Guarding email privacy

Encryption to find place in new University directory

BY DAVE AMBER
The Battalion

Most Internet users know hackers can steal credit card numbers and other information from insecure Web transactions. But in everyday communications, how can one be sure somebody sending a simple email is who he claims to be?

One answer is to encrypt, or code, email and other files. Already an integral part of e-commerce transactions on the Web, encryption is increasingly viable in email services.

Now Texas A&M is trying to build an encryption function into the new online directory currently being installed. The system would allow users to find keys for sending encrypted email to anybody in the directory who has a key in place.

The University encourages encryption use, said Thomas Putnam, director of Texas A&M Computing Information Services (CIS).

"We're living in a world where we will be seeing more encryption," he said. "It not only ensures your privacy, but the important thing is that encryption allows you to have verification of origin."

Putnam said it is easy to fake the originating name and other information on an email. "If you get an email from a professor, how do you know it's really from him?" he said.

As a groundswell builds in Texas to implement general use of encryption and "digital signatures" for confirming email origins, the University wants to institutionalize the process here, so that one standard system is in place, Putnam said.

Providing such a centralized and secure directory for public keys is one of the barriers faced by advocates of encryption technology.

With the new University directory, a user could find the public key for another person listed there and use it to encode a message to that person. At the other end, the message recipient would decipher the message with a private password key.

Charles Boatwright, a CIS senior systems analyst, said the University is laying the groundwork for this system, but there are a number of hurdles. "The emphasis is on infrastructure," he said. "We have to be careful. Are we talking about encrypting Web traffic or email? Will all operating systems be able to use it?"

He said full implementation will not happen until these questions can be worked out.

Encryption software is not new. PGP, or Pretty Good Privacy, code has been available for free online since 1991, quickly becoming the standard. Another system, X.509, is used by the state of Texas as the standard for encrypting state transactions.

Ron Woessner, vice-president of Dallas-based Zixit, Inc. and an A&M former student, said his company's new encryption software may be the solution to hard-to-use encryption systems.

Zixit, a subsidiary of the Blockbuster Corporation, publicly unveiled its encryted email program called "Zixmail" in March.

PGP critics like Woessner said the common standards are difficult to use. Products like Zixmail are "as easy to use as email," Woessner said.

Putnam said CIS is looking into services like Zixmail. "If we are emailing back and forth between the University and a company, we have to keep students' information private," he said. "That's a place we might use the Zixmail package, because you can set up a relationship with an individual or a specific company."

But, setting up a relationship is one of the problems with such software. Email users at both ends must use the same encryption software. After July 1, that will cost money for Zixmail users — they will pay $12 per year for each email address they want to encrypt. "You can't underestimate the secured delivery of it," Woessner said. "Twelve bucks for a FedEx or 12 bucks for one year of service."

But this means each recipient of an encrypted email will also have to pay for the service.

"A problem here is that people have to use the same systems," said Alexander Fowler, policy director for the Electronic Frontiers Foundation, a consumer organization that monitors issues such as the privacy of electronic communications in cyberspace. "Is the public going to pay for that?"

"The great advantage of PGP over services like Zixit's is it's free," Putnam added.

