CALEA Was a National Security Disaster Waiting to Happen

Jordan Schneider ⋮ 26-33 minutes

One never wants to be in an "I-told-you-so" position when a national security crisis comes to pass. And yet that is exactly where my cybersecurity colleagues and I now find ourselves. In October, the Wall Street Journal reported:

> A cyberattack tied to the Chinese government penetrated the networks of a swath of U.S. broadband providers, potentially accessing information from systems the federal government uses for court-authorized network wiretapping requests.
>
> For months or longer, the hackers might have held access to network infrastructure used to cooperate with lawful U.S. requests for communications data, according to people familiar with the matter.

The damage from such an exploit cannot be overstated. During 2011 testimony before Congress, I noted:

> When a Lockheed Martin or a Northrop Grumman fails to adequately secure its networks, the cost can be thousands of proprietary files stolen. But if a communications provider, an applications provider, or a switch provider fails to have an adequately secured communications system, that cost occurs over the millions of communications that utilize that switch or application.

The Wall Street Journal reported that the information potentially accessed was "wiretapping requests"; the article does not indicate that the communications themselves were compromised. But for counterintelligence purposes, U.S. wiretapping orders provide the exact information China wants—including which of their agents have been exposed by the U.S. government and which ones remain unknown. The Chinese government will also have learned which Russian, Iranian, and other agents have been revealed, so U.S. intelligence will have to assume that that information is also compromised. If Chinese hackers have indeed accessed the court-ordered wiretapping requests, we have an intelligence failure roughly on par with putting Kim Philby in charge of the FBI's Russia counterintelligence office.

Although the Journal article does not explicitly say so, the breach almost certainly occurred as a result of the Communications Assistance for Law Enforcement Act (CALEA). This 1994 law was intended to give law enforcement wiretapping capabilities as digital switching technologies were making older methods obsolete. Previously, if a spy used a wireline phone, alligator clips—or the equivalent—at the local phone exchange provided law enforcement access under a wiretap order. But new technologies introduced in the 1990s—digital switches that enabled such services as call forwarding, ISDN, a standard that enabled multiple simultaneous digital transmissions of different kinds of content (voice, video, data, and other network services) over the Public Switched Telephone Network (PSTN), and cellular service—couldn't be wiretapped that way.

CALEA's Genesis

Law enforcement's solution was to require that telephone service providers build wiretapping capabilities into modern telephone switches and retrofit existing systems to do the same. This was CALEA.

At the time of CALEA's passage, communication networks were in transition. Landlines were still the main mode for telephone calls; only nine in 100 Americans were using mobile phones. The internet had not been opened to commercial traffic. Apple was more than a decade away from introducing the iPhone.

The FBI put forth a "Digital Telephony" proposal in 1992, which telephone service providers and civil liberties groups killed. Law enforcement tried again two years later with a bill that contained a sweetener of $500 million in funding for converting old switches to be CALEA-compliant. But the money turned out to be well below the costs of retrofitting the systems, resulting in multiple court fights.

As CALEA was being debated in Congress in 1994, David Farber, who served as FCC chief technologist in 2000-2001, highlighted security risks in testimony before the House Subcommittee on Technology, Environment, and Aviation:

> The complexity of just the Plain Old Telephone System software is enormous. Re-designing large and often the most complex parts of it will not be easy nor inexpensive. One must potentially re-engineer the cellular system with its multiple manufacturers plus the local and toll and tandem switching centers. The fact that they are programmed devices makes it feasible but not cheap. The potential for decreased reliability of the national telephone grid caused by the large scale changes (presently undefined) to the software architecture could cause major dangers to the health and economy of the country. If you watch the bugs (errors) that are distributed in well tested and much simpler systems (like DOS or MACOS) you can appreciate the opportunities for chaos—and it must be done in three years.

Farber's concerns focused on redesigning the PSTN to accommodate CALEA. For most of the past century, the U.S. public phone network was a regulated monopoly run by AT&T. AT&T's security *was* the PSTN's security, which involved securing and monitoring all switching and routing facilities, transmission security, and separating communications content from communications control (the signaling information). By the 1990s, the PSTN was no longer Ma Bell, but many companies, not all of which were as attentive to security. The fledgling cellular system also provided extensive challenges—it's a lot harder to secure cell towers than brick-and-mortar telephone local exchanges.

