



VoIP Security Gets More Visible

Greg Goth

Phil Zimmermann, inventor of the email encryption application Pretty Good Privacy (PGP), was a lightning rod for the debate over user rights to data security throughout the 1990s. Zimmermann originally designed PGP as a human rights tool, but the US government investigated him for three years on the grounds that posting PGP on a domestic Usenet site might have broken encryption export law; it eventually dropped the case in 1996.

Ten years later, Zimmermann is once again at the forefront of the latest communications technology and its security implications. In July 2006, Zimmermann released the beta version of his latest brainchild, Zfone (<http://zfoneproject.com/index.html>), a voice-over-IP (VoIP) peer-to-peer (P2P) encryption application. Zimmermann, whose activist credentials extend beyond PGP to the effort to freeze nuclear weapons in the 1980s, acknowledges that the world since the attacks of September 11, 2001 is far different from the one into which he released PGP, but as the underlying telecommunications infrastructure converts from the public switched telephone network (PSTN) to VoIP networks, the implications for secure communications are no less critical.

Indeed, he says, the old assumptions about who might be tapping voice communications need to be discarded. No longer will the network's physical properties limit wiretaps to clandestine alligator-clip jobs near a specific exchange, a phone

company switch, or an international border. The underlying threat model to VoIP networks mirrors that of the threat to packet-based data networks – once an attacker gains access to a voice stream, a compromised node can be wiretapped with a mouse point and a click from anywhere in the world.

So, rather than appeal to activists concerned about governments overstepping their mandates as he did with PGP, Zimmermann says Zfone will be positioned to appeal to businesses that deploy VoIP networks and anyone afraid of what might happen in a hacked network, as well as to intelligence agents in deep cover who must have secure encrypted communications. In fact, Zimmermann and two colleagues have submitted an Internet draft to the IETF describing Zfone's key-and-session management methods. Although Zimmermann says widespread market adoption of Zfone shouldn't depend on the technology's elevation to request for comment (RFC) status, such a move could cement the technology in risk-averse industries and government deployments as well as with early adopters.

The great unknown presently is whether US policymakers who champion expanded wiretapping capabilities might attack Zimmermann's invention as enabling terrorists to use encryption as they did PGP. Regardless of how Zfone itself plays in the public discussion, Zimmermann and other industry figures say the technological

and policy implications of VoIP security need to gain wider dissemination sooner rather than later.

VoIP Technology's Many Flavors

"There are all kinds of VoIP security scenarios," says David Endler, chairman of the VoIP Security Alliance (VoIPSA; www.voipsa.org). "There are carrier and provider security issues, there's enterprise security and consumer security. We're also starting to see VoIP bleeding into other technologies like instant messaging and Web services. To address all the issues, it has to be a team effort. Once a VoIP call leaves the confines of either your home or enterprise, it ceases to be a problem of your vendor; it becomes a provider issue – so one party can't work on security by itself."

Victoria Fodale, program manager and network security analyst for research firm In-Stat, says that not only should the issue of VoIP security be considered multidimensional but so should what VoIP itself means.

"When you talk about VoIP, what flavor are you talking about? There's IP-PBX [Internet Protocol private branch exchange] equipment, collaboration and conferencing products, IM [instant messaging] clients with voice capabilities, broadband voice services, and peer-to-peer telephony. On this laundry list, P2P is actually toward the bottom of the list."

Fodale says that, as VoIP technology bleeds outward, and as the barrier

between home and work erodes further, the VoIP security equation will have to keep step with dual consumer-enterprise needs as well as public policy concerns.

“We see a lot of things in business that start in the consumer world,” she says. “Social networking applications, wikis, and similar technologies start in the consumer world and are pushed to business. VoIP is kind of a gray area. Your solutions have to be robust enough to fit multiple scenarios. It’s not an either-or; our jobs carry over to home, home carries over to jobs, and technology is going to need to be flexible.”

