorities from responding to true emergencies. At the time, NTT DoCoMo could offer no immediate remedy for the prank, but has since corrected the flaw.

Needless to say, such cross-technology attacks are difficult to track and eradicate. The symptom of the Japanese situation, for example, was a mistaken telephone call to emergency services. The natural assumption would be that something had gone wrong with the phone. Only by finding individuals affected with this, and carefully interviewing them about the circumstances, could a researcher make the connection to the online quiz. Even when such a connection is made, devising a quick solution is difficult. Pulling the plug on the offending quiz is an obvious first step, but what should be done about the phones themselves, since one of their main features is to receive, interpret and act on transmitted data? There's no easy answer.

TABLE 1: KNOWN HANDHELD MALWARE			
NAME	TYPE	PLATFORM	EFFECTS
Phage	Virus	Palm	Deletes all application, but leaves database files alone
Alarm	Trojan horse	EPOC	Continuously triggers the alarm to drain battery
Alone	Trojan horse	EPOC	Simulates an infrared data transfer (beaming) and then displays a virus warning. A black box will bounce around the screen until the user types in "Leave me alone"
BadInfo	Trojan horse	EPOC	Replaces the owner's contact information with the text "Some fool owns this"
Fake	Trojan horse	EPOC	Displays an error message that the C drive is corrupt and then simulates the formatting process to scare the user
Ghost	Trojan horse	EPOC	Flashes insulting messages on the screen
Liberty	Trojan horse	Palm	Deletes all applications

Lights	Trojan horse	EPOC	Toggles backlight on and off to drain the battery
Vapor	Trojan horse	Palm	Changes file attributes to "hidden"
911	Trojan horse	i-mode	Accesses URL that runs script to dial 911

### Multiple Platforms, Multiple Problems

The variety of handheld devices, the multiple means of infection and the broad range of consequences complicate the wireless virus problem. Given the number of different handheld operating systems--Palm OS, EPOC, Microsoft CE, etc.--devising a single solution may prove difficult. Further complicating matters are handhelds' primary users, most of whom are technically unsophisticated consumers with little or no awareness of the threats posed to their devices. Without risk awareness, users will likely not employ any protective measures--say, an AV application specific for their PDA.

Thus far, the proving ground for mobile AV technology is the Palm OS, which is the most widely used system in the United States and a favorite target of virus writers. "We have seen the threat to the Palm, and it is the most popular platform," confirms Laura Garcia-Manrique, senior product manager for Symantec AntiVirus. Developing Palm AV products makes sense from a vendor's perspective. Given the large number of users, the creation of a reliable Palm AV solution has a reasonable ROI.

More important for the overseas markets--particularly Europe and Asia--is the development of AV applications for EPOC-powered Web phones. Unlike North America, in other parts of the world Web phones are far more popular than PDAs. However, Web phones have more limited processing capacity, memory storage and battery power than PDAs. From a marketing perspective, AV developers are contending with the need to provide AV solutions against consumers' desire for Web-phone applications, including ever-popular gaming programs. Trend Micro, McAfee and F-Secure, among others, are marketing AV products specifically for EPOC Web phones.

The need for individual AV solutions for each handheld platform presents AV vendors with a number of problems. First, they need software developers with knowledge of and experience with the various handheld OSes. Such professionals are in high demand and short supply, mostly because the technology is so new. The next problem is size--a major consideration for any handheld application. Unlike a desktop OS, such as Windows, applications for handhelds are designed for their compact processing environments and limited battery power. An AV solution would have to contend with their limited memory and processing capacity. Finally, the AV application would have to run in the background without adversely affecting the handheld's performance--not an easy task given its limited processing power. Despite these challenges, several AV vendors have developed host-scanning software for the handheld platform (see Table 2).

In a way, the good news is that the virus writers must also contend with these obstacles. Some experts believe these limitations will stem the development of hand-held-targeted malware--at least in the short term. At the very least, the viruses released will probably be less sophisticated and easier to root out.

Handheld-based AV solutions work a lot like conventional desktop AV scanners. Once installed, the application scans for malware, alerts the user if anything suspicious is found and provides options for removing the malicious code. Similarly, new files downloaded onto the handheld would be scanned, and malicious executables would be stopped before they can launch their payloads.

