



1

Interception

Steven M. Bellovin

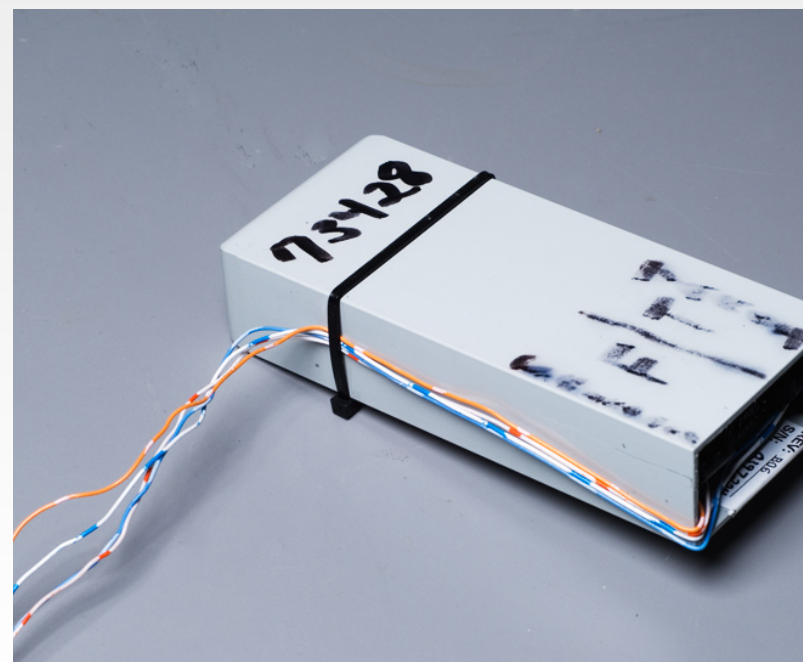
<https://www.cs.columbia.edu/~smb>





Classic Wiretaps

- When *Katz* was handed down, every residential phone line was served by a separate pair of wires from the phone company to the person's house
- If you attached a tap to those wires, you'd get *only* that line's calls
- Even then, a call might be to someone else in the residence



(Photo of a "loop extender" by Matt Blaze)



Classic Pen Registers

- Pen registers—including most of those in use at the time of *Smith*—were similarly simple
- They attached to a wire pair and recorded dial pulses and perhaps touchtones
- They contained no circuitry or recording equipment capable of intercepting speech





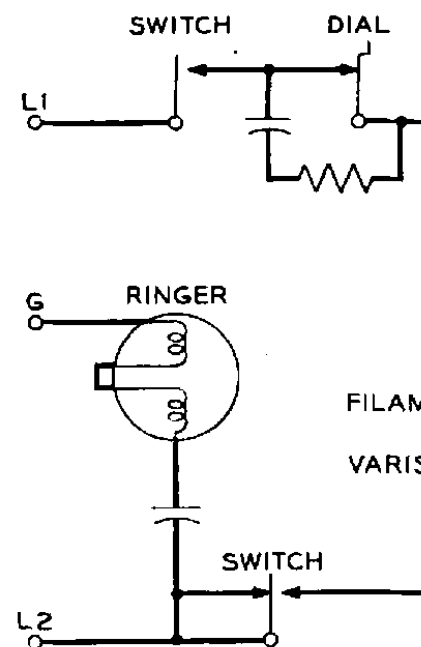
Life is No Longer That Simple

- Virtually all communications equipment uses software
- Many features that were formerly done with inflexible hardware are now done by changeable—and often subvertible—software
- Most network media are *shared*: an interception device has to look at the content of a message to decide if it is relevant to the interception order
- There are many newer ways to get data, but the law hasn't always kept up



Software Control

- On older telephones, the microphone was physically disconnected from the phone line when the phone was on-hook
- Today, the microphone's connectivity is controlled by *software*
- Changed software, either in the phone or (sometimes) at the central office, can turn the microphone on while the phone is on-hook
- (Does your desk phone have a "speakerphone" button? Mine does...)





