Safeguarding your electronic 'John Doe'

SIMSON GARFINKEL

Earlier this year, a suspicious program turned up on bulletin board systems around the country. The program was called PKZ300B.EXE, and it purported to be latest and greatest version of PKZIP, a popular shareware program for compressing and archiving files.

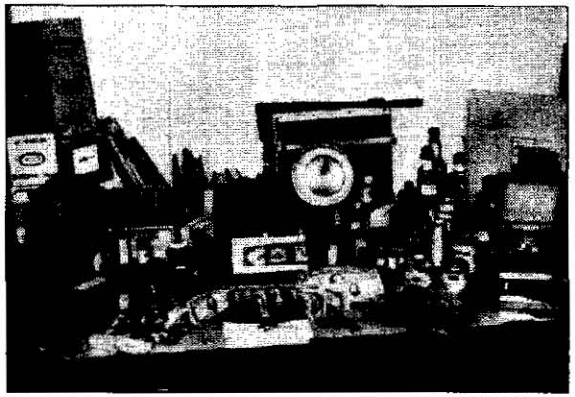
But people who downloaded and ran PKZ300B.EXE got a nasty surprise: Instead of compressing their files, the program erased their hard disks. PKZ300B.EXE was a malicious fraud.

Electronic mail is one of the most popular uses of the Internet. But e-mail has an Achilles' heel: It's all too easy to forge electronic messages. When I send an e-mail message to a friend, I usually sign it "–Simson." But anybody else could send a message and sign it exactly the same way. Indeed, with a little technical sophistication, it is possible to create a fake message that cannot be distinguished from an authentic one.

Computers have even created problems for printed documents. With a scanner, a laser printer and a program such as Adobe Photoshop, it's a simple matter to scan somebody's signature from one legal document and paste it onto the bottom of another. Some of my friends at MIT used this technique in the early 1980s to create fake ID cards so that they could go out drinking. They scanned in a Pennsylvania driver's license (which at the time was nothing more than a photograph in a fancy plastic holder), changed the date from 1965 to 1962, then printed the new license onto a piece of glossy photographic paper. Instead of desktop publishing, this was desktop forgery.

Thankfully, today there is a powerful way to stamp out digital forgeries. Called "digital signatures," the technique gives governments, organizations and even individuals a simple way to create fraud-proof digital documents.

Digital signatures are based on something called public key cryptography. To use this kind of cryptography, you first need to create two "keys": a public key, which you can give to your friends and publish on the Internet, and a secret key, which you don't share with anybody. To sign your digital signature, you need a special program. That program reads in the document, seals the message with your secret key, a special set of electronic instructions, and attaches a code to the bottom of document. To verify your signature, somebody needs a copy of the signature program and your public key.



1947 FILE PHOTO

High technology has replaced the tools of the trade of yesteryear's desktop forgers.

One popular program for signing digital signatures is called Pretty Good Privacy. For several years PGP has been at the center of a storm of controversy – not because of its digital signatures, but because of its ability to encrypt, or scramble, messages. That's because the encryption system that PGP uses, an algorithm called RSA, can be used for either purpose.

Cryptography has long been a sore spot for the federal government. The government wants Americans to use cryptography that's strong enough so that our messages won't be intercepted by criminals and foreign businesses, but weak enough so that such organizations as the FBI will still be able to intercept and decode messages by drug dealers and terrorists.

No such controversy exists in the world of digital signatures, and many governmental agencies are implementing plans for using such signatures for a variety of purposes.

The General Services Administration is looking to use digital signatures for signing electronic purchase orders. The Federal Aviation Administration is considering them for signing electronic pilot credentials. The Social Security Administration might use it for benefits.

To use these systems, you'll have to get your public key registered with the government, so that the agencies will know you are really you. Sensing an opportunity to move into the 21st century, the US Postal Service is gearing up to be the country's registrar. Current plans are to offer four categories of certification, the lowest being a "smart card," which you can purchase in a vending machine, the highest being a "biometric certificate," which you need to verify with a fingerprint or retina print every time you use it.

To avoid getting bogged down on the question of cryptography, the government has developed a competing digital signature system called DSS, for Digital Signature Standard. Unlike RSA, DSS can't be used for encryption.

DSS hasn't caught on outside the government. Instead, a growing number of companies are putting RSA signatures into commercial products. A new company, VeriSign Inc., based in Redwood City, Calif., is providing certification services. You can find more information on VeriSign's WWW page, http://www.verisign.com/.

Digital signatures can stamp out fraudulent software distributed on the Internet; rogue software wouldn't be properly signed, and people would know not to trust it. They can also put an end to faked e-mail. Already, RSA signatures are built into Apple Computer's PowerTalk e-mail system, and they are expected in an upcoming version of Microsoft Mail.

Digital signatures could even stamp out fake IDs. Earlier this year, Pitney Bowes Inc. announced a system for putting digital signatures on driver's licenses and other paper documents. Called Veritas, the system puts on the license's back a two-dimensional bar code that contains a copy of all the information that's on the front, as well as a digital copy of the person's face. A small reader scans the bar code, verifies the digital signature and then displays the information: your photograph, name and age.

My friends at MIT would have had a hard time getting around that.

Michael Putzel is on vacation. Globe correspondent Simson Garfinkel can be reached at simsong@vineyard.net.

Boston Globe, Friday, August 25, 1995. Plugged In section p. 79