Where handheld-based solutions differ from their PC counterparts is in their ability to scan for the wide variety of viruses. A conventional desktop AV scanner will run through a database of thousands of known virus signatures, searching for even the most obscure pieces of malware. The limited processing and memory capacity of handhelds makes the installation of a large signature database impossible. This will likely prevent these applications from identifying viruses that use PDAs as carriers for desktop and malware, or from catching more obscure scripts.

Faced with this dilemma, AV products are taking a dual approach to the handheld malware problem, augmenting a device-based application with a desktop- or network-based software that scans a handheld during each synchronization. This additional layer of malware defense makes up for the limitations of the handheld-based AV solution, helping to keep handhelds free of viruses and guarding against allowing a handheld to infect a desktop or network.

Through this layered approach, AV vendors can reasonably focus on a single handheld platform. However, they cannot be so choosy about desktop- or network-based software, which must be able to guard against any malware carried by any one of the numerous handheld OS platforms. In practice, this means that vendors must actively follow and find solutions for viruses on even those handheld platforms for which they have no on-device solution.

One school of thought holds that service providers and gateways should shoulder the burden for virus detection. Since deployment of a single vendor's AV product on all platforms and gateways isn't realistic, the probable course would be to include AV specifications within the very protocols that these systems use. Escalation of the antivirus problem to the level of standards is wise and necessary, but definitely a long-term solution. In addition, this protection only makes sense for Internet- or telephone-borne viruses. Transmission from a host machine or by beaming would remain viable

vectors, so on-device solutions would still be required.

The multi-OS problem isn't much of a concern to AV developers. As the handheld space matures, it's likely that OEMs will migrate to one or two operating systems--perhaps the Palm OS and Microsoft CE. After all, that's what happened with desktops and networks--99.9 percent of which run on Windows, Mac OS, Unix or Linux. When the field of handheld OSes narrows, vendors will have a greater ability to provide more general AV solutions.

VENDOR	PRODUCTS	PLATFORMS
<b>F-Secure</b> <a href="http://www.f-secure.com/wireless">www.f-secure.com/wireless</a>	F-Secure Anti-Virus for EPOC, F-Secure Anti-Virus for Palm OS, F-Secure Anti-Virus for WAP Gateways	Symbian EPOC, Palm, WAP Gateways
<b>McAfee</b> <a href="http://www.mcafee.com/wireless">www.mcafee.com/wireless</a>	VirusScan for Symbian/EPOC, VirusScan for Pocket PC, VirusScan for Windows CE, McAfee VirusScan Wireless	Symbian EPOC, Palm, Pocket PC, Windows CE, Windows
<b>Symantec</b> <a href="http://www.symantec.com">www.symantec.com</a>	Symantec AntiVirus for Palm (beta)	Palm
<b>Trend Micro</b> <a href="http://www.trendmicro.com">www.trendmicro.com</a>	PC-cillin for Wireless Palm, PC-cillin for Wireless EPOC, PC-cillin for Wireless Pocket PC	Symbian EPOC, Palm, Pocket PC

### Reality Check

In the movie *Field of Dreams*, Kevin Costner's character heard a voice telling him to build a baseball diamond in a cornfield--"If you build it, they will come." For admins trying to protect their systems and vendors developing new AV products, the movie's message is more of a question:

"If we make AV products for handheld and wireless devices, will consumers use them?" In the movie, baseball legends emerged from thin air to play in Costner's field. Malware experts aren't as optimistic about consumers flocking to handheld AV solutions if they build them.

User naiveté may prompt handheld OEMs to take matters into their own hands by making AV applications a part of the basic PDA or Web phone packages. Let's face it, average users will blame the manufacturer if anything goes wrong with their little magic box, even if it's of their own doing. By including an AV application as a standard feature, OEMs will mitigate risks to users, the networks they connect to and their own brand name's reputation. Such a tactic is not unprecedented. Microsoft added a simple AV application to Windows 3.1 in the early '90s when disk-borne viruses were causing major problems for PC users.

There's some indication that handheld OEMs are moving in this direction. Already a number of manufacturers are embedding Certicom's ([www.certicom.com](http://www.certicom.com)) Elliptic Curve Cryptography (ECC) algorithm for wireless security (see sidebar). While many users either don't need or don't want this feature, many OEMs are choosing to include security apps in their handhelds now, rather than trying to catch up to a rival later on. Antivirus protections could become another one of these must-have features.

