New digital security program doesn't protect as promised

September 29 2009

(PhysOrg.com) -- University of Texas at Austin scientists have shown that they can break "Vanish," a program that promised to self-destruct computer data, such as emails and photographs, and thereby protect a person's privacy.

There is no way to permanently delete any material posted or sent through the Internet, and this leaves people's information vulnerable to breaches in privacy.

Vanish, created by University of Washington researchers, claimed to solve that problem by encoding digital data so that they can only be read for a limited time window, such as eight hours. After that time, the data still exists, but it can no longer be read because the "encryption key" used to access it is no longer available. The data looks like digital gibberish.

The Texas scientists, along with colleagues from Princeton University and the University of Michigan, created a program called "Unvanish" that makes Vanished data recoverable after it should have disappeared.

"Our goal with Unvanish is to discourage people from relying on the privacy of a system that is not actually private," says Emmett Witchel, assistant professor of computer science. "We wish to respect the privacy concerns of people that might be using the Vanish system."

The Vanish system encrypts data and takes advantage of the structure of

peer-to-peer file sharing systems to manage encryption keys in a novel way. The keys are split up into many small pieces and stored at many different places on the network.

Unvanish works by collecting and storing anything that looks like a fragment of a Vanish key on the network. Later, when given a message that should have disappeared, the program consults its archive of these fragments and finds the pieces it needs to decrypt the message. Using Unvanish, it is possible to make Vanish messages reappear long after they should have disappeared, nearly 100 percent of the time.

"Messages that self-destruct at a predetermined time would be very useful, especially where privacy is important," says Brent Waters, assistant professor of computer science. "A true self-destruction feature continues to be challenging to provide."

The lead programmer on the Texas research was computer science graduate student Owen Hofmann. Post-doctoral researcher Christopher Rossbach also contributed to the project.

University of Michigan graduate student Scott Wolchok and Assistant Professor J. Alex Halderman and Professor Edward Felten from Princeton University independently broke the Vanish system.

Provided by University of Texas at Austin (news : web)