Using Software for Interception

- The FBI (apparently) converted a cellphone into a roving bug (allowed, *US v. Tomero*, 471 F. Supp. 2d 448, 2007)
 - The details in the order are suggestive but not definitive
- The FBI used a car's cellular "help" system to eavesdrop on conversations in the car (excluded, *Company v. United States*, 349 F.3d 1132, 1145 (9th Cir. 2002))
- Someone—probably an intelligence agency, though which one isn't known—hacked a cellphone switch in Greece to tap all calls to 100 different phones, including the prime minister's
- Researchers have shown how to activate a Mac's camera without turning on the light ("*iSeeYou: Disabling the MacBook Webcam Indicator LED*", Brocker and Checkoway, *Usenix Security 2014*)
 - Criminals have used similar abilities to spy on (mostly) women



How It's Done: Many Ways

- Hack the phone or computer to install new code; the new code will turn on the microphone or camera
- Control the server (the car case)
- Control the server and use it to push new code to the device (United Arab Emirates tried that: <http://news.bbc.co.uk/2/hi/8161190.stm>)
- Control the vendor and have it push new code to the device (most have the ability: <http://www.extremetech.com/computing/196391-apple-pushes-its-first-ever-silent-automatic-security-update-to-mac-os-x-to-fix-ntp-bug>)
- Order other companies to issue bogus cryptographic authentication credentials
- Physical intrusion



The Internet

- The Internet is composed of many different networks linked together by special computers known as *routers*
- Computers—*hosts*—are attached to networks
 - Each computer has one or more *IP* (Internet Protocol) *addresses*
 - IP addresses are the (very) rough equivalent of phone numbers
- *Services* are provided by regular computers attached to the Internet, *not* by the network
 - This is very different than how the phone network functions
 - ISPs can run mail servers—but so can Google, and so can I
- A given computer can offer many different services: email, Web, and more
 - Which service is being requested on a computer is determined by the *port number*
 - Port 25 is for email, port 80 is for Web, port 443 is for encrypted Web, etc.



Tapping the Internet

- Example: a pen register order or full-content warrant for Chris Doe
- Attach an eavesdropping device to some network
 - It's best to tap a network link very close to the target—ideally, the *access link*
- Remember that the medium is *shared*
 - The eavesdropping device *must* look at every packet (a fragment of a message) to determine if it has the right IP address
 - Sometimes, a *different* conversation has to be tapped to learn the target's IP address
 - It *must* verify that the packet has the right port number (e.g., email)
 - It may have to examine the *content* of the packets to verify that they're Chris Doe's email and not Pat Doe's—even if it's a pen register order

