

Facing the Challenge of Wireless Security

Sandra Kay Miller

Increasingly, companies and individuals are using wireless technology for important communications they want to keep private, such as mobile e-commerce transactions, e-mail, and corporate data transmissions.

At the same time, as wireless platforms mature, grow in popularity, and store valuable information, hackers are stepping up their attacks on these new targets.

This is a particular problem because wireless devices, including smart cellular phones and personal digital assistants (PDAs) with Internet access, were not originally designed with security as a top priority. Now, however, wireless security is becoming an important area of product research and development.

As in the wired world, wireless security boils down to protecting information and preventing unauthorized system access. However, it is challenging to implement security in small-footprint devices with low processing power and small memory capacities and that use unreliable, low-bandwidth wireless networks.

Vendors and others have developed several security approaches for the various wireless technologies, although each of these early efforts has some shortcomings.

Security researchers are thus busy developing new technologies and fixing holes in existing ones.

TODAY'S WIRELESS SECURITY

The major wireless technologies have their own approaches to security.

LAN standard

The IEEE 802.11 wireless LAN standard is rapidly gaining popularity. According to Cahners In-Stat, a market



research firm, vendors sold a bit more than a million 802.11 network interface cards in 2000. As Figure 1 shows, Cahners predicts sales will increase to 2.1 million this year, 2.9 million next year, 3.05 million by 2003, and 3.9 million by 2004.

The technology's security mechanism is the wired equivalent privacy protocol. Encrypting data with WEP protects the wireless link between clients and access points. Wireless network administrators provide a WEP-algorithm-based key for each authorized user, thereby denying access to anyone without an assigned key.

WAP

The wireless application protocol lets WAP-compliant machines access and interact with other devices and resources. WAP specifies the WTLS (wireless transport layer security) protocol, which is similar to the Internet's transport layer security protocol.

WTLS provides authentication, data integrity, and privacy services within wireless technologies' limited processing power, memory capacity, and bandwidth.

WTLS generally uses RSA-based cryptography. However, the protocol can also use elliptic-curve cryptography (ECC), which provides a high level of security while demanding fewer computing and memory resources than other encryption approaches. This is an important consideration for the small-footprint handheld devices.

Authentication

A key aspect of security for activities such as mobile e-commerce and mission-critical corporate communications is the ability to authenticate a message sender's identity. There are several ways to accomplish this using variations of wireline public-key-infrastructure (PKI) mechanisms.

PKI. The mechanism provides a set of technologies that relies on encryption and digital certificates. The certificates are message attachments, issued by a certificate authority, that authenticate a sender's identity and provide encryption keys.

PKI works with public-key cryptography, in which a certificate authority uses a single algorithm to create a public and private key pair. The public key encrypts the message, and the private key decrypts it. Senders of digital certificates keep their private key secure but make the public key available to people with whom they communicate. Anyone with access to the public key can send an encrypted message, but only the certificate sender can decrypt it.

PKI is difficult to implement in the wireless world, said John Troyer, chief strategy officer and cofounder of Neomar, a software company that sells a platform for delivering enterprise applications securely to smart devices.

The challenges have been designing PKI to work on devices with low throughput and computational power and developing wireless PKI systems that can interact with their wireline counterparts. With this in mind, the WPKI (wireless PKI) protocol offers a slimmed-down version of PKI optimized for wireless communications.

There are several PKI products for wireless communications, including MobileTrust by Certicom.

Using technology from security vendors such as Certicom, eTrust, and VeriSign,

Neomar is shipping a commercial wireless browser that can store and manage PKI keys.

Troyer said organizations should leverage their existing wireline authentication infrastructure. "It's important that you don't build a new system that replicates and doesn't interact with [current] authentication systems. And on the back end, your authentication system needs to work with existing corporate directories and authorization databases."

Smart cards. Individuals can store PKI-based authentication information in smart cards that they can insert into a device-mounted reader.

For mobile communications, smart cards historically have been used as subscriber-identity-module cards in GSM (global system for mobile communication) phones and wireless identity modules in WAP phones.

Simon Blake-Wilson, Certicom's director of business development for emerging technologies, said his company is studying mobile-application-level security for smart cards.