Convenience and Security Must Coexist

From both economic and convenience standpoints, Fodale and Endler say that some of the existing VoIP security measures might not measure up to their conceptual strengths. Existing enterprise-class technologies are often time consuming to set up and tear down, and the most popular P2P telephony technology — Skype, which claims to be secure — is both proprietary and incompatible with many enterprise network policies.

“The biggest barrier to enabling encryption today is the overhead of maintaining a public-key infrastructure,” Endler says. “You have to take great strides to install certificates on everyone’s phone, then there’s the headache of revoking somebody’s credentials if they leave — and that’s just for encryption.”

As for Skype, Fodale says “Skype is a problem in a business network for a lot of reasons. One, it’s a port seeker, and it drives the network guys crazy. There’s an emerging equipment and solutions segment built around Skype-blocking. Since Skype’s all over the place, you can’t just block off *x* port and it’s solved. And, in particular industries such as healthcare and finance, where people are security conscious for compliance reasons, they need policy controls, they

need to be able to log traffic. So Skype is a problem.”

Both Fodale and Endler have seen Zfone’s early iterations, and believe Zimmermann has devised an application that could bridge the consumer-enterprise gap. Zfone is a P2P technology compatible with multiple VoIP client applications and doesn’t rely on public-key infrastructure. The users on each end of a Zfone-enabled call establish the call’s security by reading and comparing a short authentication string. In addition, the keys are destroyed at the end of the call, which precludes retroactively compromising the call by future disclosures of key material.

Although Zimmermann has yet to negotiate a deal with vendors of analog telephone adapter equipment, which could comprise the bulk of the market in the first stages of the PSTN-to-VoIP conversion, a complex legal element might encourage VoIP carriers to encourage their customers to use Zfone.

Will Law Drive the Market?

The legal element in question is the Communications Assistance for Law Enforcement Act of 1994 (CALEA), which mandates that carriers provide access for law enforcement agencies to conduct electronic surveillance of common carrier communications networks. The US Federal Communications Commission (FCC) has decided that CALEA also pertains to broadband Internet and VoIP networks as well as PSTN circuits (www.askcalea.net/docs/20060503_2nd-memorandum.pdf).

According to the FCC, by 14 May 2007, CALEA will “apply to all facilities-based broadband Internet access and interconnected VoIP providers.” However, the carriers are expected to shoulder the costs of making their networks CALEA-compliant themselves, and the FCC order was written broadly enough that many carriers have expressed dismay over the lack

News in Brief

The **US Department of Commerce (DOC)** and the **Internet Corporation for Assigned Names and Numbers (ICANN)** reached an agreement aimed at transitioning the **Domain Name System (DNS)** to the private sector. Paul Twomey, president and CEO of ICANN, says the agreement “means that ICANN is more autonomous.” The agreement, announced 29 September, gives ICANN greater flexibility in deciding both working procedures and which projects to pursue. It also loosens ICANN’s reporting requirements to the DOC.

More information is available at www.icann.org/announcements/announcement-29sep06.htm.

The **ISOC** has selected **Dawit Bekele** to lead its **African regional bureau**. The regional bureau — ISOC’s first — will be the focal point for ISOC education, policy, and capacity-building activities in Africa. Bekele, an Ethiopian citizen living in Addis Ababa, has been involved in Internet-related teaching, research, management, and consultancy activities in Africa for a dozen years, focusing on distributed systems, security, advance databases, network systems, and e-commerce.

More information is available at www.isoc.org/isoc/media/releases/060915pr.shtml.

Asserting problems with **Wikipedia**, including rules abuse, insular leadership, and a dysfunctional community that discourages academic contributions, the online encyclopedia’s founder has announced plans for an alternative source for organizing online information. Calling his new project “a progressive fork of Wikipedia” **Larry Sanger** said that **Citizendium** (“a citizens’ compendium of everything”) will begin initially as a mirror of Wikipedia with expert editors revising its articles. In addition to using experts to vet content, Citizendium will require contribu-

continued on p. 10

News in Brief

continued from p. 9

tors to log on using their real names and to work according to a community charter. Langer outlines Wikipedia's shortcomings and his vision for the new project in his essay, "Toward a New Compendium of Knowledge" (www.citizendium.org/essay.html).

