Voltage Unveils Encryption Program

New Software Is Designed to Help Users Send Protected Messages, Boosting E-Mail Security

By DON CLARK
Staff Reporter of THE WALL STREET JOURNAL

A Silicon Valley start-up has developed an unusual technique to encrypt e-mail or documents, addressing an obstacle that has prevented widespread adoption of the data-security technique.

Voltage Security Inc., a closely held company based in Palo Alto, Calif., Monday is announcing software that is based on a new way to create encryption keys, which scramble messages to protect unauthorized people from reading them. The software is designed to make it much easier to send protected messages, especially when corresponding with people for the first time.

The company's software is based on technology proposed by computer-science professors Dan Boneh, of Stanford University, and Matt Franklin, of the University of California at Davis. Taher Elgamal, a well-known encryption expert, said their invention is recognized as a breakthrough in the scientific community. If Voltage's software works as advertised, he said, many more companies and computer users could begin protecting their electronic communications.

"I am both hopeful and optimistic," said Mr. Elgamal, who is chairman and chief technology officer of Security Inc., an unaffiliated company that makes network-security technology.

Sathvik Krishnamurthy, Voltage's chief executive officer, said its software could help financial-service companies and health services adapt to new laws that impose tight controls over consumer information. Initial companies testing its software include eHealthInsurance Services Inc. and Silicon Valley Bank.

Encryption keys -- lengthy strings of letter and numbers -- are typically built into specialized software that makes recognizable words and numbers unintelligible. One approach, called public-key encryption, creates a private and a public key that work together to lock and unlock messages. Senders, in theory, find a potential recipient's public key in a directory, and use that identifier to encode a message for that recipient alone.

In practice, those keys are combined with other information in electronic documents called certificates, and distributed by special service companies called certificate authorities. People often have trouble finding recipients' certificates, or find that their correspondents don't have certificates or the right software.

"It's a big impediment to using the technology," said Paul Kocher, president of Cryptography Research Inc., a San Francisco consultancy focusing on encryption.

In 1984, an encryption pioneer named Adi Shamir challenged other researchers to come up with a plan in which a user's public key could be any ordinary string of numbers. In 2001, Mr. Boneh and Mr. Franklin proposed what they called identity-based encryption.

Their approach uses some esoteric mathematical techniques and a master key -- controlled by a company or another organization -- that generates a private key from a piece of public information about a person. That person's e-mail address, for example, could act as a public key, avoiding the need to hunt for one through a certificate authority.

Voltage, formed by Mr. Boneh and three of his students, developed server software that authenticates users and generates private keys from users' e-mail addresses or other information. It sends those keys to users that have a related piece of PC software, which is designed to spread rapidly.

An existing user could send a scrambled message to another person who had never used the technology. To unlock it, the recipient would click on a link in the e-mail to go to a site running Voltage's server software, which would send the recipient the software to both read and create messages. In Microsoft Corp.'s popular Outlook mail program, Voltage's PC software appears simply as a button labeled "send secure" that is next to the familiar "send" button on a message.

A bank or insurance company could use the technology to send out encrypted information to its users, Mr. Krishnamurthy notes. The company, which hasn't disclosed pricing of its software, says it also can protect instant messages or even voice communications on the Internet. Users also don't have to be connected to networks as often as most public-key systems, he says.

One drawback, to some users, is that a company could use the master key to decode employee messages. But many companies haven't deployed encryption for fear of disgruntled or departed workers locking up sensitive information.

Jamie Lewis, a market researcher at the Burton Group, said some large corporate partners may hesitate before adopting a proprietary technology from a small company for such an important application. "There are some challenges they will face," he predicted.

Write to Don Clark at don.clark@wsj.com