But there were even greater security threats looming.

The PSTN and the Internet: Different Approaches to Security

In 1994, authenticating providers and users was easy. In those days, the PSTN consisted of a limited number of known service providers. The communication endpoints—the phones—were "authenticated" because the network needed that information to bill for

calls.

The internet is different. In part, this is because the networks were not originally designed to perform user identification. The failure to authenticate also provides an important feature: anonymity. The internet is a network designed to share information, and government sites, libraries, and other organizations seek to provide information without requiring users to identify themselves.

As long as the PSTN and the internet were separate, the different security models of the two networks might not have presented problems to the PSTN's security. But in the 1990s, internet users began connecting to the phone network in ways PSTN designers had not anticipated.

In 1997, one such incident led to the first case in which critical infrastructure—a regional airport in Worcester, Massachusetts—was shut down because a teenage hacker on the internet accessed a NYNEX phone switch in central Massachusetts. The switch, built under the assumption that only authorized parties would have access, did not require authentication. The teenager hacked the switch and corrupted information, disabling access to the Worcester airport. Consequently, the airport's main radio transmitter and control tower could not communicate, requiring that the airport be shut down for six hours. The problem itself was relatively minor; the Worcester Regional Airport is not heavily used. But the incident, apparently the first critical infrastructure attack in the U.S., illustrates the security problems of interconnecting the PSTN and the internet.

Adding wiretapping to a telephone switch creates an architected security breach. CALEA had a requirement about protecting the wiretapping systems' security (Section 301(b) of the statute). So in 1997, the American Civil Liberties Union, Electronic Privacy Information Center, and Electronic Frontier Foundation presciently filed objections to CALEA being implemented before "industry security procedures are determined." That didn't happen. Instead, development of CALEA wiretapping requirements proceeded apace.

CALEA's Reach Expands and Security Risks Increase

During 1994 congressional testimony on CALEA, FBI Director Louis Freeh was very clear that the law applied only to telephony and would not extend to the nascent internet. Thus, CALEA specified that the capability requirements did not apply to "information services"—that is, the internet. That proscription didn't last long. In 2003, the FBI pressed to extend CALEA to Voice over IP (VoIP)—phone calls made over the internet. Two years later, the Federal Communications Commission (FCC) agreed to do so for broadband access providers and providers of VoIP services that could connect to the PSTN.

Industry and civil liberties groups went to court. In a two-to-one decision, the U.S. Court of Appeals for the D.C. Circuit concurred with the FCC. Calling the decision "gobbledygook," the dissenting judge told his colleagues to read the law.

From a technical vantage point, extending CALEA to this type of VoIP was relatively easy because the VoIP user was connecting to the phone network from a predetermined location; this simplified knowing where to place a wiretap. From a security vantage point, it was now putting wiretapping capability right at switches connecting the PSTN and an internet service provider (ISP).

Steve Bellovin, Matt Blaze, and I objected:

> 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.

We weren't the only ones expressing such concerns. In 2007, the Electronic Frontier Foundation (EFF) raised security concerns about CALEA increasing the vulnerability of internet communications:

> EFF is also concerned that making the Internet CALEA-compliant might backfire: many of the technologies currently used to create wiretap-friendly computer networks make the people on those networks more pregnable to attackers who want to steal their data or personal information.
>
> When broadband service providers are forced to make their networks or applications tappable, this introduces more points of vulnerability into the system. ...
>
> Ultimately, all of these problems can be traced back to a single root cause: CALEA was drafted specifically to regulate phone networks, which are designed to be closed systems. The Internet is an open, global system that handles countless forms of data-transfer and accommodates an ever-changing array of smart edge-devices. If CALEA is misapplied to the Internet, the results will be disastrous.

