

# IT SECURITY

THE PROFESSIONAL JOURNAL OF IT SECURITY & INFRASTRUCTURE PROTECTION

## SIMPLIFYING SECURE COMMUNICATIONS

By Luther Martin

In homeland security operations, communicating securely can be just as important as communicating at all. This can be challenging, however, because many technologies that enable secure communications can be expensive, difficult to use and ill-suited for the dynamic environment that incident response may require. The digital certificates that are issued by traditional public key infrastructure (PKI) can be used to provide encryption of sensitive information and digital signatures to authenticate the sender of a message, but the administrative functions required to enroll a user in a PKI system make it difficult to communicate securely to users whose identities are not known in advance.

PKI certificates derive their high assurance from a rigorous enrollment process where a user's identity is confirmed before a certificate is issued. This means that it is difficult to enroll additional users quickly. So PKI can be very useful in a well-defined environment, like federal agencies and their contractors, where all of the participants are well-known, but the technology is difficult to deploy to new users, particularly when speed is required. And because ceasing communication is not an option for those responding to homeland security incidents, this can leave many communications channels unsecured, like e-mail, instant messaging and portable wireless devices.

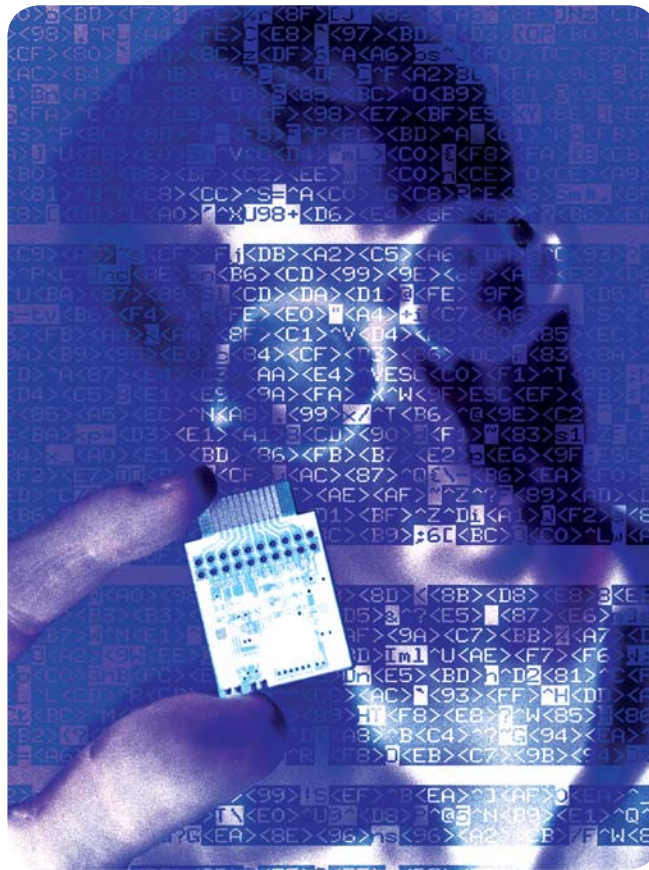
A response to a homeland security incident may require

the involvement of many different government agencies, but the actual agencies involved may not be known until the nature of the incident is more clear. State and local governments may also need to be involved in an incident response, but again, the exact organizations that will need

to respond will not be known until the exact location of an incident is known. Because it is not feasible to enroll every one of the millions of possible responders to a homeland security incident in a PKI system, a different technology needed to be invented.

To solve this problem, Professors Dan Boneh of Stanford University and Matt Franklin of the University of California, Davis, invented the first feasible and secure instance of a technology called identity-based encryption (IBE) under a Defense Advanced Research Projects Agency (DARPA) contract for research into technologies for creating dynamic coalitions. Instead of needing to get a user's encryption key from a digital certificate, IBE uses an e-mail address for the key. To send an encrypted message, a sender only needs to know the e-mail address of the recipient. The overhead

of creating and managing digital certificates is no longer incurred, and users no longer need to be enrolled before they can receive and read secure communications — all they need is an e-mail address. IBE is a public key encryption technology, but one that does not require digital certificates, and IBE technology has been incorporated into



# Feature

the products of Voltage Security Inc., a security software company based in Palo Alto, California.

