Technology Review AN MIT ENTERPRISE

Encryption Software May Halt Wire Tapping
The creator of the most popular e-mail encryption program has a new application for Voice-over-Internet-Protocol phone calls.
By Kate Greene

E-mail encryption creator Phil Zimmermann hopes to bring the same level of privacy to Voice-over-Internet-Protocol phone calls. (Image courtesy of Phil Zimmermann.)

Phil Zimmermann, creator of the Pretty Good Privacy (PGP) e-mail encryption software, wants to bring a similar level of security to phone conversations. A decade after U.S. Customs investigated him for allegedly violating export restrictions on cryptographic software (when PGP began to spread worldwide), Zimmermann has released encryption software, called Zfone, that makes it impossible for eavesdroppers to listen in on Voice-over-Internet-protocol (VoIP) phone calls.

VoIP encryption isn't new -- Skype, the most popular VoIP service uses encryption -- but Zimmermann's software issues encryption keys that bypass the servers routing Internet calls and sets up the encryption directly on the voice channel. That added layer of protection means even if someone can access the server that routes a call, there's no way to decrypt the call's contents.

With the ongoing controversy over the National Security Agency's program to collect information about phone calls made by Americans, privacy advocates are becoming increasingly concerned about the government's access to citizen's information. Thus, Zimmermann's software has serious implications, particularly for those involved with national security, since it could pose a technical challenge to the laws that currently allow the government to access information held by phone and VoIP service providers.

Technology Review: How does Zfone work?

Phil Zimmermann: Zfone is the software that implements my new encryption protocol, called ZTRP, in a certain way. Zfone is not a VoIP client; it watches for the packets of Internet data going in and out of the machine and looks for ones that are VoIP related. Upon detection of a VoIP call, it intercedes to encrypt the call by setting up a key agreement in the media stream and encrypts the packets of voice data.

As time goes on, you'll start to see ZTRP inside VoIP clients. I have a software development kit that people can stick in their VoIP clients, including companies that make VoIP hardware.

TR: How is Zfone different from most VoIP encryption schemes?

PZ: The other approaches all require the involvement of servers -- and some of them are egregiously insecure. To understand how they work, you need to understand how VoIP works. At the beginning of a call, a couple of packets go in between you and your server and say "Here I am. Here's my IP address." When I call you, my server knows where to call and sends packets to your server. Then the servers allow us to send voice packets directly to each other. They're involved at the beginning and get out of the way.

In one encryption scheme, the key that encrypts and decrypts your voice packets is sent to your server, which sends it to my server, which then sends it to me, and then we talk using that encrypted channel. Unfortunately, now the servers know the sessions key, so what if I live in China and my service provider [that owns the servers] is in China? The Chinese government is going to know the key and they can wiretap the call. If you trust the service providers, then fine, no problem. But the people that operate the servers don't necessarily have in mind the best interests of the people who use them.

I'm the only one who does it through the voice stream. The voice packets already flow and I jump in there and put in special packets that negotiate all the keys between the two parties. The servers are not involved in any way in the process.

TR: Skype, the most popular VoIP client, already has encryption software, so why doesn't Zfone work with Skype?

PZ: Skype is not compliant with VoIP standards; they have a closed protocol. Skype uses its own encryption software and it doesn't tell anyone how it works. I prefer to use encryption that is open; I publish my source code.

TR: Who would use this VoIP encryption software?

PZ: Who wouldn't use this? Who wants to not be wiretapped? I'm not talking about wiretap from law enforcement -- I'm talking about wiretap from organized crime. Organized crime is doing phishing attacks and taking over your computer with hostile software. I'm making the prediction that those same criminals will attack VoIP when it gets big enough. It could be point-and-click wiretapping from the other side of the world.

TR: With your e-mail encryption software, you were under a criminal investigation by the U.S. government, which alleged that you violated export restrictions for cryptographic software. The case was eventually dropped, but how do you plan to avoid such a complication this time around?

PZ: This time I'm being careful about getting good legal advice and following export controls. I've filled out the paperwork and filed with the U.S. Commerce Department. I'm getting things back that clear it for export. I'm being very careful this time.

TR: Your software release is timely in light of the ongoing news about NSA's program to collect information about phone calls in the United States. Could you discuss the tension between technology and the law, especially when it comes to emerging forms of communication and keeping information safe and private?

PZ: I don't see this as a black-and-white situation. I sympathize with the need for NSA to catch the bad guys, and I want them to catch these bad guys. But we have to be careful about creating surveillance machinery that may be used for other purposes later.