The integration of PSTN and internet communications was already occurring. One example is Apple's iMessage, which can be a purely internet communication or a PSTN-mediated one (that is, an SMS). Another is E911 services. E911 connects callers to local emergency services. Consumers were replacing home PSTN lines with VoIP, seeing the two messaging systems as interchangeable. They are not. Connecting a caller with emergency services in their location had been easy for landlines, since the service provider knows the phone's address and passes the information along. With VoIP, the caller has an IP address, not a phone number. ISPs are competitors to the

phone companies, which had a competitive advantage in being able to serve E911 calls while VoIP systems ran into trouble

After a number of times when consumer calls to E911 using VoIP failed to connect the caller with local emergency services, Congress intervened, requiring telephone companies to provide VoIP services the same interconnection capability to E911 services as cellular calls had. This made a great deal of sense from a public safety vantage point but created another interconnection between the two networks. The two networks were increasingly intertwined, simplifying hackers' ability to access phone company control systems.

A Short Intro to the Security Risks of Modern Telephony

Hacking telephone company systems—that is, breaking into the systems operating the dialing, routing, addressing, and signaling—did not start with this recent Chinese effort. The classic case is the 1960s blue-box attacks. Phone signaling—handset off the receiver (the signal to the phone company that a user was about to make a call), numbers dialed, call over—all traveled over the same channel as the voice communication. In the 1960s, some enterprising hackers found that the whistles given away as prizes in Cap'n Crunch cereal generated a 2600 Hz tone, exactly the frequency that the phone company used to signal a call's completion. A generation of young hackers used this to fool the phone system into charging 800-numbers for calls that were placed to other numbers.

Separating signaling from the actual communication should—in theory—have solved the problem. Modern telephony has two channels: the Call Data Channel (CDC) for phone signaling (e.g., phone engaged, call coming in, call ended) and the Call Communication Channel (CCC) for voice and other types of communications content. CDC sets up the call, which is then transmitted over the CCC. A "hanging up" signal on CDC ends the call.

But in practice, law enforcement requirements post-CALEA broke the clear separation between the CDC and the CCC. Sometimes digits are dialed after the call has been connected. These can be prescription numbers for a pharmacy or money transfer information to a bank—clearly content—or they can be providing a phone number to a long distance service for dialing the number the user wishes to call (these services, popular in the 1990s, lowered customers' long distance costs). The latter qualifies as call data even though it is transmitted on the CCC.

In the 1980s, phone companies were converting their electromechanical switching systems to computer-controlled ones. As the New York Times reported at the time:

> As a result, personal computer experts, often called "hackers," can illegally connect their personal computers to the phone network. With the proper commands, these intruders can eavesdrop, add calls to someone's bill, alter or destroy data, steal facsimile documents being transmitted, have all calls to a particular number automatically forwarded to another number or keep someone's line permanently busy.

One of those "experts" was Kevin Poulsen, who wiretapped databases held by PacBell. He was one of the first hackers to be charged with espionage.

A phone tap requires a connection from the CCC to the tapper. In 1930s film noir, you can see the tapper putting alligator clips on the line. In 1980s technology, for every tapped call, there was a phone line being tapped to the law enforcement office. Phone companies stored databases for every tap as well as for any line that had a pen register or trap-and-trace device. These databases were at phone company "work centers"; there were a few per city.

CALEA appears—and I emphasize "appears," as no technical details have been forthcoming—to have made this type of hacking easier in several ways.

First, the government regulations for implementing CALEA allows delivering the CCC and CDC data over the internet rather than, as originally specified, over leased lines. The latter were much more easily secured.

Second, automation has largely removed humans from the loop. It is easier to hack a system than to find a phone company insider and "hack" them.

Third, unlike the old landline model in which wiretap orders were localized, CALEA has resulted in more centralized storage of interception orders. While lawful intercept systems may be implemented differently, the warrant status of a user of a mobile phone is included in the Home Location Register (HLR), the carrier's subscriber database.

The HLR, which carries information about hundreds of thousands of subscribers, stores such data as the user's Mobile Subscriber ISDN Number (MSISDN), International Mobile Subscriber Identity (IMSI), the services to which the user is entitled (e.g., SMS), the user's current location, and support for roaming. The last means that when a user is roaming and seeks to make a call, send a text, or use other services, the roaming carrier's Visitor Location Register (VLR) will check status with the user's HLR to ensure the requested services are within scope of the user's subscription. This is when the carrier supporting the roaming visitor will learn of the court order and, thus, institute the interception.