Interested parties can apply to contribute to a private alpha version of Citizendium at www.citizendium.org/cfa.html.

In another move toward **international electronic-signature recognition**, the **European Telecommunications Standards Institute (ETSI)** has mapped **US Federal Bridge Certification Authority's public-key infrastructure (PKI) certificate policy requirements** into the European Qualified Certificate Policy (TR 102 458). ETSI electronic signature activities focus on procedures for handling advanced electronic signatures on digital accounting and electronic signatures applied to registered emails.

More information is available at www.etsi.org/pressroom/Previous/2006/2006_10_esi.htm.

Teledensity has more than doubled in the most **underdeveloped countries** since 2000, according to a recently released **International Telecommunications Union (ITU)** report. The report, which examines key developments in information and communications tech-

nology, trends, and challenges from 2001 through 2005, says that connectivity has increased in some of the world's poorest countries by as much as 20 times, due mostly to the rapid growth in mobile technology deployment. According to the ITU's report, *ICT/Telecommunication Development in Least Developed Countries (LDCs)*, 25 of the 50 least-developed nations have met the teledensity targets set by the Brussels Programme of Action, a decade-long project launched in 2000.

More information is available at www.itu.int/newsroom/press_releases/2006/16.html.

"Geek spam" — email that uses technology-related keywords to both dupe tech-sector employees and pollute their Bayesian filters — is on the rise according to **MessageLabs'** third-quarter 2006 *Intelligence Report*. The report noted that spammers are increasingly using targeted-keyword techniques to penetrate particular industries. The report also noted a sharp increase in **phishing attacks**, which accounted for half of the malicious emails that MessageLabs intercepted in September, as attackers have switched their focus to financial institutions that haven't implemented two-factor authentication security.

More information is available at www.messagelabs.com/publishedcontent/publish/about_us_dotcom_en/news_events/press_releases/DA_173629.html.

way down to provider-equipped residential broadband data/voice modems, which would undoubtedly add more cost and complexity to the industry's CALEA compliance mandate. Zfone, on the other hand, being an end-user controlled technology, might be exempt from CALEA.

On his Web site, Zimmermann says:

"I'm not a lawyer, but it's my understanding that the Communications Assistance for Law Enforcement Act applies to the PSTN phone companies and VoIP service providers, such as Vonage... [Zfone] does all its key management in a peer-to-peer manner, so the service provider does not have access to any of the keys. Only the end users are involved in the key negotiation. CALEA does not apply to end users."

Parsing the legal as well as the technological issues will become critical fairly soon for a wider variety of enterprises. According to In-Stat data from the first quarter of 2006, VoIP technology cracked the 50 percent barrier in businesses with 500 to 999 employees in multiple areas: IP-PBX, broadband voice and collaboration applications, and P2P. Even a third of the largest businesses surveyed had deployed some P2P telephony somewhere in their organization. In-Stat analyst Fodale says stakeholders across the board must begin a concerted education campaign to bring the full complexity of VoIP security to light.

"You need to broaden the discussion," she says. "We need to be looking at use cases — does this serve more than the niche looking to keep their communications from government surveillance? You can say that there is definitely a need for this technology for people working in areas where they cannot trust the communications infrastructure — but I think this is much broader — and I hope the discussion gets larger." □

Greg Goth is a freelance technology writer based in Connecticut.

of technical guidance and the potential to have to add more back doors — hardware and software that offers no revenue potential — every time they expand their infrastructure.

VoIPSA's Endler says the very nature of packet-based communications might make the expensive CALEA provisions moot given the Internet's global architecture.

"The infrastructure in which the PSTN routes calls has a definite geographical architecture," he says. "If

you want to look at data from a PSTN-carried call, you know exactly where it originated because of the path it took. But something like Skype comes from the P2P model, and that's not as clear cut. A call can originate in the US, travel outside, and come back in. The Internet doesn't have any geographic boundaries, so that will be interesting to see how that plays out."

On the other hand, the definition of "facilities-based" might extend all the