Stephen M. Bellovin, Matt Blaze, Whitfield Diffie, Susan Landau, Jennifer Rexford, and Peter G. Neumann

Internal Surveillance, External Risks

Building surveillance technologies into communications networks is risky. Two years ago, Greece discovered that legally installed surveillance software in a cell phone network had been surreptitiously activated by unknown persons: over 100 senior members of their government were tapped for almost a year. Things were no better in Italy, where a number of employees at Telecom Italia were arrested for illegal wiretapping (with attempts at blackmail). In the U.S., recently released documents show that an FBI-designed communications interception system has security problems—difficulty providing auditing, relying on passwords rather than token-based or biometric authentication, having no unprivileged user ids—leaving the system potentially vulnerable to insider attack.

Although we focus here on U.S. legislation, the security and privacy risks are global. For example, consider the Protect America Act (PAA), the August 2007 wiretap law updating the 1978 Foreign Intelligence Surveillance Act (FISA). FISA permitted warrantless interception of radio communications traveling outside the U.S. if the communications didn't involve targeted "U.S. persons" (citizens, residents, or U.S. corporations). The value of the exemption comes from the U.S. role as a hub: communications from other continents often transit the U.S. This role has been a real boon to the National Security Agency (NSA), the U.S. signals intelligence organization.

In recent years, however, cable has broadly replaced satellites. NSA pressed for broadening the radio exemption, arguing it had become inadequate. The PAA went significantly further, allowing warrantless wiretapping whenever one end of the communications is "reasonably believed" to be outside the U.S. Beyond eliminating the delays associated with warrants, the PAA arguably allows using the communication carriers' transactional data, including histories for real-time determination of interception targets.

Determining the origin of a communication in real time is not always easy. Locating the source of a phone call depends on the accuracy of information from the remote phone switch, but technologies such as VoIP and PBXs may alter the data. An Internet address reveals neither a computer's geographic location nor the user's identity, and techniques for inferring the rough location are not always accurate. While most calls outside the U.S. involve foreigners talking to foreigners, most communications within the U.S. are constitutionally protected U.S. persons talking to U.S. persons. Any surveillance system built to satisfy the new law (or later amended versions) increases the chances that communications of U.S. residents will be inadvertently collected.

PAUL WATSON

When you build a system to spy on yourself, you entail an awesome risk. By building a communications surveillance system itself—and saving its enemies the effort—the U.S. government is creating three distinct serious security risks: danger of exploitation of the system by unauthorized users, danger of criminal misuse by trusted insiders, and danger of misuse by government agents. How can these risks be mitigated?

Minimization matters. An architecture that minimizes the collection of communications lowers the risk of exploitation by outsiders and exposure to insider attacks. Collect traffic at international cableheads rather than at tandem switches or backbone routers, which also carry purely domestic traffic. Regardless of where communications are intercepted, collected traffic could be subjected to multiple tests to determine whether its source and destinations are inside the U.S., and, if so, discarded before any further processing is done.

Architecture matters. Using real-time transactional information to intercept high volume traffic makes architectural choices critical. Robust auditing and logging systems must be part of the system design. Communication providers, who have technical expertise and decades of experience protecting the security and privacy of their customers' communications, should have an active role in both design and operation. "Two-person control"—control by two authorized parties who know how the system should work—is as applicable to organizations as to individuals.

Oversight matters. The new system is likely to operate differently from previous wiretapping regimes, and likely to be using new technologies for purposes of targeting wiretaps. There should be appropriate oversight by publicly accountable bodies. While the details of problems may remain classified, there should be a publicly known system for handling situations when "mistakes are made."

Surveillance built into communications networks must include minimization, robust controls, and oversight into system design. Otherwise, Trojan horses could threaten the central nervous systems of entire nations, where the threats to citizens' security and privacy could be immense. C

This column is based on a paper by the named authors, *Risking Communications Security: Potential Hazards of the "Protect America Act"* (http://crypto.com/paa.pdf).