Fourth, because CALEA is complex to implement, there are now intermediary service providers that sit between wiretap delivery systems and different law enforcement agencies (e.g., state and various federal ones, including the FBI, the Drug Enforcement Agency). The existence of these services simplifies implementing CDC and CCC delivery for small and medium telephone services. Given that a number of carriers appear to have been compromised, it is possible that some or one of these intermediary services was the source of the original compromise.

There are many issues to chew on here. Opening the telephone network to ISP access made it almost certain that serious hacks were likely to occur. Automation of the wiretap process from the time that Poulsen accessed PacBell's wiretap databases makes it easier to infiltrate a larger pool of wiretap orders.

That such an attack could occur should have been expected. Not only had researchers and civil society organizations warned of the theoretical possibility, in 2005 Blaze and his students showed various vulnerabilities in wiretapping systems; these systems did both

communications interception and signaling collection (pen register and trap-and-trace). Taking advantage of the fact that built-in tolerances for reading dialed signals vary by manufacturer, the researchers showed how to deceive pen registers about numbers that were being dialed. They also showed that the wiretapping system could be tricked into thinking that no call was being conducted when in fact one was. What was even worse, however, was the fact that the standard for CALEA compliant switches, J-STD-025A, did not include authentication requirements for accessing the CDC or CCC.

In 2011, I met with the FCC to discuss threat modeling of CALEA switches. Threat modeling is a standard security technique for systematically security stress testing a system. I began by asking if FCC oversight of CALEA compliance included threat modeling. I then found myself in perhaps the strangest meeting of my professional career.

For the majority of our conversation, I simply couldn't make myself understood. Finally, just before the end, the FCC engineers and lawyers in the room said, "Oh my God, we never thought about this." Amazingly, although CALEA mandated and FCC enforced a security breach into telephone switches, the FCC had simply not considered requiring security testing of the switches.

The National Security Agency (NSA) had. Later that year, I spoke with Dickie George, who had been technical director for information assurance at the agency, about CALEA-compliant switches. He told me that when several large manufacturers submitted their switches to NSA for testing—a requirement if the switches were to be used by the Department of Defense—the agency found there were security problems with *every* switch that NSA tested. George did not comment on the switches that NSA had not tested; the implication—their probable lack of security—was nonetheless clear.

The Chickens Come Home to Roost

The dangers we all feared came to pass. One well-known example—occurring long before the most recent Chinese hack— was the Athens Affair. The private communications of 100 senior members of the Greek government, including the prime minister, the head of the opposition, and the heads of the Ministry of Interior and Ministry of Defense, were wiretapped for 10 months. Wiretapping was done through rogue software implanted on a switch with a wiretapping interface designed to satisfy European Telecommunications Standards Institute (ETSI) specifications. That interface was modeled on CALEA requirements.

In 2010, examining public Cisco specifications for an IP network wiretapping architecture based on ETSI standards, IBM researcher Tom Cross found multiple security problems. Among others was a red-hot one: The system permitted unauthorized people to intercept communications.

And in a precursor to the Wall Street Journal article, in 2013 the Washington Post reported that "Chinese hackers who breached Google's servers several years ago gained access to a sensitive database with years' worth of information about U.S. surveillance targets, according to current and former government officials." Yet CALEA endured.

By 2016, the intelligence community was aware of intrusions similar to the Athens Affair. And now we have the report of the likely collection by Chinese hackers of U.S. wiretap targets, an intelligence loss that will reverberate for years.

From a policy point of view, what went wrong is unfortunately easy to explain. Law enforcement's focus was on accessing communications when authorized with a court order. They thought a little about adversaries thwarting the new wiretapping services but were concerned primarily with the organized criminals and drug dealers of the 1990s, not the far more skilled "professional" criminal and state hackers we face today. Meanwhile, service providers were in a highly competitive market (Voice over IP, new players in the telecommunications market) and facing a very different adversary: a nation-state intent on accessing their systems. These are sophisticated adversaries, ones with time and increasing capabilities on their side.

What's the Solution?

