Security Risks of the Protect America Act

by Steven M. Bellovin (Columbia University), Matt Blaze (University of Pennsylvania), Whitfield Diffie (Sun Microsystems), Susan Landau (Sun Microsystems), Peter G. Neumann (SRI International), and Jennifer Rexford (Princeton University)

The Protect America Act passed in August 2007 changes U.S. law to allow warrantless foreign-intelligence wiretapping from within the U.S. of any communications believed to include one party located outside the United States. U.S. systems for foreign intelligence surveillance located outside the United States minimize access to the traffic of U.S. persons by virtue of their location. The new law does not. Many have expressed civil-liberties concerns over this change to FISA; our focus is on the security risks this law introduces, and whether it puts Americans at risk of illegitimate surveillance by criminals, terrorists, and other governments.

Technical Issues

Monitoring international traffic requires an effective way to identify whether the communication starts or ends outside the United States. This aspect of the PAA arguably changes the rules on using Call Detail Records (CDRs).

- Call Detail Records: CDRs are records of such transactional information as calling and called numbers for phone calls, IP addresses and user URI in the case of VoIP, SMTP headers for email, etc., time and date of communications, etc., and can be surprisingly revelatory of relationships and organizational structure. CDRs can, in particular, be used for targeting further surveillance, i.e., wiretapping.

- Limitations: Yet even though CDR is an amazingly effective guide to to communications activity, the data can't always provide real-time answers to the location of a call. Doing real-time location of communication endpoints is a surprisingly difficult problem to solve, both on the telephone network and on today's Internet.

- Why is Determining Location so Hard?: Location of the source of a phone call is dependent on the remote phone switch telling the truth. Technologies such as VoIP and PBXes mean that one cannot assume that. An Internet address does not reveal a computer's geographic location, or the identity of the user, and techniques for inferring the rough location are not always accurate.

- Consequences: (i) With real-time access to CDR, NSA could conceivably learn of a call in progress in time to intercept the content. Thus real-time CDR could be used to target which people to wiretap and then do so without a court order; the more tightly-coupled CDR and content collection are, the more likely it is that content wiretapping will occur as a result of CDR information. (ii) This information will undoubtedly pick up purely domestic communications as well.

Risks

The change from a system that wiretapped particular lines upon receipt of a wiretap order to one that sorts through high-speed transactional data in real time and selects communications of interest is massive. Can such a selection process be built securely without risking exploitation of U.S. communications by others? We see a number of serious risks that need to be addressed.

Risk 1: Risks of exploitation by opponents: A system that is accessing domestic communications necessarily poses greater direct risks to communications of Americans than a surveillance system that is fielded overseas. While it was undoubtedly the case that, even prior to the PAA, U.S. systems were vulnerable to surveillance, building surveillance systems costs money. The system is designed as a result of the PAA should not provide an easier way for foreign powers to gain access to U.S. communications.

Risk 2: Removal of safeguards by communications carriers: Previous approaches to foreign intelligence surveillance of U.S. persons went through the communications carriers, who combine technical expertise regarding communication with responsibility for their customers' security and privacy. Leaving a single entity in charge of selection and retention decisions provides no recourse in cases where 'mistakes were made."

Risk 3: Lack of inherent technical minimization of traffic: Intercepting at switches creates unnecessary risks because the switches handle domestic as well as foreign communications.

Risk 4: Remote control of filters; Who controls the filter? Is NSA designing sufficiently robust mechanisms to assure complete control?

Risk 5: Domestic traffic entering the NSA collection system: It is likely that the current surveillance architecture filters out most "US-person traffic" before such traffic gets to NSA headquarters at Fort Meade. Does the design of the expanded surveillance system take into account that much of the traffic entering the NSA system will be purely domestic?

Risk 6: Large attack surface: Because of the likelihood that similar NSA systems are being deployed around the globe, it is likely that the system design is well known. Thus risks include the ability by various enemies to modify content capable of evading the NSA's controls, thus reducing the value of the surveillance system — and increasing the risk of even further surveillance down the road.

Risk 7: Call Detail Record information: It is a truism in the security field that problems frequently occur when new uses are found for an old system, since the protection mechanisms and system architecture were never designed for such uses. Will new vulnerabilities be created when copies of this data are sent to law enforcement or intelligence agencies? It is impossible to give a definitive answer, but the past history of such changes do not leave us sanguine.

Security risks will be exacerbated by the direction of the Internet's future evolution. While the current Internet may look large, it only has millions of devices connected to it; the Internet is moving to a situation in which billions of resource-limited small devices such as radio-frequency ID (RFID) tags and sensors will use the network for communicating. Many of these devices will be on local-area networks, but others will make use the Internet. Any future surveillance architectures must take such growth and directions into account.

Recommendations

The Protect America Act, a law quickly proposed and enacted, potentially vastly increases the number of Americans whose communications and communication patterns will be studied. This sets up access to U.S. communications, a target of great value. The nation may build for its opponents something that would be too expensive for them to build for themselves: a system that allows them to see the intelligence interests of the U.S., a system that may tell them how to thwart those interests, and a system that might be turned to intercept the communications of American citizens and institutions. It is critical that the new surveillance system neither enable exploitation of U.S. communications by unauthorized parties nor permit abuse by authorized ones.

Minimization is critical. Allowing collection of calls on U.S. territory, necessarily entails greater access to the communications of U.S. persons; the architecture must minimize collection of both the call details and the content of these communications. The best way to prevent problems is to intercept as early as possible: at the cableheads; such a solution, by decreasing the number of interception points will simplify the security problem. Surveilling at the cableheads will help minimize collection but it is not sufficient. Intercepted traffic should be studied (by geo-location and any other available techniques) to determine whether it comes from non-targeted U.S. persons and if so, discarded before any further processing is done.

The architecture should be developed in collaboration with the communications carriers, organizations with long experience of responsibility for the privacy and security of their customers' communications. That responsibility should *not* be removed from the communication providers.

Oversight is necessary to prevent abuse and ensure information assurance. Independent oversight of operations is also essential and is a fundamental tenet of security. To assure independence the overseeing authority should be as far removed from the intercepting authority as practical.

To guarantee that electronic surveillance is effective and free of abuse *and* that minimization is in place and working appropriately, it is necessary that there be frequent, detailed reports on the functioning of the system. Of particular concern is the real-time use of CDR for targeting content, which must neither be abused by our own government nor allowed to fall into unauthorized hands. For full oversight, such review should be done by a branch of government different from the one conducting the surveillance. We recommend frequent ex post facto review of the CDR-based real-time targeting.

The oversight mechanism must include outside reviewers who regularly ask, "What has gone wrong lately — regardless of whether you recovered — that you have not yet told us about?"

Security of U.S. communications has always been fundamental to U.S. national security. The surveillance architecture implied by the Protect America Act will, by its very nature, capture some purely domestic communications, risking the very national security that the act is supposed to protect. In an age so dependent on communication, the loss may be greater than the gain. To prevent greater threats to U.S. national security, it is imperative that proper security — including minimization, robust control, and oversight — be built into the system from the start.