### Future Shock

The few pieces of malware specifically targeted toward handheld devices may be a forecast of the virus epidemic to come. As it stands, the only thing keeping handheld viruses in check is the devices' own limitations. With only the latest generation having wireless Internet connectivity capabilities, the risk of widespread infection has been relatively remote up to now. Further, PDAs' and Web phones' limited processing power places the same limitations on virus writers that it does on application developers. However, security experts anticipate the wireless virus problem will mirror the inevitable improvements in handheld performance and connectivity.

In the not-too-distant future, enhanced handheld devices will take on more of the characteristics of their desktop and network counterparts. Word processing, spreadsheets and high-end applications will become more common on PDAs and Web phones. The advent of these capabilities will also bring the potential for macro viruses and HTML-embedded scripts--problems unheard of in today's handheld environment. Threats now faced by desktop and network administrators will become common among handheld users.

Lastly, current handheld malware poses little more than an inconvenience to users, with the most extreme designed to wipe out the memory of a PDA or drain the battery of a Web phone. However, these minor threats may serve as a blueprint for future exploits, giving virus writers a "proof of concept" to follow in the development of future malicious codes. Through these building blocks, virus writers will learn how to best manipulate these portable devices. Who knows what plague could be unleashed? Imagine wireless devices infecting each other by beaming malicious code over invisible airwaves, wreaking havoc on a scale a thousand-fold greater than the Tokyo "911" outbreak.

Is the situation really that bad today? Not really, says F-Secure's Stout. Each operating system and application will eventually draw the attention of hackers, but the discovery of a handful of Trojans doesn't necessarily reveal a clear and present danger to PDA and Web-phone users. However, he adds that the dire warnings alone could quicken the pace of handheld malware development. "I think there's enough hype, for lack of a better word, 'marketecture' on all of this stuff with wireless," Stout says. "As we do that, obviously we are going to attract some attention from the folks that cause trouble."

**EDMUND X. DEJESUS** ([dejesus@compuserve.com](mailto:dejesus@compuserve.com)) is a contributing writer for *Information Security*.

## CASE STUDY

### SECURING THIN AIR

Academia seeks better security solutions for handheld wireless devices.

BY ANNE SAITA

Dr. Agnes Hui Chan and a team of Northeastern University computer science graduate students wanted to test the soundness of wireless voice security using the popular Code-Division Multiple Access (CDMA) technology. Voice data is arranged in frames, and it took Chan's crew only 20 frames--or two seconds--to tap into the stream.

"We knew that it was weak, but we didn't know you could actually do it in real time," says Chan, associate dean of Northeastern's College of Computer Science and director of its new Wireless Security Laboratory. "We thought that it would take longer, but it didn't."

Northeastern is one of a growing number of academic institutions researching ways to improve wireless security protocols as third-generation (3G) cellular phones, wireless handheld devices and mobile commerce gain popularity in the United States. "A lot of the security breaches are not as widely known, and wireless communication--particularly for low-power devices--is still a relatively new field," Chan says.

Under scrutiny are encryption algorithms and authentication protocols currently employed to secure wireless networks and mobile devices handicapped by limited computational power. Security researchers at the University of California at Berkeley discovered a number of ways to intercept transmissions using the popular 802.11b wireless networking protocol, even when protected with a 128-bit key. But weaknesses in the Wired Equivalent Privacy (WEP) protocol under the 802.11 standard have been known since its adoption by the Institute of Electrical and Electronics Engineers (IEEE) in 1997. That's why its members have long advocated layered security--such as VPNs--for wireless networks.

While security experts preach two- and three-factor authentication, scientists and mathematicians are working on new security protocols that will improve the current wireless authentication processes without overburdening a handheld's limited abilities. As it stands, many mobile units are authenticated through a desktop computer acting as a server because handheld devices lack the necessary CPU power for processing verification requests.

"We're at the base of the evolution of this," says Shon Harris, security solutions architect for Amsterdam-based Getronics Security Consulting ([www.getronics.com](http://www.getronics.com)). "We're kind of doing baby steps."