There's no putting the secrets China stole back into the safe. If the database of surveillance targets was indeed accessed by Chinese hackers, they are gone, and this will have long-term national security impacts on the U.S. The real question is how to avoid recurrences.

Sen. Ron Wyden (D-Ore.) wrote to FCC Chairwoman Jessica Rosenworcel and Attorney General Merrick Garland to recommend four actions:

- The FCC should institute rulemaking to ensure that CALEA regulations fully implement the system security required by law.
- Rather than indicting foreign conspirators who hack U.S. systems, the Department of Justice should, through a combination of carrots and sticks, focus on holding U.S. companies liable for failures in security.
- The Justice Department should stop seeking backdoors in communications technologies.
- The Justice Department should investigate whether the companies involved in the Wall Street Journal breach were broadly negligent in their cybersecurity responsibilities, not just in the wiretapping systems.

It should be no surprise to readers of my articles that I am strongly against communications backdoors. I am less convinced of the efficacy of Senator Wyden's other recommendations. While I agree that holding U.S. companies liable for security failures is an important aspect of increasing the nation's cybersecurity, I don't hold with halting the indictment of foreign nationals. Indicting foreign hackers of U.S. systems is less about criminal convictions than it is about influencing international law and norms; I believe that the Justice Department effort has value in a number of ways. And though I understand the spirit of the first and fourth of Wyden's recommendations, I believe these needs should be constituted quite differently.

Wyden's first recommendation is that rulemaking to ensure that CALEA regulations fully implement the system security should be required by law. As I learned in 2011, the FCC did not even appear to be fully aware that it should be ensuring CALEA-compliant systems were secure. And this was after the paper by Blaze and his students, the Athens Affair, and Tom Cross's discovery of security flaws in the Cisco implementation of equivalent European standards.

There are a number of technical requirements that could be placed on CALEA-compliant systems—for example, the design specification should maximize separation between the control management software and other applications; hardware tokens should be used for user

authentication; and two parties should be required to enable access to the systems. (I go into these and related recommendations in greater detail here.) Such technical requirements are part of a needed change.

But rulemaking is only one aspect of improving the security of mandated communication interception systems. What is really necessary is that such systems be stress tested *before* being put into use—and *while in use*. After the Chinese cyber exploit of Google systems in 2010, the company went about remaking its security posture. One crucial aspect was red teaming: using in-house engineers to attempt to break into Google's systems from the outside (the name and effort were adopted from the military). This, and other proactive security technologies, have proved very useful in keeping Google's data and software secure.

Our society has become dependent on highly complex systems. We've done so without developing the societal or technical infrastructure to ensure these systems are secure. An NSA colleague once told me that on the internet "there's malice out there trying to get you. When you build a refrigerator, you have to worry about random power surges. The problem is that [internet] projects are designed assuming random failure rather than targeted attacks." Regulations and stress-testing are needed; funds would have to be allocated for this work. It's not cheap, but the failure to secure systems on which society depends will cost the U.S. far more in the long run.

So I don't disagree with Senator Wyden's fourth concern. But given the technical complexity of CALEA-type systems, I'd put my emphasis elsewhere. Indeed, here I would hand out a plaudit to the Biden administration, whose 2021 executive order on cybersecurity placed cybersecurity requirements on government contractors. This is a first real step in improving the security of our digital infrastructure. Although Silicon Valley continues to move fast and break things—rather than ensuring security in its products—the direction pursued by the executive order is very much needed. My vote is for using the power of the purse, as the administration was doing here, as a way of increasing the pressure on companies to move slower and make it harder to wreak havoc.

In 2016, as Apple and the FBI faced off over whether the government could force the company to undo security protections and unlock a terrorist's phone, an interesting cartoon hit the press. It showed the FBI getting into the unlocked phone—followed by hackers, other government agencies, foreign spies, cyber criminals, and terrorists. The public understood what the FBI had failed to recognize: If you build a system so that it is easy to break into, people will do so—both the good guys and the bad. That's the inevitable consequence of CALEA, one we warned would come to pass—and it did. It's now well past time to take action.

Acknowledgment: Thanks to Steve Bellovin and Matt Blaze for discussions about this piece and previous ones that led to numerous joint works on this issue.