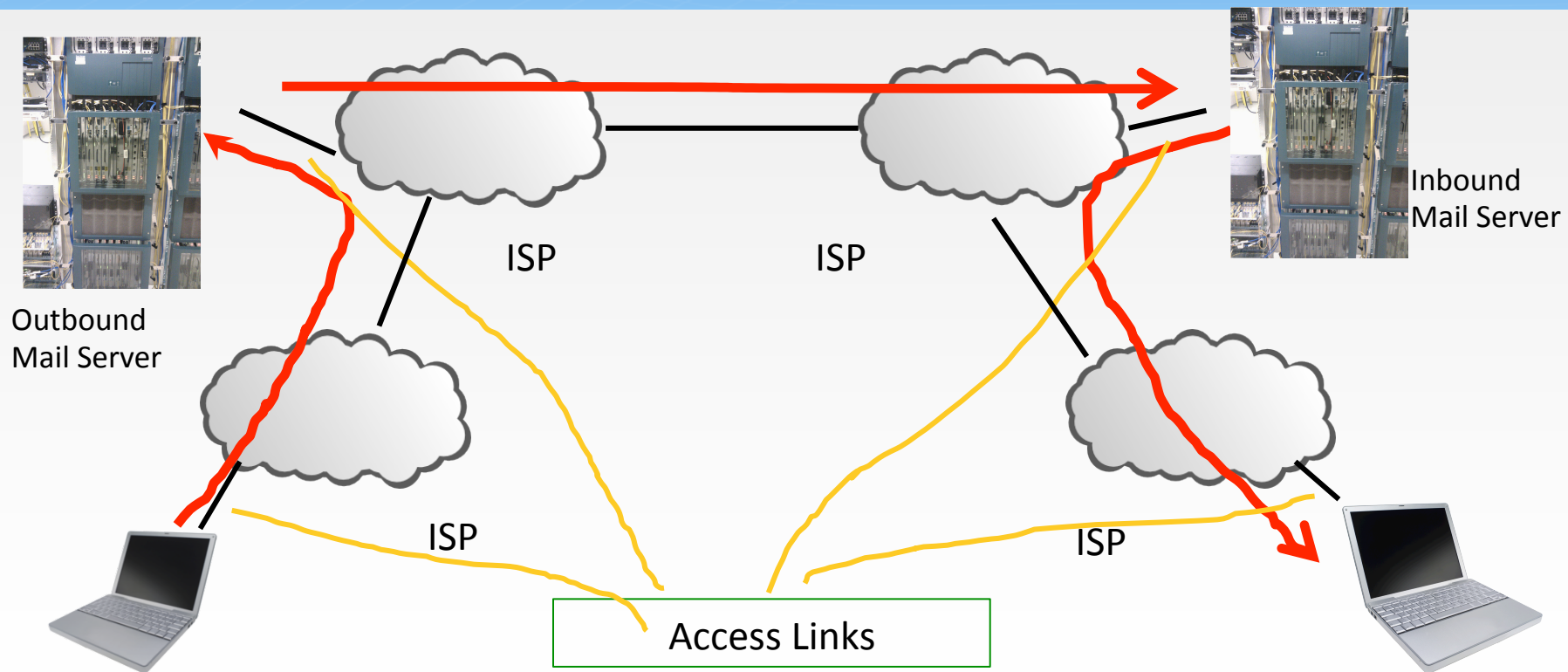


Sending Email

- A user composes a message using some email app
 - The message has a *header* (From:, To:, etc.) and a *body*
- It is then uploaded to her *outbound email server*
 - A special *protocol* known as *SMTP* (Simple Mail Transfer Protocol) is used for this
 - The message is probably also copied to the Sent Messages folder via the *IMAP* protocol
- This server sends to to the recipient's *inbound mail server*, also via SMTP
- The recipient's email app downloads it, probably via the IMAP protocol
- Note that there are four different network connections (using two protocols) and four different computers
 - (It's actually far more complicated than that)



Sending Email






Sending Myself Email—An SMTP Transcript

```
220 machshav.com ESMTP Exim 4.82 Tue, 11 Mar 2014 19:43:03 +0000
HELO eloi.cs.columbia.edu
250 machshav.com Hello eloi.cs.columbia.edu [2001:18d8:ffff:16:12dd:b1ff:feef:8868]
MAIL FROM:<smb@eloi.cs.columbia.edu>
250 OK
RCPT TO:<smb@machshav.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: Barack Obama <president@whitehouse.gov>
To: <smb2132@columbia.edu>
Subject: Test

This is a test
.
250 OK id=1WNSaS-0001z5-1d
QUIT
221 machshav.com closing connection
```

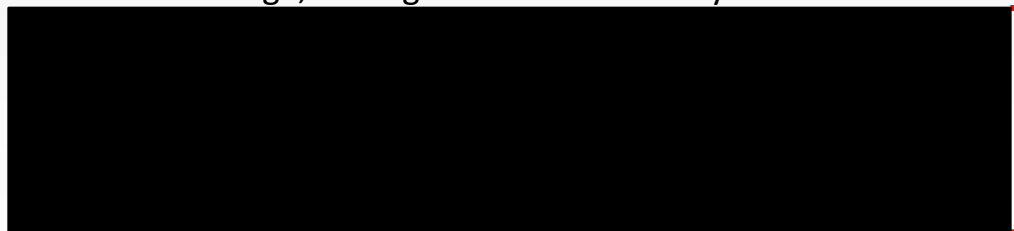


Message body



Conversation With A Third Party

```
220 machshav.com ESMTP Exim 4.82 Tue, 11 Mar 2014 19:43:03 +0000
HELO eloi.cs.columbia.edu
250 machshav.com Hello eloi.cs.columbia.edu [2001:18d8:ffff:16:12dd:b1ff:feef:8868]
MAIL FROM:<smb@eloi.cs.columbia.edu>
250 OK
RCPT TO:<smb@machshav.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
```