At issue is IT managers' attitudes toward handhelds, pagers and other mobile devices. "They are viewed as [an] individual's tools and toys, instead of an extension to our beloved networks that we strive to protect," Harris wrote in a recent paper. "A majority of security policies, corporate standards and guidelines do not add Palm Pilots and cell phones under their security umbrella. This is exactly what an attacker wants; an unprotected door into [a] seemingly fortified environment."

At Oregon State University, Dr. Cetin K. Koc and a team of mathematicians and computer engineers are developing a chip that they say will offer long-term security for all types of mobile devices--regardless of size, memory capacity or computational power.

Like many security experts, Koc is concerned about manufacturers rushing new wireless devices to market without fully vetting potential security vulnerabilities. "First you make a house, then you realize you need a lock on the doors," is the way manufacturers have developed handheld and wireless devices, Koc says.

Industry figures vary, but estimates indicate there are some 25 million cell phones and 3 to 4 million other wireless devices currently in use in the United States--relatively low numbers compared to other industrial markets, notably Asia and Europe. According to analysts at the consulting firm Accenture

([www.accenture.com](http://www.accenture.com)), the low U.S. penetration of mobile devices stems from a high concentration of PCs with Internet access, a fragmented wireless carrier market, multiple cellular standards and difficulties with allocating broadcast frequencies on the electromagnetic spectrum.

But the growing use of mobile devices and the demand for greater connectivity may force changes that will resolve these problems. "This proliferation is one of the important trends that is going to effect security in the next dozen years or so," said David Black, a manager in Accenture's security division.

Europe and Asia may be hooked on wireless devices, but the nearly 30 million--and growing--deployed in the United States can hardly be ignored. Nonetheless, many corporate IT departments have yet to incorporate PDAs and Web phones into their security policies and strategies, even though these devices are now carrying a wealth of proprietary data.

"We need to build software capable of inspecting code being transferred to a device," says Pirkka Palomaki, VP of product marketing for F-Secure ([www.f-secure.com](http://www.f-secure.com)), which specializes in mobile security. Such programs must be easy to install remotely to thousands of devices or include embedded code for easy installation.

"It takes a lot of design. You can't take Windows antivirus software and just slap it on the device," he adds.

Another wireless security issue is the "gap in WAP," a problem that lies at the core of the Wireless Application Protocol (WAP), which was designed for optimal use of wireless bandwidth. WAP uses Wireless Transport Layer Security (WTLS), the wireless equivalent of Secure Sockets Layer (SSL), for privacy, data integrity and authentication. The problem is wireless data is momentarily decrypted at the wireless gateway as it's passed to the carrier server and re-encrypted in SSL. That momentary lapse of encryption is the "gap," which is most exploitable by a "man-in-the-middle" attack. It's also made some security experts question how long before WTLS and WAP migrate to TCP/IP and SSL.

"These air-gap issues are the biggest ones in wireless right now. That's your big gotcha," says Damon Herbst, technical architect at Accenture's Mobile E-Commerce Enablement Center. "People don't want to hear their data is free and clear."

Users don't want to hear their conversations and data are being intercepted, copied or deleted, either. Vendors continue to develop new encryption algorithms and security hardware that can work in handheld's power- and space-handicapped environments. "I think we need to continue research at the university- and graduate-school level," says Accenture's Black. "We need to invest in training and awareness, and we need to spawn computer scientists and engineers who are aware of the security issues and think about it earlier in the design stages.

## PORTABLE PRIVACY

The case for mobile VPNs is clear cut. But limitations in PDA bandwidth and processor capacity may slow market adoption.

BY MIKE BOBBITT

For handheld and Web-enabled phone users, the ability to access services, information and applications any time, from anywhere, is a dream come true. For security professionals, it's a nightmare.

Imagine, for whatever reason, that your organization relies on one person for support of a critical service, with no backup whatsoever. This shouldn't happen, of course, but it often does. Now, suppose that this person takes a vacation and, while he's gone, a critical system only he knows how to service goes down. Meanwhile, the boss wants it fixed...yesterday.