Other approaches

Companies run Neomar's Enterprise Server (NES) behind their firewalls. A company configures its secure enterprise router proxy to permit only specified handheld devices to contact the NES, where authentication takes place. Devices communicate with the server via a dedicated connection that eliminates the need to penetrate and thereby create vulnerabilities in firewalls.

A device sends a message through an encrypted tunnel via the service provider to a recipient's NES, where decryption takes place, thereby providing security for a transmission. The process is reversed when the NES initiates a transmission.

VPNs. Virtual private networks, traditionally used in wireline communications, provide security by creating an encrypted tunnel through the public Internet. This reduces costs by eliminating the need for companies to build secure private networks. Basic wireline VPN mechanisms can be used for wireless networks, clients, and servers.

Once a handheld device's VPN client obtains an IP address by connecting to

the Internet, it can authenticate itself to a company's VPN server. The client and server then set up the encrypted tunnel through which they communicate.

Neomar's Troyer said, "The first steps have started, and we are already seeing standard VPN technology on wireless devices."

Firewalls. A WAP gateway can serve as the single point of entry for an enterprise's wireless systems. Companies can secure and monitor the gateway as they do a traditional firewall.

WIRELESS SECURITY ISSUES

Each wireless security technology has its shortcomings.

IEEE 802.11

Researchers with the Isaac (Internet security, applications, authentication, and cryptography) project at the University of California, Berkeley, say they have found security flaws in the IEEE 802.11 standard that skilled hackers could exploit. Researchers at the University of Maryland say they have found additional flaws.

Some observers argue that the flaws are no more serious than problems found in early versions of many technologies. In addition, said Stuart J. Kerry, chair of the IEEE 802.11 Working Group, the flaws are very difficult to exploit.

He said WEP was intended only to provide the same level of basic security found in wireline LANs. "WEP is not intended to be a complete security solution but . . . should be supplemented with additional security mechanisms."

Given its goals, Kerry said, "WEP has been and continues to be a very effective deterrent against the vast majority of attackers."

Cryptography. Isaac member and UC, Berkeley, doctoral student Nikita Borisov said researchers found problems with the way WEP uses cryptographic primitives. Also, he added, the Working Group made a poor choice of checksum for WEP to use to verify that a message has arrived intact.

Hackers could exploit the flaws to intercept and decrypt communications passing through the wireless link, he explained. They could even develop and

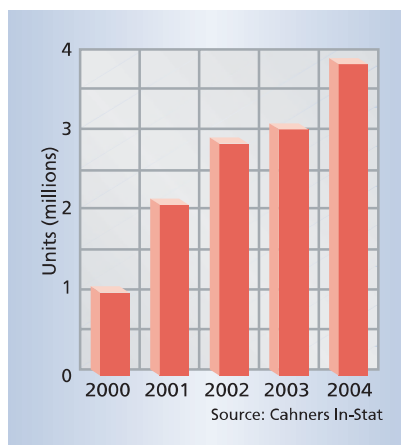


Figure 1. Market research firm Cahners In-Stat predicts sales of IEEE 802.11 network interface cards will rise steadily during the next few years.

distribute tools for this purpose, thereby helping less-skilled attackers.

Isaac researcher Ian Goldberg said the IEEE 802.11 Working Group could have avoided these problems by consulting more actively with the cryptographic community.

Kerry responded, "The development of WEP as an integral part of the IEEE 802.11 standard was accomplished through a completely open process. Participation is open to all interested parties."

Authentication. William Arbaugh, assistant professor of computer science at the University of Maryland, said IEEE 802.11's shared-key authentication service has important weaknesses.

With this service, authorized devices and servers share a secret encryption key. Participating devices and servers authenticate one another by using their keys to decode a decrypted challenge message and determine whether they got the same, correct result.

Researchers claim hackers could exploit the weakness to authenticate themselves to a server and then discover the media-access-control addresses used on wireless LAN cards. They say hackers could program the MAC address on their own devices, which could then access the network.

John Drewry, 3Com's senior director of business development, said the shared-authentication problem isn't significant

because most vendors don't use the approach, which is complex and doesn't offer the level of security it was supposed to provide.

In addition, he said, most wireless LAN cards don't let users change MAC addresses.