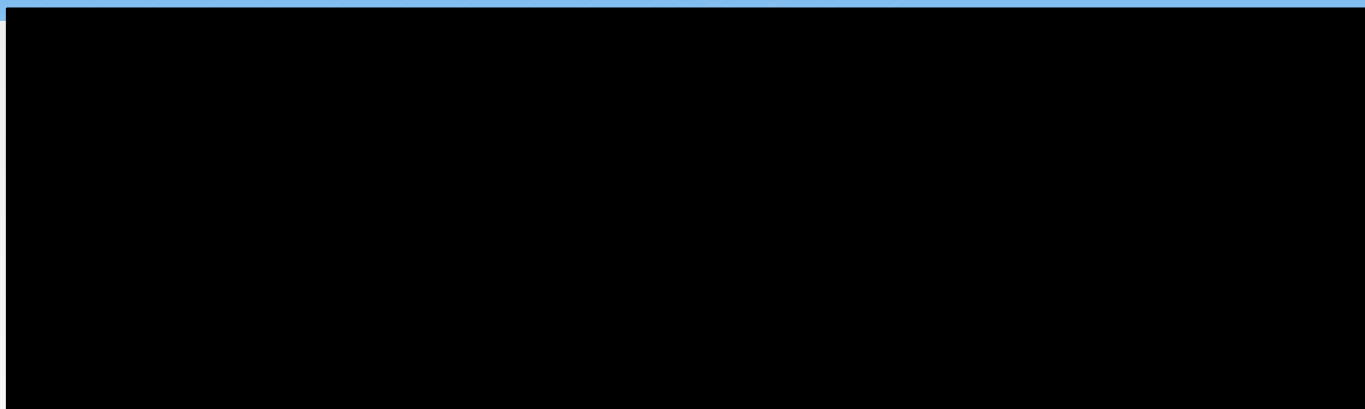


Message body

```
.
250 OK id=1WNSaS-0001z5-1d
QUIT
221 machshav.com closing connection
```



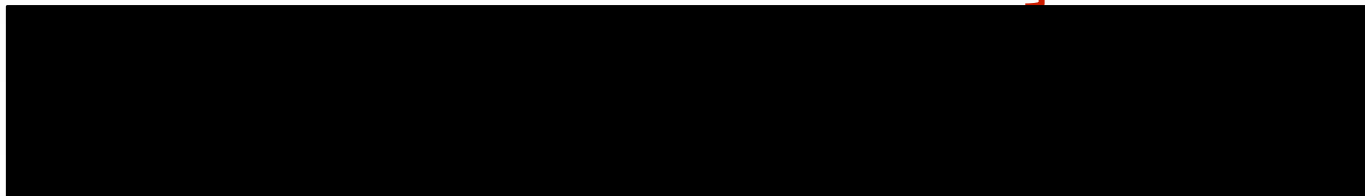
What the Recipient Sees



From: Barack Obama <president@whitehouse.gov>
To: <smb2132@columbia.edu>
Subject: Test

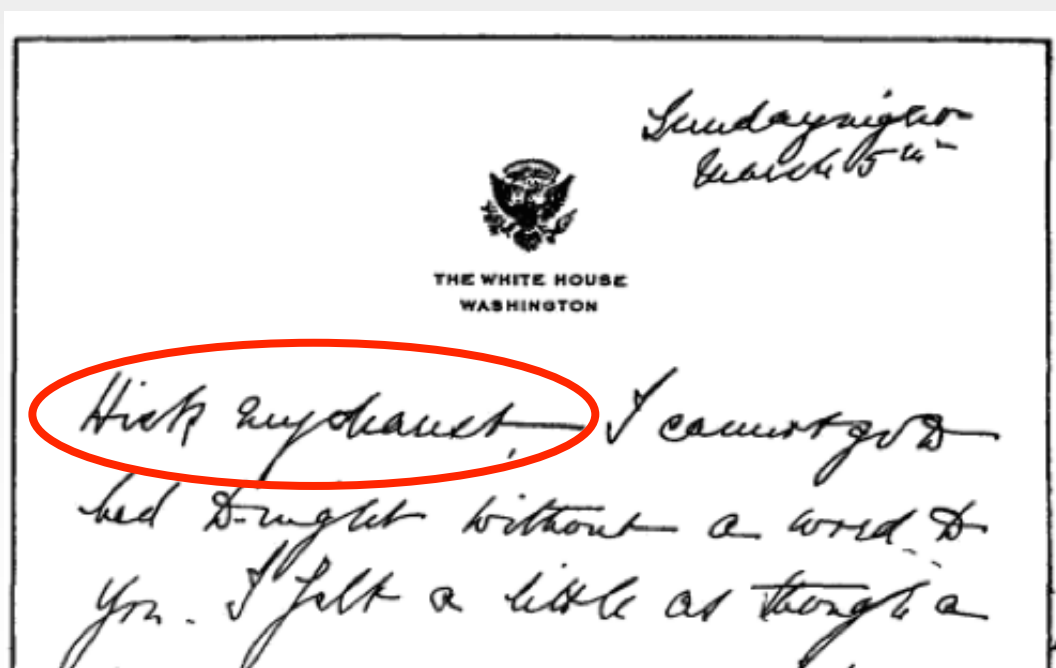
Message body

This is a test





A Letter from Eleanor Roosevelt to Lorena Hicks (March 1933)



It begins "Hick my dearest".

