
Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet

Steven M. Bellovin

`https://www.cs.columbia.edu/~smb`

Join work with Matt Blaze, Sandy Clark, Susan Landau



Once, Wiretapping Was Easy



Steven M. Bellovin

- The phone system was simple
- Tapping was simple
- Very little technology was needed



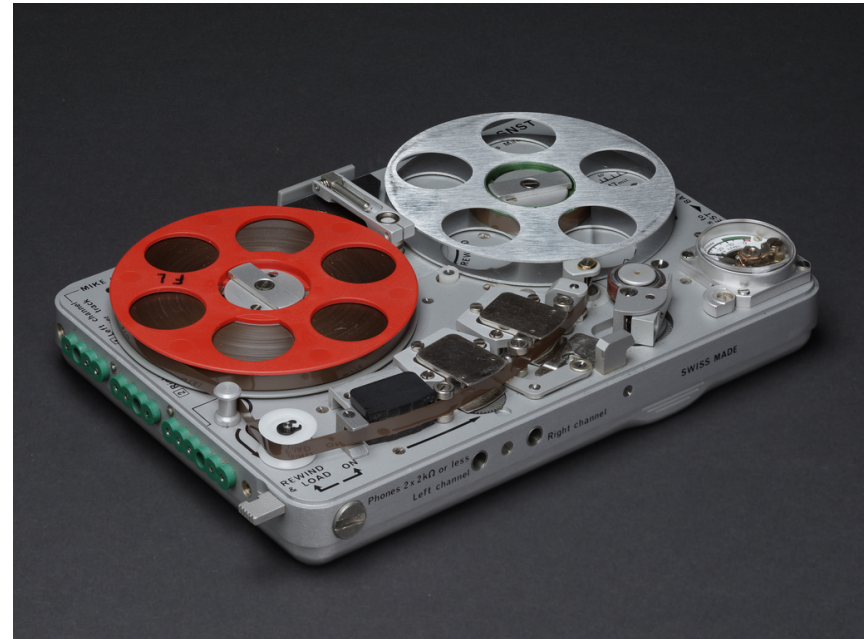
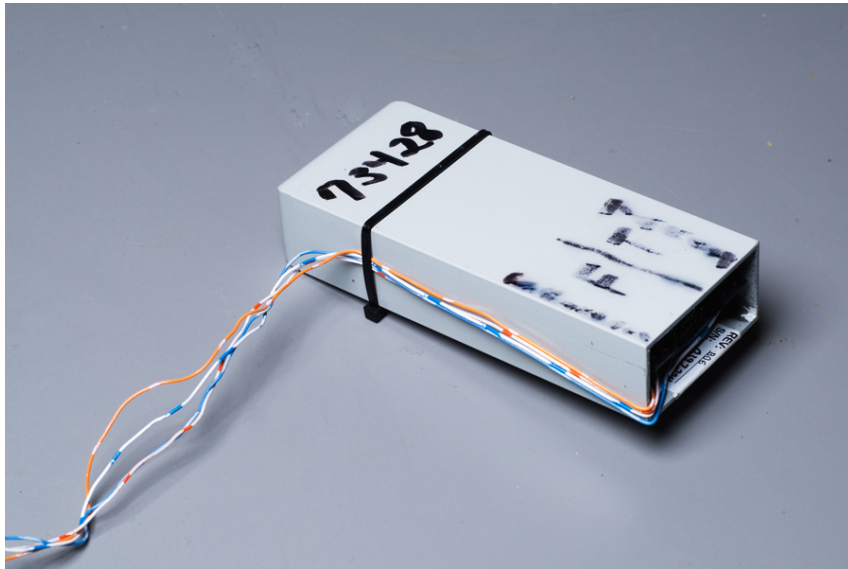
© Benjamint444:

[https://en.wikipedia.org/wiki/File:](https://en.wikipedia.org/wiki/File:Alligator_clips_444.jpg)

[Alligator_clips_444.jpg](https://en.wikipedia.org/wiki/File:Alligator_clips_444.jpg)

Steven M. Bellovin — October 4, 2013 — 2

The Modern Incarnation Isn't Much Harder



© Matt Blaze; used by permission

A Harbinger of Change



<https://en.wikipedia.org/wiki/File:WE1500D10buttonDSCN0217.JPG>

- Signaling could now be done after the call was set up
- Eventually, this gave rise to redialing services
- The original number dialed might not be the actual number of interest

Enter CALEA

- By 1992, the FBI saw problems coming
- They knew there were technologies they couldn't tap with simple tools
- They knew there were more changes coming
- They got Congress to pass CALEA: the Communications Assistance to Law Enforcement Act (1994)



https://en.wikipedia.org/wiki/File:Mobile_phone_evolution.jpg

CALEA

- All phone switches were required to have a standardized wiretap interface
- The technology was irrelevant; the switch handled the details
- The solution was rapidly copied around the world, under the generic name “lawful intercept”
- The law was intended to apply to local phone service only
- There were problems. . .



en.wikipedia.org/wiki/File:

[Cisco7960G.jpg](http://en.wikipedia.org/wiki/File:)