IBE technology has been tested in two homeland security exercises and has proved a good solution to communicating to dynamic groups of homeland security users: first at the 2004 Joint Warrior Interoperability Demonstration (JWID) and more recently at the U.S.-Canadian Secure Mobile Data Communications Trial.

At JWID 2004, an exercise that simulated responses to several concurrent homeland security incidents, IBE technology let exercise participants securely share information with other participants, but without the administrative costs of using traditional PKI. Using IBE, JWID 2004 participants were able to quickly and easily communicate securely to other exercise participants, including those from the Federal Emergency Management Agency, the Coast Guard, and state and local governments.

"JWID 2004 set high objectives for Voltage IBE including information sharing, multi-level security and intelligence, surveillance and reconnaissance dissemination. Voltage met or exceeded all of these objectives and was truly a 'top performer' of JWID 2004," said Coalition Warrior Interoperability Demonstration (CWID) officials. "Voltage IBE is uniquely positioned to support Department of Homeland Security [DHS] organizations requiring data encryption, secure e-mail communications and external interfaces to BlackBerry or personal digital [PDA] devices."

The U.S.-Canadian Secure Mobile Data Communications Trial evaluated and demonstrated cross-border interoperability of a secure data communications architecture using commercially available wireless technologies and devices that allow homeland security agencies to achieve their mission. IBE was a key part of this trial, providing easy-to-use encryption of data sent to and from BlackBerry hand-held devices.

"Identity-based encryption provides the ability to quickly establish secure communications with dynamic groups of people at the edge of the enterprise, such as incident responders at the national, state and local level," said Dr. Doug Maughan, cybersecurity research and development program manager, Homeland Security Advanced

**"IDENTITY-BASED ENCRYPTION PROVIDES THE ABILITY TO QUICKLY ESTABLISH SECURE COMMUNICATIONS WITH DYNAMIC GROUPS OF PEOPLE AT THE EDGE OF THE ENTERPRISE, SUCH AS INCIDENT RESPONDERS AT THE NATIONAL, STATE AND LOCAL LEVEL"**

**Dr. Doug Maughan, cybersecurity research and development program manager, HSARPA**

Research Projects Agency (HSARPA). "It allows sensitive information to be rapidly and easily disseminated to them over a secure channel."

Because IBE is encryption technology, its use is governed by Federal Information Processing Standard (FIPS) 140-2, which precludes the use of unvalidated cryptography for the cryptographic protection of sensitive or valuable data within federal systems. To satisfy the requirements of government users, Voltage Security obtained FIPS 140-2 validation of its IBE Cryptographic Module, has its products under Common Criteria evaluation, and expects to achieve an EAL2 certification in early 2006.

IBE only provides encryption of information, so digital signatures must be created using other means. The Voltage technologies that have been demonstrated in homeland security exercises provide their own digital signature capability, but other ways to digitally sign can easily be integrated with IBE. It is possible to use IBE for encryption, but using a digital certificate from a Common Access Card (CAC) or Transportation Worker Identification Credential (TWIC) smart card to digitally sign messages combines the high-assurance proof of identity with ease of use and deployment.

The ease of use, simple management and low infrastructure requirements of IBE make it well suited for many homeland security applications, including secure wireless communications. The successful use of IBE-based technology in homeland security exercises has shown that it has a useful role in addressing the challenges of establishing secure communications with rapidly changing dynamic groups, like those that are needed to respond to various security incidents. Expect to see more of this technology in the future as it is deployed in greater numbers in the homeland security community.

## About the Author

Luther Martin is a cryptographer at Voltage Security Inc. in Palo Alto, Calif. His 18-year career in security has included experience at government agencies, consulting firms and security product companies, including the design and implementation of the public key infrastructure used by the U.S. Postal Service (Postal PKI).

Reprinted with permission from IT Security, March 2006.

© HOMELAND DEFENSE MEDIA. All Rights Reserved. On the Web at [www.itsecuritymagazine.com](http://www.itsecuritymagazine.com).



## Voltage Security

1070 Arastradero Road, Suite 100 • Palo Alto, CA 94304 USA  
(888) 2-VOLTAGE • [www.voltage.com](http://www.voltage.com) • [info@voltage.com](mailto:info@voltage.com)