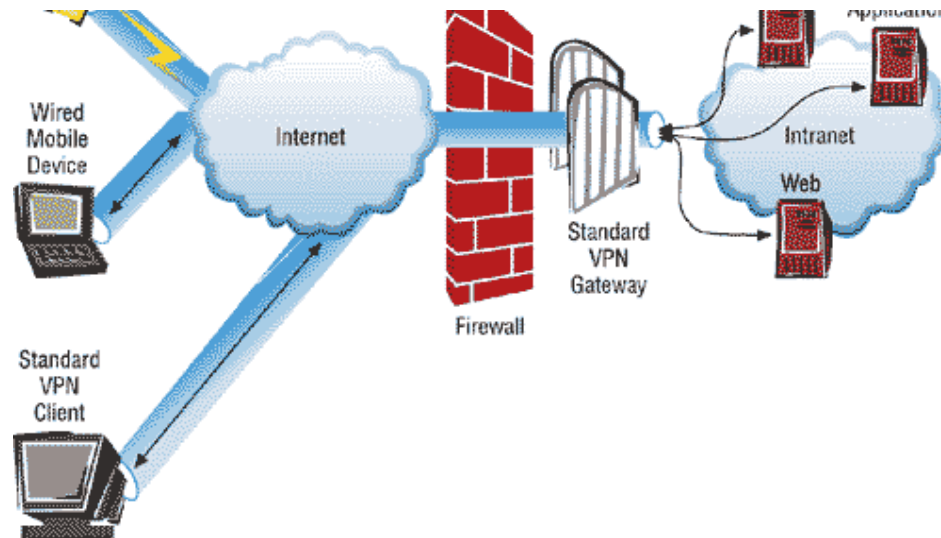
After much effort, you're able to contact your guru at some Caribbean resort, where he's soaking up sun and suds. He's confident he can correct the problem in less than 30 minutes, except for a couple of little problems--he doesn't have a laptop, a power source or a phone jack. But he does have his Palm Pilot, along with a modem and his cell phone.

At this point, your options are: (1) Resign yourself to the fact that the problem will remain unfixed until he returns; (2) Force the guru to cut his vacation short; or (3) Give your guy the root password for your critical service and allow him to fix the problem remotely. (Of course, this also means allowing your password to pass in the clear through every backwater router between St. Martin and your office.)

This scenario is certainly not beyond belief. In fact, it's simply an amalgamation of several real-life incidents, exemplifying the need for mobile VPNs--particularly for handheld devices and Web-enabled phones.



Application



### Inside the Tunnel

Mobile VPNs are elegant in their simplicity. In essence, they're a handheld-based VPN client that "snaps" into your existing VPN architecture. By using the IPSec and IKE protocols, these clients look and act just like every other VPN client your gateway communicates with (see Figure 1). This architecture was created out of necessity, since building a new VPN client system specifically for mobile devices would slow, if not prevent, its acceptance.

The one downside to this transparent integration is that specific policies cannot be applied to mobile devices. Since they can't be distinguished from standard VPN clients, there's no way to pick out a user tunneling in via his iPAQ from another user tunneling in via her desktop.

### VPNs vs. WTLS

Though vaguely similar, mobile VPNs are quite different from the well known, widely used Wireless Transport Layer Security (WTLS) protocol--the over-the-air equivalent of SSL. To date, WTLS has been used with the Wireless Application Protocol (WAP) for securing mobile transmissions, such as credit card information and e-mails.

While both VPNs and WTLS encrypt wireless transmissions, WTLS's security ends at its wireless gateway interface, where it must be decrypted and translated into TCP/IP. This creates what's often called the "gap in WAP," the point at which wireless information is vulnerable to compromise between the wireless gateway and the Web server. In contrast, a typical VPN will maintain encryption to the VPN gateway, usually situated well behind a network's firewall.

Most organizations will own and manage their own VPN gateway, but outsource their wireless gateways to an ISP. The reason is that wireless technology is far less mature than VPN technology, which makes it harder to integrate and manage. While WTLS will provide a certain degree of security, these outsourcing arrangements mean wireless transmissions are being decrypted outside the corporate network. WTLS sessions may be re-encrypted as SSL sessions before they leave the wireless gateway, but the potential for exposure still exists. With mobile VPNs, the data isn't decrypted until it hits the VPN gateway.