The Athens Affair

- The lawful intercept capability is a deliberate back door
- In theory, only authorized law enforcement agencies can use the capability
- But: phone switches are *computers*, and are hackable
- In Athens, someone—just whom isn't known—hacked a mobile phone switch
- About a hundred phones belonging to high officials, up to and including the prime minister, were tapped by abusing this mechanism (<http://spectrum.ieee.org/telecom/security/the-athens-affair/0>)
- The intercepts were relayed to prepaid phones located elsewhere in Athens

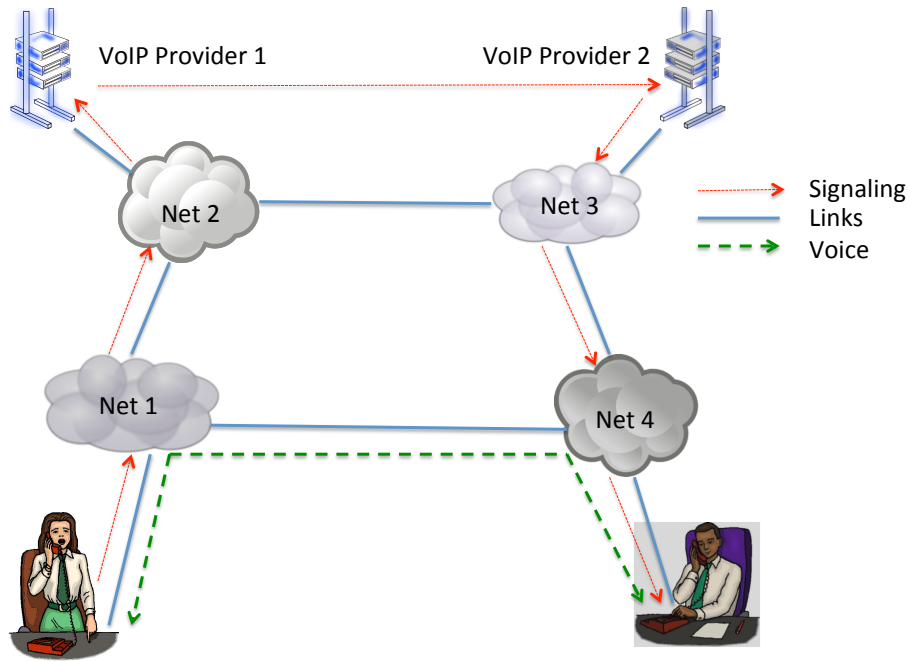
The Problem Isn't Greece

- *Every* CALEA-compliant phone switch tested by the NSA had security problems
- There was a larger (though less-publicized) abuse in Italy
- Some of the attacks on Google from China were intended to discover which users were the subject of wiretap orders
- There have been rumors that the Russian mob has hacked into CALEA interfaces in the US, to spy on law enforcement

Technology Changed Again

- Voice Over IP (VoIP) has a very different architecture than the authors of CALEA anticipated
- Skype was different still
- Many other means of communication sprung up on the Internet
- Should these be covered by CALEA? How?

VoIP Call Paths



- The signaling path is not the same as the voice path
- The “switch” may be in a different jurisdiction than the local Internet link
- Where can the CALEA tap go?

Skype is Stranger Still

- A peer-to-peer network
- There are *no* trusted phone switches
- Calls are routed through random other Skype users' computers (that's been changed of late by Microsoft)
- There is *nowhere* to place a tap interface

Other Communications Paths

- Email and IM
- Text messages in all their variants (Snapchat, anyone?)
- Voice communications in games
- Voice over IM systems
- More...

CALEA II

- For the last few years, the FBI has publicly advocated changes to CALEA to cover Internet services
- What they want is for *all* communications services to include a wiretap interface
- (No bill has been introduced yet, but they keep telling Congress they're "going dark")

Four Problems with CALEA-II

It won't (and can't) work:

- Attempting to make it work will drive up costs, hinder innovation, and cede the Internet service market to other countries
- How do you handle other countries' access requests?
- It creates security problems
- Other than that, it's a fine idea. . .

It Doesn't Work

- You can't put an overt back door into open source software; folks will just delete it
- End-to-end crypto defeats server-side solutions
- If run on end system clients, it may become easier for the target to notice the tap (though this can be done cleverly)
- Software can come from and/or be run in other countries

It Hinders Innovation

- CALEA-like laws are based on the implicit assumption that there is a more-or-less trusted place where you can tap all calls—which isn't true of peer-to-peer architectures
- Innovative designs may have no central servers
- Forcing small, innovative companies that are trying to ship on “Internet time” to add extra code will drive up their costs and slow down releases
- Developers in countries without such a law will thus have a competitive advantage

International Problems

- Which country should have access to a lawful intercept mechanism on a given computer?
- The US? The UK? France? India? Russia? China? The country in whose territory the target physically is?
- How do you enforce this?

