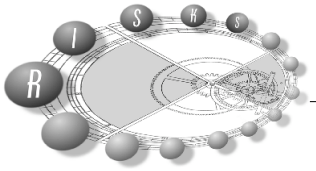

The Real National-Security Needs for VoIP

In August 2005 the Federal Communications Commission announced that the Communications Assistance for Law Enforcement Act (CALEA) applies to broadband Internet access and "interconnected voice over IP" (VoIP). VoIP *providers* already had to comply with legally authorized wiretap orders; the FCC ruling means that all VoIP *implementations* would now have to pass federal wiretapping standards before they could be deployed. This is not merely a hair-splitting distinction of concern only to telephone companies; in essence, this new ruling places the FBI in the middle of the design process for VoIP protocols and products.

Those who think the new FCC ruling will affect only the U.S. are mistaken. After CALEA (which requires that digitally switched telephone networks be built wiretap-enabled) became law in 1994, the FBI pressedother nations to adopt similar legislation. Digital-switching technology sold in the U.S. telecom market must comply with CALEA, thus effectively forcing much of the rest of the world to adopt CALEA access interfaces.

There were objections to the ruling from many quarters: civil-liberties organizations, Internet providers, and the computer industry. Although CALEA applies to services that provide a "replacement for a substantial portion of the local telephone exchange service," there is currently a clear exemption for the Internet. It is likely that the FCC ruling will be challenged in court. If, as some expect, the FCC ruling is overturned, the FBI is likely to seek Congress's help in expanding CALEA to include VoIP.

CALEA applied to VoIP might simplify the FBI's efforts to conduct legally authorized wiretaps (although the FBI has not disclosed any instances in which it has had difficulty conducting VoIP wiretaps). However, applying CALEA to VoIP would necessitate introducing surveillance capabilities deep into the network protocol stack. The IETF considered such a surveillance protocol five years ago in RFC 2804, and concluded that it simply could not be done securely. Networks have become even more fragile since then.

Over the last decade, the Internet has proven irresistible to business; it and private networks using Internet protocols are now used to control much of the world's critical infrastructures. The vulnerabilities inherent in the Internet put vital assets at risk. In the wake of September 11 and the Madrid and London bombings, protection of such infrastructure has taken on a new urgency. Introducing surveillance capabilities into Internet protocols is simply dangerous, the fundamental problem being that designing and building secure surveillance systems is too difficult.

It might be argued that the surveillance technology can be built securely and without risk of penetration by hostile forces. The track record is not encouraging. Even organizations considered in excellent positions to prevent penetration have been vulnerable. A number of U.S. Government agencies, including the Defense Department and the Department of Justice, have been successfully attacked.

It is possible to write better software, even with the limited state of the current art, but the processes still aren't foolproof. For example, avionics software (which is held to a very high standard and is not expected to deal with Internet attacks) is not immune to critical flaws.

With CALEA, incentives work against security. VoIP companies are unlikely to pay for high-assurance development; they don't rely on the proper function of wiretapping software in their normal operations. The software won't be available to many friendly eyes that might report bugs and holes. Instead, the likely targets of wiretaps—organized crime and foreign and industrial spies who would want to subvert the monitoring capabilities for their own ends—would most certainly not disclose any holes that they find.

Given this, how likely is it that ISPs will be able to secure their surveillance and remote monitoring capabilities from attack and takeover by hostile agents? Not imposing CALEA on VoIP does *not* mean that law enforcement will be helpless to wiretap VoIP. Instead it means that wiretapping will be accomplished at either the application layer (by the VoIP provider) or the link layer (by monitoring the target's network connection), rather than from functions embedded more pervasively across the network stack.

In the debate over cryptography policy, several nations (including the U.S. and France) wisely concluded a decade ago that weakening Internet security in the hope of occasionally helping law enforcement was a bad trade-off. Extending CALEA to VoIP would be a dangerous step backward. C

PAUL WATSON

Steven M. Bellovin (smb@cs.columbia.edu) is a professor of c o m puter science at Columbia University. **Matt Blaze** (mab@crypto.com) is an associate professor of computer and information science at the University of Pennsylvania. **Susan Landau** (susan.landau@sun.com) is a Distinguished Engineer at Sun Microsystems.