



## Putting E-Mail Under Lock and Key

### Memory Device Encrypts Messages for Privacy

By PAUL ENG

Nov. 22, 2004 - Who's reading your e-mail besides the intended recipient? It could be anyone on the Internet.

Like most other digital data, e-mail can pass through any number of computer servers as it travels the global Internet en route to its final destination. And with a clear majority of e-mail being just plain text, many security and privacy experts say messages can be intercepted, read, copied and stored at any point along the way -- all without anyone else's knowledge.

Some tech-savvy Net surfers are using so-called public key encryption software such as PGP to scramble any sensitive e-mail from prying eyes. But two companies have joined forces to make such encryption setups even easier to use.

Stealth Ideas, a maker of computer security peripherals in Sherman Oaks, Calif., has introduced a new device and Web service geared toward protecting online privacy.

Its StealthSurfer is a "USB drive," or a small solid-state memory device that acts like a hard drive when plugged into a computer's USB port. The drive contains a modified version of the Netscape Navigator Web browser that stores every bit of online information -- history of Web sites visited, login passwords, copies of Web pages, images -- using the device's built-in memory. Since it bypasses the hard drive in a computer, all traces of online activity go with the drive once it's removed.

The latest version of StealthSurfer, however, adds a free Web-based e-mail service powered by a public key encryption technology developed by Hush Communications in Vancouver, British Columbia.

### A Ring of Keys

When a StealthSurfer user signs up for an e-mail account, a small encryption program is downloaded from the company's e-mail servers. The program follows so-called OpenPGP encryption standards to create a unique pair -- one public, one private -- of software "keys."

Both keys are uploaded to StealthSurfer's e-mail servers. The user's public key is made available in a publicly accessible database while the private key is further encrypted by a pass phrase created by the user.

When a user wants to send an encrypted e-mail using the system, the program asks for the user's pass phrase to retrieve the user's private key. The encryption program uses that key to create a one-time "message key" that scrambles the e-mail's text.

Once encrypted, the program retrieves the recipient's public key from the database of keys stored online to encrypt the message key. Both the encrypted message and the scrambled message key are then combined in a single e-mail.

When the user sends the encrypted message, the StealthSurfer's e-mail servers will append to the end of it a unique digital signature -- a string of characters that is created based on the encrypted message itself. This ensures that the locked e-mail isn't tampered with as it makes its way through the Internet to the recipient.

Only the recipient's corresponding private key can unlock the embedded message key which in turn unscrambles the e-mail message.

## Simply Unbreakable?

Brad Weber, chief executive officer of Stealth Ideas, says there are plenty of PGP-based encryption programs that security-conscious Net surfers can use to guard their e-mails. But the company believes the StealthSurfer device and the company's Web-based e-mail solution offer several unique advantages.

"Privacy and security are always a matter of annoyances versus conveniences," says Weber. "In the Hush Communications solution, it's all Web-based. It's small, easy and accessible [from any Web computer]. It's not a big burden."

And like other OpenPGP encryption programs, the digital security offered by Hush's software is of 2,048-bit length. In other words, Hush's encryption is nearly impossible to crack.

"By using all the technology known today, if all those computers were put on to break 2,048-bit encryptions, they would be going at it for years," says Ben Cutler, CEO of Hush Communications. "But who has the super-advanced computers and knowledge [to crack it]? I can't say that I know."

## Little Lock Ups

Whether or not such encrypted e-mails are truly spy-proof, there are several other shortcomings to the StealthSurfer and Hush Communications security solutions.

For one, very few Net users -- less than an estimated 10 million worldwide -- have installed OpenPGP-based encrypted schemes. That means, for now, encrypted e-mails can be sent only among other StealthSurfer accounts or other OpenPGP-based e-mail services, such as Hush Communications' own Hushmail.com.

StealthSurfer can still send unencrypted e-mail to any Internet address, but the only security feature that can be added is the unique digital signature. That will help the recipient verify the message as authentic -- as opposed to a cleverly disguised piece of junk e-mail or virus. But the message could still be copied or read by others as it winds through the Net.

StealthSurfer's free e-mail service won't offer a lot of room either. Google's free G-mail service, for example, offers one gigabyte of online storage space for messages. StealthSurfer offers -- for now -- only two megabytes of space.

"We'll be considering upgrading the [storage] quota," says Weber. "But even at Web mail services with upgraded quotas, only a small number [of members] use large portions of it. People who understand StealthSurfer's benefits appreciate it for the service it provides -- privacy and security."

They'll also need to understand that while using the encrypted e-mail service from Stealth Ideas is free, the actual StealthSurfer device isn't. The USB memory device costs \$99 to \$299, depending on how much storage capacity the model has.

Copyright © 2004 ABC News Internet Ventures