# PGP founder unveils new VoIP security

March 23 2006

Somewhere out there, someone is a little too curious about your data. This is the main concern of Phil Zimmermann, the creator of the industry standard PGP (Pretty Good Privacy) e-mail encryption protocol who has just debuted a new standard for encrypting Voice over Internet Protocol data. Zfone, Zimmermann's new VoIP program, incorporates a new security protocol that is being presented for peer review within the academic and Internet security communities.

Zfone, which is presently available for the Mac OS X and Linux operating systems with a Windows version to be released in a few weeks, is the continuation of PGPfone, a VoIP effort started by Zimmermann in 1996. Hampered by a lack of broadband Internet connections throughout the United States, the program was put on the back burner while Zimmermann looked into other concerns regarding online security and privacy efforts.

Ten years later, at a time where broadband Internet services have become prevalent and 11 million people worldwide use VoIP services either for home or business use, the effort can now continue.

Where most Internet security procedures tend to be intricate and technical, Zfone is designed to be robust, simple enough for anyone to use and secure enough not to leave anything left over for other users to snag and use for their own ends. In the past, encryption technologies have relied on techniques such as certificates, passwords and shared keys. While functional, these technologies rely on interaction with servers and trade data that could remain on the servers. Under Zfone's

encryption protocol, no keys are traded and the necessary data for a secure connection between two parties is produced by the hardware and destroyed at the end of the call.

This may have arrived just in time. Beyond e-mail scams and viral attacks that seem to plague PC users every couple of months and keep them constantly updating bundled protection software, it's become more profitable to gather and sort any and all personal information that can be collected.

Phishing scams asking for user identification and passwords from seemingly valid companies are simply the beginning, and where these efforts leave off, more sophisticated tactics are under way. Voice data such as VoIP-based telephone calls made from an office environment can be captured and sorted into audio files using tools such as Voice Over Misconfigured Internet Telephones. From there, the software can be easily expanded upon to make sorting, filtering and categorizing the captured data easier and more specific to office personnel.

Where wiretapping and spying on an older phone system could only be done in a few ways, migration towards VoIP networks could open the doors for people looking to gather personal and sensitive data.

"With VoIP, the threat model is vastly more expansive. Imagine you have 1,000 PCs in your company and just one becomes infected with software that sniffs packets, including voice packets and captures them, sorts them in .wav packets and organizes them by who's calling who," proposed Phil Zimmermann. "You could point and click as to which calls you wanted from the CEO or the in-house legal counsel."

Zimmerman then illustrated that Zfone and its encryption protocol can both function independently as well as be integrated into both the hardware and software of popular VoIP applications and devices.

"We have to encrypt VoIP," said Zimmermann. "We have no choice."

"Ultimately, the phone networks will switch over to VoIP because it allows for better functionality and that's where both the cable and telecom networks are going," said Ross Rubin, an analyst for the NPD group, which specializes in consumer and retail trends.

"It's not difficult to spy on traditional voice networks or unencrypted Internet data," said Rubin. "The former uses a wiretap; the latter can be done with a packet sniffer."

Zfone is currently in a deployment stage wherein the program is freely available for download and will be ready for widespread deployment within a year. Zimmermann's encryption protocol has been sent along for peer review to boards such as the Internet Engineering Task Force for inclusion with current VoIP programs. Zfone's source code, which includes documentation for the new encryption protocol, has also been posted for download by anyone looking to study the code and use it in their own programs.