Other problems. Steve Bellovin, a security expert and researcher at AT&T Labs, said the security breaches discovered by the two universities are "minor" because it would take a fairly sophisticated intruder to exploit them.

He said IEEE 802.11's main problem is its cryptography standard. For example, Bellovin said, the standard was designed so that all users in an organization share the same cryptographic key. An intruder who accesses the key could compromise all users' security. The solution, Bellovin said, is to use multiple keys, as well as key-management protocols, although this is complicated and can slow a system down.

Stronger security. To make WEP more secure, Kerry said, the IEEE 802.11 Working Group is developing extensions to the protocol.

The enhanced security mechanisms would provide more sophisticated authentication, key management, and encryption capabilities.

"The enhancements," he explained, "are intended to counter extremely sophisticated attacks."

The Working Group says it eventually wants to implement the US government's newly adopted AES (advanced encryption standard) in WEP. Until that occurs, the IEEE is working on WEP 2, which would standardize 128-bit, rather than the original 40-bit, encryption on the protocol.

WAP phones

Many e-commerce and corporate sites use SSL-based security. Therefore, a transmission to such a site from a WAP phone must first pass through a gateway that converts the encryption formatting from WTLS to SSL. During the conversion process, however, the message is very briefly unencrypted and thus is subject to interception.

Some security experts say this represents a serious security problem, but others say that intercepting a message that

is unencrypted for such a short period of time within a gateway is very difficult.

WHAT THE FUTURE HOLDS

Until recently, few vendors sold complete wireless-security packages. Users had to piece together various technologies to get the security they wanted, creating additional work and cost. Now, however, companies such as Cisco Systems and 3Com are starting to fill the demand for end-to-end wireless-security systems.

One of wireless security's key challenges is adapting wireline technologies to the constrained mobile environment.

Meanwhile, the impending release of third-generation wireless-network technology, which would standardize TCP/IP on mobile systems, promises to permit strong, end-to-end SSL security, which functions only over IP networks. Currently, many wireless networks don't use IP.

Standards

Several new wireless-security standards are under development.

PIC. The Internet Engineering Task Force's IP Security Remote Access Working Group is studying a proposed Pre-IKE Credential standard (<http://www.ietf.org/html/charters/ipsra-charter.html>). (IKE is the IETF's Internet key exchange protocol, which provides additional features, flexibility, and ease of configuration to the IPsec [IP security] standard.)

A PIC-based system's authentication server would authenticate devices that are authorized to communicate with the system. The server would provide credentials to these devices, which could then authenticate themselves via IKE to a system's secure IPsec gateway.

OMAP. Texas Instruments has developed the open multimedia applications protocol, a library of software from various vendors that will permit secure transactions on wireless devices that use TI's digital signal processors. Vendors

such as Ericsson, Nokia, and Sony plan to use OMAP (<http://www.ti.com/sc/docs/apps/omap/overview.htm>) in their next-generation smart phones.

OMAP software would enable such services as memory and firewall protection, public- and private-key encryption, virus screening, and fingerprint-based biometric security.

MeT. Leading mobile phone makers Ericsson, Motorola, Nokia, and Siemens formed the MeT (Mobile electronic Transactions; <http://www.mobiletransaction.org/>) alliance to develop standards for secure mobile activities.

According to proponents, the initiative will enhance interoperability among wireless products and technologies, thereby facilitating access to mobile Internet services, including mobile e-commerce. They say MeT will be based on existing specifications and standards.

Biometrics

Biometrics uses a person's unique physical characteristics—such as fingerprints, voice patterns, facial geometry, or retinal images—to identify authorized users. Some analysts say biometrics technology could be accurate and inexpensive enough for vendors to use in smart phones and PDAs by 2004.

Wireless security faces a number of hurdles, especially the challenge of adapting wireline technologies to work with the mobile world's more constrained resources.

Such efforts are relatively new and thus not fully developed. However, vendors and users alike hope that security will keep pace as other aspects of wireless technology continue to advance. ★

Sandra Kay Miller is a freelance technology writer based in Newburg, Pennsylvania. Contact her at sandra@pa.net.

Editor: Lee Garber, Computer, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org