Certificates Strengthen Network Security

Infrastructure effort provides users, applications with digital identification passes.

By Henry S. Kenyon

The goal of the U.S. Department of Defense Public Key Infrastructure (DOD PKI) program is to develop and issue electronic certificates, or identity cards, to users and applications. These certificates protect wireless devices such as this tactical radio from being illegitimately used to access secure communications and data networks.

Every year, scores of wireless communications products enter the commercial marketplace, but ensuring their security in U.S. government applications remains a major cause for concern for federal authorities. Through the Defense Information Systems Agency and the National Security Agency, the government is creating an architecture as resistant to hacking and other cybercrime as it is secure and efficient for approved users to navigate. A key part of this effort is an accreditation regime that tests and approves all new technologies set to enter civilian government and military programs.

Wireless applications extend information technology into the ether, freeing it from its landlines and fixed infrastructure. But this new environment also opens another window, leaving computer networks vulnerable to attack. As federal and military systems become increasingly mobile, it is necessary to provide adequate protection through the use of cryptography and access codes.

The effort to develop a secure architecture for landline and wireless systems is known as the U.S. Department of Defense Public Key Infrastructure (DOD PKI) initiative. The goal of the program is to provide interoperable electronic identity credentials for authentication, encryption and digital signatures throughout the department, says Trish Janssen, DOD PKI deputy program manager. She adds that these credentials are generated using commercially available systems supporting multiple applications and vendor-neutral products.

The National Security Agency (NSA) and the Defense Information Systems Agency (DISA) manage the program, with primary oversight directed by the NSA. Janssen notes that as the deputy program manager, DISA is responsible for the engineering, implementation, operation and support of the DOD PKI infrastructure. The individual services and agencies are then responsible for user registration and the PKI enabling of applications and Web sites.

Although the program does not directly accredit commercial products and applications, DISA's Joint Interoperability Test Command (JITC) at Fort Huachuca, Arizona, and several other services, such as the U.S. Army's Technology Integration Center (TIC), also at Fort Huachuca, have test facilities to evaluate commercial products for interoperability with DOD PKI. All new systems being considered for use by the government or Defense Department must be approved by the National Institute of Standards and Technology (NIST) before moving on to pass a rigorous series of tests at these facilities to achieve certification.

According to the DOD PKI program management office, the initiative is a critical part of the Defense Department's information assurance capabilities. In addition to achieving security for the defense information infrastructure, public key certificates allow users and applications to authenticate communications or network transactions confidentially and to verify data integrity and nonrepudiation of these exchanges. Janssen notes that the program has issued credentials to more than 3.5 million users and that future development and enhancements are currently under consideration.

Electronic certificates also can be issued by select non-Defense Department organizations. Known as external certification authorities (ECAs), they provide non-Defense Department personnel with certificate services that interoperate with the DOD PKI. These applications allow contractors, vendors and other personnel to use certificates issued by an accredited ECA to conduct electronic business with department organizations.

The JITC is responsible for performing standards compliance testing on ECA-issued certificates; for providing other services, such as maintaining certificate revocation lists, online certificate status protocol requests and response formats; and for conducting interoperability testing on ECA-issued certificates.

Like all commercial wireless products offered for government use, 3e Technologies International's AirGuard family of wireless products must meet a variety of government standards for security, durability and compatibility with the DOD PKI architecture.

One example of the systems being approved through JITC is the AirGuard series of products. Manufactured by 3e Technologies International, Rockville, Maryland, AirGuard consists of rugged, secure, military-qualified and government-tested wireless access points, explains Marty Gilroy, 3e Technologies' director of marketing.

In addition to access points, which include wireless bridges and repeaters, the company develops security server software and client devices such as laptop cards and laptop cryptographic drivers. Gilroy notes that AirGuard represents a bundled package of different products that users can select and modify.

A major driver behind the intensive wireless testing is a government mandate stating that government agencies or organizations cannot purchase or install wireless applications or infrastructure unless it has been NIST tested and approved. This testing examines a product's functionality, durability, resistance to hacking, and supporting documentation and software. Based on his own firm's experience, Gilroy observes that once a product is approved by NIST, other branches of the government, such as the Defense Department, request additional testing for specific applications or use.

For example, during the testing process, JITC examined AirGuard for compliance with the DOD PKI compatibility standards. It was then evaluated by the TIC. "We tested our products down there for use throughout the Army. Those are three different labs within the federal space that we've been exposed to," Gilroy says.

The U.S. Navy and the Army National Guard both use 3e Technologies' products. The company, which was founded in 1996, currently is competing for contracts for the U.S. Air Force. Gilroy notes that the Navy is 3e Technologies' traditional customer. The firm has installed wireless local area networks (LANs) in a number of destroyers, minesweepers and high-speed vessels. But to install its equipment on these ships, it must have NIST approval, he explains.

Because of the strict requirements governing the qualification of new applications, Gilroy believes that there is a large pent-up demand for wireless systems in the government. He notes that some of this delay began two years ago when scientists at AT&T laboratories cracked a commonly used wireless algorithm called the wired-equivalent protocol. The sudden vulnerability of the protocol combined with the additional security demands of the war on terrorism forced the government to issue a moratorium on any new wireless systems unless they were NIST-approved.

To meet the requirements of its Navy customer, the company submitted its products to NIST for federal information processing standards (FIPS) certification. Gilroy contends that his firm had the first wireless access points that were FIPS 140-2 level-two certified. He adds that the lower the level number, the more secure the product. Based on a seven-layer model, AirGuard systems can operate at level two. By comparison, virtual private networks operate at level three, he explains. Additional security is provided via 256-bit advanced encryption standard encryption with user options to add dynamic user keys and DOD PKI security certificates.

Gilroy explains that the company's products operate at the media access control level, which is in the radio hard-

ware itself. "There is nothing between us and what goes out over the air. No software can get between you and the transmission to muck it up," he says.

To protect against electronic eavesdropping on wireless LANs, AirGuard systems have a feature called variable radio frequency that lowers a network's power output to nearly zero. This capability is important for certain platforms such as minesweepers, which must shut off all radio emissions while sweeping for mines to avoid attracting and detonating the munitions. The equipment also features high levels of transmission security. "Even if someone were able to grab the signal over the air, it's so heavily encrypted and coded that they [the eavesdroppers] wouldn't make much sense of it," Gilroy shares.

The company also is working with the TIC at Fort Huachuca. According to Gilroy, the service is interested in 3e Technologies' 527 wireless mesh access point. He notes that a normal wireless node is an entry point into a network. A stand-alone node with user authentication will transmit encrypted messages to the access point, which then inserts the message into a wire-based LAN and transmits the data back to the wireless client.

The Army is examining using mesh architecture for mobile forces. Gilroy says that a mesh network is self-healing and self-forming. When activated, individual access points contact and connect with other access points within radio range to create a multilink network. He adds that the 3e Technologies-based mesh network can support up to 41 access points.

As access points move out of range, they leave the mesh, and the system reconfigures itself automatically. In a mobile unit, one lead vehicle equipped with a very small aperture terminal or other satellite communications equipment to connect back to higher echelons would serve as a root node. This allows similarly equipped vehicles to communicate with each other and with other units over the horizon, Gilroy explains.

WEB RESOURCES

Department of Defense Public Key Infrastructure:
www.defenselink.mil/nil/org/sio/ia/pki

Joint Interoperability Test Command:
http://jitc.fhu.disa.mil

U.S. Army Technology Integration Center:
www.hqisec.army.mil/isec/isec/directorates/tic/tic.asp

3e Technologies International: ***www.3eti.com***