### Hardware Limitations

Unfortunately, mobile VPNs are anything but a simple proposition. The PDA market is still grappling with memory and processing limitations, which also limits processing-intensive crypto applications like VPNs. The biggest stumbling block is CPU power. Setting up a VPN is a CPU-intensive operation, making a VPN difficult to maintain on most mobile devices. In fact, the old standby encryption algorithms (TripleDES, CAST, etc.) are practically unusable with low-capacity PDAs, such as the Palm and Microsoft CE.

The limited bandwidth available for transmitting wireless data places another restriction on security. Most mobile devices connect at nearly intolerable speeds (somewhere around 28,800 bps), making every bit count. Introducing a VPN adds a lot of overhead to an already overtaxed connection, despite the possibility of compression with some algorithms.

The good news is that both of these problems are getting better. Mobile devices are being built with faster processors and more memory. Simultaneously, mobile networks are increasing their bandwidth capacity, allowing for larger streams of data to pass through their gateways. Some VPN vendors, such as Cisco Systems ([www.cisco.com](http://www.cisco.com)), Check Point ([www.checkpoint.com](http://www.checkpoint.com)) and Nortel ([www.nortel.com](http://www.nortel.com)), are enhancing their VPN gateways to allow the use of Elliptic Curve Cryptography (ECC), a compact,

symmetric algorithm that is compact, fast and ideal for mobile VPNs.

### Vendor Offerings

Though many vendors are promising to move into this space, only a handful currently offer practical mobile VPNs. V-One ([www.v-one.com](http://www.v-one.com)) manufactures the SmartPass mobile VPN, which supports a number of conventional platforms, including PocketPC, Windows CE and, soon, Palm OS. The SmartPass client's Dynamic Configuration feature allows the SmartGate server to push configuration information out to all VPN clients after a successful authentication.

In an attempt to reduce processing overhead and power consumption, the mobile version of SmartPass uses RC4-128 as its encryption algorithm. While more efficient than most symmetric ciphers, RC4-128 is less suited to mobile use than ECC is. SmartPass is capable of using RADIUS, RSA's SecurID ([www.rsasecurity.com](http://www.rsasecurity.com)) or FIPS-141-1 virtual token-based authentication. One problem is that, though it claims to use IPSec, SmartPass actually uses proprietary "IPSec-like" protocols designed to work exclusively with V-One's SmartGate VPN gateway.

Certicom ([www.certicom.com](http://www.certicom.com)) recently unveiled movianVPN ([www.moviansecurity.com](http://www.moviansecurity.com)) after running a long beta program. MovianVPN is available for Palm OS 3.5, with versions on the way for Windows CE 3.0 and Symbian EPOC. After installation, movianVPN is configured with many of the same conventional VPN client settings, such as user name, password, gateway and connection settings. Once configured, a user can create a tunnel in one simple step. For added security, the Palm policy database is encrypted to prevent unauthorized disclosure of sensitive settings.

Currently, movianVPN supports only user name and password authentication. Certicom is gearing up a beta program for expanded authentication mechanisms, such as RADIUS and two-factor authentication. The company also plans to add PKI support in a future release.

In an effort to adhere to the limited resources of most mobile devices, movianVPN can use ECC (which comes as no surprise, since Certicom is the developer and caretaker of ECC). While most VPN gateways aren't capable of using ECC, the major vendors are working to support this algorithm. Since Certicom isn't a VPN gateway vendor, it has attempted to remain vendor-neutral in the development of its VPN products. Included with the client are server configuration documents for many popular VPN gateways. Certicom plans to bundle its movianVPN client with third-party services and devices, allowing ISPs to sell the applications as part of their overall VPN service.

### Best Yet To Come

It's obvious that the mobile market is expanding at a fantastic rate. While some market segments may have a cloudy future, the destiny for mobile device security is fairly certain.

The obstacles facing mobile VPNs are by no means permanent. CPU power will increase, ECC and other processor-friendly algorithms will gain wider acceptance, bandwidth will increase and more vendors will jump in with new mobile VPNs products. When this happens, mobile VPNs will become as commonplace as conventional VPNs.

In the meantime, the current state of mobile VPNs makes them little more than a novelty. It's the promise of what's to come that will make this particular area a hot (and undoubtedly profitable) technology.

**MIKE BOBBITT** ([bobbitt@cipherlogic.on.ca](mailto:bobbitt@cipherlogic.on.ca)) is a technical editor for *Information Security* and a consultant for Cipher Logic Canada.

[HOME](#)