It Creates Security Problems

- As noted, existing CALEA implementations are at best problematic
- This is code developed by sophisticated, skilled developers working for major phone switch vendors
- Furthermore, the problem they are trying to solve—tapping ordinary phone calls—is well-understood. It's much less obvious what it means to tap a new kind of service.
- Most developers are not security experts. Indeed, their own product-specific code will often have security problems, especially early on.

But other than all that, it's a fine idea...

Is There Even a Problem?

- Newer services create a vast amount of metadata
- Even Skype leaks IP addresses
- In fact, most people voluntarily carry location tracking devices, a.k.a. mobile phones
- Mobile phones are generally person-specific; law enforcement is thus more likely to capture the conversations of interest
- Cloud services (e.g., gmail) make preservation of data a priority
- Official statistics show that previous “serious threats”, such as encryption, have not turned out to be problems
- Most criminals use off-the-shelf tools and don’t do a particularly good job of covering their tracks

 Late-breaking news: look at the take-down of the Silk Road

Lawful Hacking

- Suppose there is a problem. What should law enforcement do?
- Proposal: Hack the endpoints
- Plant whatever wiretap software is needed on the target's machine
- Avoid all crypto issues: capture conversation before encryption or after decryption
- Perhaps install taps in the microphone or audio device drivers
- Or simply send out a very few packets with the session keys, encrypted with the FBI's public key

Huh? Hacking? By Law Enforcement?

- Is this legal?
- Can it be done?
- Will it lead to more security holes in our software?

Legality

- Lawful hacking is done today, under court order. In other words, it is probably permissible even without new laws.
- We do suggest a new statute, along the lines of the wiretap statute (known in the law biz as “Title III”), to specify the conditions under which this can be done.
- 👉 The current wiretap law places many restrictions on when taps can be done, because they’re so invasive. The same should be done, by statute, for lawful hacking.

Feasibility

- Today's computer systems are quite buggy—better than years ago, but still insecure
- Example: despite all of the effort Microsoft has put into software security—and they've put in a tremendous amount—there are critical patches released virtually every month
- There is a thriving market in “0-days”: holes for which no patches exist because the vendor doesn't know about them
- Most of the customers are intelligence agencies; this won't add much volume.
- The FBI already has a lab (DCAC: Domestic Communications Assistance Center) that develops such technology

The Market

- There's a big market for vulnerabilities
- Many companies, some legit and some less so, sell them
- Some sell to all buyers; others sell only to “certain” governments

0-Days Found: March–July 2012

<i>Month</i>	<i>Vul-Labs</i>	<i>Microsoft V.R.</i>	<i>Vupen</i>	<i>Bugtraq</i>	<i>ZDI</i>
March	9	1	41	11	13
April	37	2	38	6	20
May	31	1	39	2	0
June	32	2	25	5	39
July	15	2	6	17	14

Will this Hurt Security?

- The bugs already exist; finding them doesn't create the problem, it merely exploits it
- We advocate a mandatory reporting requirement: if law enforcement finds or buys an vulnerability, it must report it immediately to the vendor
- This will lead to a patch, so it will *help* overall security
- Studies show that bugs remain unpatched on most users' computers for a very long time. There is thus plenty of time to use the vulnerability
- 👉 Most of the actual wiretap code is vulnerability-independent, and won't have to be rewritten after a given hole is patched

How To Do It

- Scan the target and/or target net
- ☞ Must allow for NATs, multiple devices, etc.
- Figure out OS and software used, versions, etc.
- Select a vulnerability; build a tapping package
- Install it: drive-by download, infected attachment, hacking the target from the outside, maybe even a black bag job

Non-Proliferation

- It's important to keep the exploits from being reused, especially if they use 0-day holes
- Obfuscate the code
- Strongly tie the tapping package to the target machine
- Use DRM techniques—maybe even the OS's built-in DRM schemes—to do this
- In some situations, erase the vulnerability part as soon as the code is installed; maybe even download the tapping part anew each reboot so that it's never stored on disk
- You know, standard virus and malware techniques. . .

The Full Picture

- Law enforcement (and private sector?) labs find holes and develop exploit tools
- New holes are reported to the vendor
- When need arises:
 - Get a scanning warrant
 - Figure out the target's OS, applications, etc.
 - Get a hacking warrant
 - Plant the wiretap code

Why This Helps

- It does not introduce new security holes
- It works without regard to national boundaries
- The mandatory reporting element will improve security
- The new law will regularize and regulate the hacking that already takes place
- The country will have a debate about the difficult issues raised by lawful hacking, e.g., how to limit the search as required by the Fourth Amendment

Further Reading

- Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. Going bright: Wiretapping without weakening communications infrastructure. *IEEE Security & Privacy*, 11(1):62-72, January-February 2013.
<https://www.cs.columbia.edu/~smb/papers/GoingBright.pdf>
- Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. "Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet." *Northwestern Journal of Technology and Intellectual Property*, 2014. To appear.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312107
(draft)
- "CALEA II: Risks of Wiretap Modifications to Endpoints," May 17, 2013.
<https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf>
- "Eavesdropping on Internet Communications," editorial board, *New York Times*, May 20, 2013, <https://www.nytimes.com/2013/05/20/opinion/eavesdropping-on-internet-communications.html>