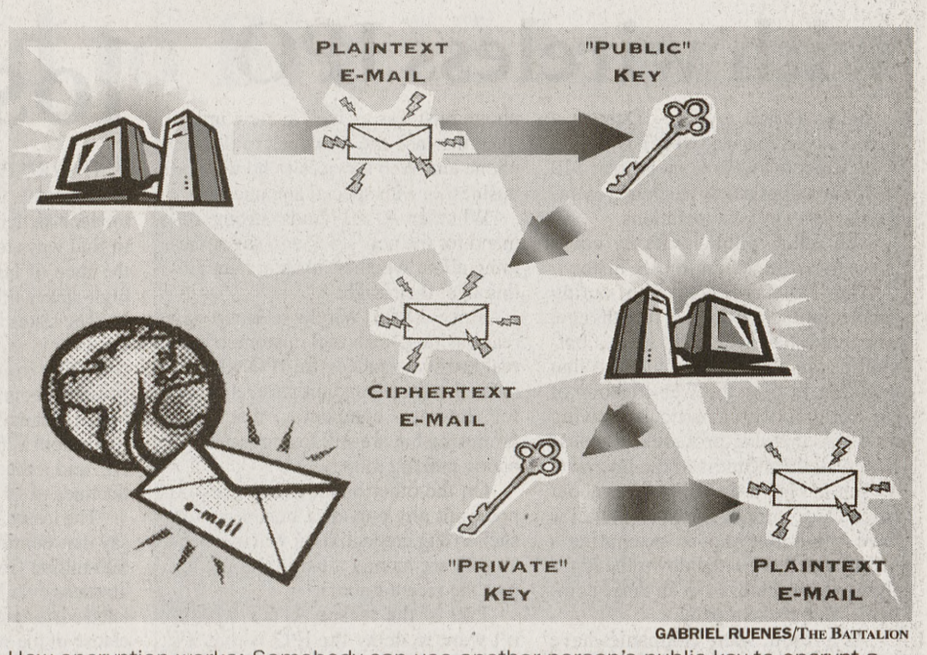
Encryption systems — free or not —still raise flags about security. While they encrypt emails and other files, the systems can also be used to encrypt materials that are illegal to transmit over the Web, like child pornography.

"Encryption is a double-edged sword. If you are doing something illegal, you can hide it," Putnam said.

But Putnam said spying on messages is not a concern at the University. "The University has a policy not to look at anybody's email unless it suspects illegal activity," he said.

"There's a certain amount of paranoia about privacy. At the University we generate a million email messages a day. Imagine the work involved if you wanted to go look at all of those," he said.

"If we suspected illegal activity, we would go to the police or FBI. It's not us who ask" Putnam said.



GABRIEL RUENES/THE BATTALION

How encryption works: Somebody can use another person's public key to encrypt a message to that person. When the recipient receives the encrypted email, or ciphertext, he decrypts it with his personal "private" key that he stores on his computer.

21st century "Enigma" machines: regulations for exporting code

In the movie *U-571*, which opened last week, World War II Allied forces race to capture an "Enigma machine" used by the German navy to encode radio messages. The movie underscores the historical importance of encryption for message security, the value of breaking those codes and the reason some governments may be nervous about sharing encryption technology.

Until this year, email encryption technology had been a concern of the United States justice system. The Department of Justice (DOJ) feared encryption codes would fall into the hands of terrorists or spies from other governments.

Putting encryption codes up on the Web, the government said, violated export controls because nations restricted from receiving such information, like Libya, Cuba and Iran could "import" the software online.

"It's considered aiding and abetting the enemy," said Don Tomlinson, a Texas A&M professor of journalism and media law. But he added the government's enforcement was impractical. "Cyberspace has no physical boundaries, so the usefulness of regulation is limited."

Until last year, the Justice Department held fast to regulations of overseas sales of encryption software, but in January, the White House eased export controls.

Earlier this month, a Case Western Reserve University professor targeted by the DOJ for criminal investigation for posting encryption codes on the Web won his case before a federal court of appeals. The court ruled that encoding software was protected under the First Amendment.

As a result of the government's loosening of restrictions, programmers can now put their source code up on the Web providing they email the Commerce Department the URL for the Web site.

Diverse groups, ranging from First Amendment and human rights organizations to scientific associations, have been involved in the campaign to relax export controls.

The National Academy of Sciences, for example, urged in a 1996 report that the federal government should promote commercial use of encryption.

And in terms of safeguarding original creative works, encryption offers a margin of safety for transferring literature, music or other original materials through cyberspace.

"Encryption is the best solution as a means of protecting intellectual property," Tomlinson added.