(excerpt from
Amazon.com)



Things to Note

- The SMTP *envelope*—that’s the technical term!—can have different information than the message headers
- Unlike the phone network, anyone can run their own mail servers
 - I personally run two, one personal and one professional
 - This complicates third party doctrine analysis
- The reality of email is far more complex than I’ve outlined here
 - Example: many people read their email via a Web browser—and the NSA has stated that even for them, picking out just the From/To information from a Webmail session is very difficult
- I haven’t even begun to address server-resident email, virus scanning, spam filtering, and the like, let alone all of the other metadata that’s present



A Few Other Problematic Aspects of Wiretapping on the Internet

- IP addresses are used by every router along the path of a network connection
- TCP port numbers are of interest only to the receiving host, and are generally *not* used by intermediate routers
 - DoJ's 2005 Electronic Surveillance Manual says that they're fair game for pen register orders
 - The technical aspects of this are *very* complex, and fact-specific
- DoJ's 2010 Prosecuting Computer Crimes manual warns prosecutors to contact them about which parts of a URL are content and which are metadata
 - My own analysis suggests that they're quite correct—even I was surprised at how complex a question that is
- There have been very few in-depth technical/legal analyses of less-used Internet protocols to determine which parts are content and which are metadata
- Taps are done by software—and tapping software, like all software, can be buggy
 - Both exculpatory and incriminating information can be missed
 - Because of the packet nature of the Internet, it's easy for parts of a conversation to be missed



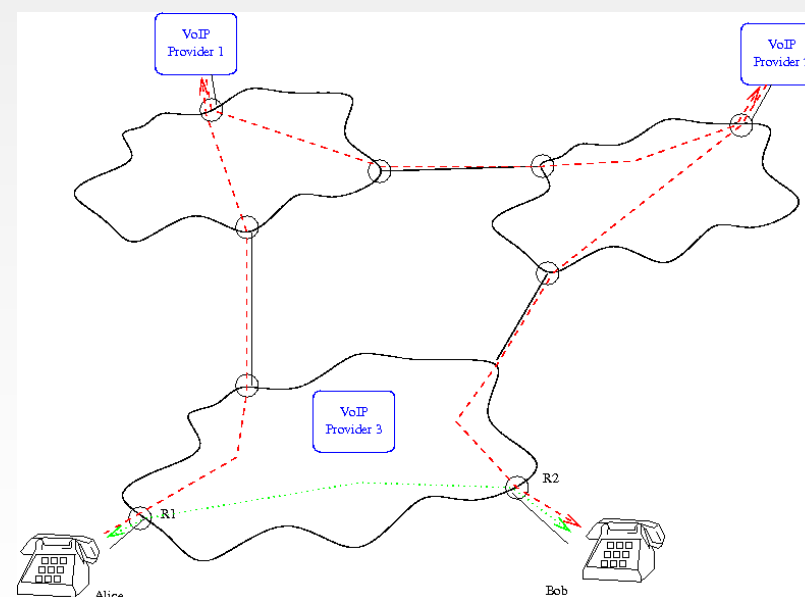
From a FOIAed FBI Memo

The software was turned on, and did not work correctly. The FBI software not only picked up the E-Mails under the electronic surveillance of the FBI's target, [REDACTED] but also picked up E-Mails on non-covered targets. The FBI technical person was apparently so upset that he destroyed all the E-Mail take, including the take on [REDACTED] [REDACTED] is under the impression that no one from the FBI [REDACTED] was present to supervise the FBI technical person at the time. Now the FBI technical people want to run a new software experiment at the carrier to see if it works.



VoIP is Hard to Tap

- The call is set up via the VoIP carriers, who may be in other jurisdictions
 - This is where the pen register information would be gathered
- The actual conversation uses a different Internet path
 - The call may be encrypted
- The ISPs are not involved, and can't lend assistance





Encryption on the Internet

- It exists, but except for email from the user to the mail server and some Web traffic, it's very hard to use
- “You don't go through strong security, you go around it”
 - Modern algorithms are probably impossible to break if properly used
 - But—they're rarely used correctly
 - Guess at passwords (or find them written down)
 - Look for software bugs or program design flaws
 - Find a plaintext copy of the message, e.g., on the mail server
 - Monitor non-access links
- Most technologists agree that encryption “back doors” or “golden keys” are a bad idea for *technical* reasons