Wiretapping the Internet --- (or How Not to Introduce Security Holes into a Communications Infrastructure)

Susan Landau
Distinguished Engineer
Sun Microsystems Laboratories

Frank DeMarco

"Tidewater Muse"

Communications Assistance for Law Enforcement Act (CALEA)

- U.S. law that digitally switched telephone networks must be built “wiretap-enabled.”
- Standards determined by the FBI.
- International effect.
- Law originally applied to telephone services, not “information services.”
- 2003-2006 expansion of law to “easy” case of VoIP.
- Now attempt to expand the law to all cases of real-time communications.

Circuit-Switched v. Packet-routed Networks

- Circuit-switched means a dedicated circuit that lasts the whole call.
- Packets of a packet-routed network can, theoretically, take different paths between the endpoints.
- Packet-routed is versatile; it routes “around” problems.

The Networks are the Same:

- Same type of transmission facilities (often sharing same cable).
- Use electric routing/switching devices
- Use transmission links and switching and routing equipment parsimoniously.
- Many facilities-based companies operate networks and must work together to deliver user's traffic.
- Both began with all-you-can-eat pricing model.
- Both use digital transmission and time-division multiplexing.

The Networks are Different:

- PSTN historically used expensive switches to provide quality. Internet and Arpanet used relatively inexpensive routers for “best-effort.” Internet now migrating to switch-based technology for QOS.
- Internet eschews intelligence in the network. PSTN uses network-based intelligence for dumb terminals, enabling legacy telephones.

What's Important about VoIP?

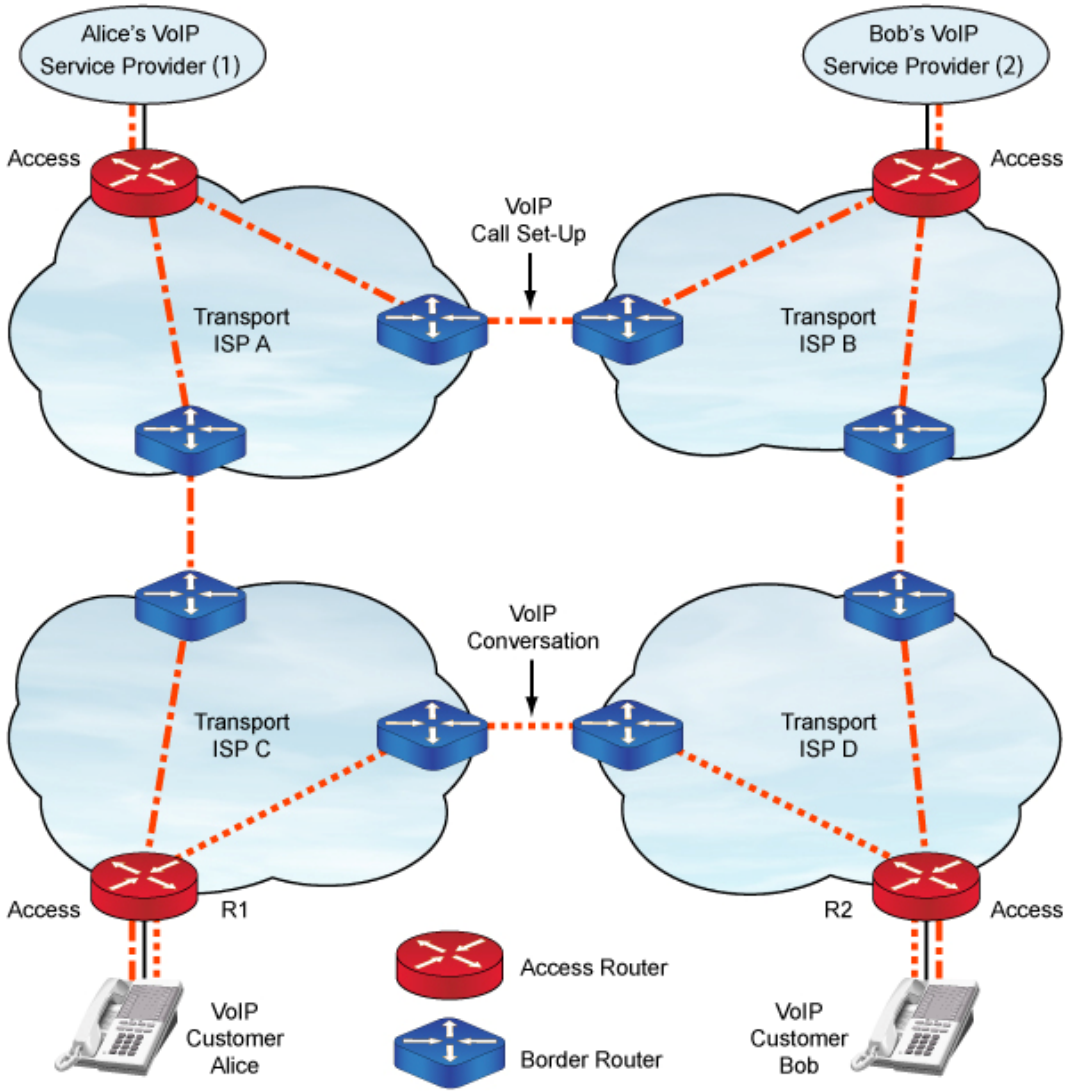
- Variety of VoIP models.
- Mobility.
- Ease of creating new identities on the Internet.

What's Complicated about Applying CALEA to VoIP?

- Variety of VoIP models.
- Mobility.
- Ease of creating new identities on the Internet (artifact of little or no authentication for most Internet applications).

Don't We Already Have Wiretaps with Mobility?

- Cell phones
- Roving wiretaps


Alice's VoIP
Service Provider (1)
Bob's VoIP
Service Provider (2)
Access
Access
VoIP
Call Set-Up
Transport
ISP A
Transport
ISP B
VoIP
Conversation
Transport
ISP C
Transport
ISP D
Access
R1
R2
Access
Access Router
Border Router
VoIP
Customer
Alice
VoIP
Customer
Bob

What's the Problem? I

- Physical security of the switching/routing equipment into which wiretaps are inserted --- can't be predicted in advance. There are 1300 VoIP providers in U.S. with fewer than 100 employees. The same model exists elsewhere in the world.
- Ease of creating new identities on the net.
- Secure transport of signals to law enforcement.

What's the Problem? II

- Increases risk that target discovers wiretap is in place.
- Difficulty of ensuring proper minimization because of mobility and agility issues.
- **Increased risk of introducing vulnerabilities into Internet (IETF RFC 2804).**
- Search engines + vulnerabilities = a dangerous combination.

Here's One Risk (there are others):

- At 10:23 PM PST, attackers found vulnerabilities in computers at the U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona.
- At 1:19 AM PST, they found the same hole in computers at the military's Defense Information Systems Agency in Arlington, Virginia.
- At 3:25 AM, they hit the Naval Ocean Systems Center, a defense department installation in San Diego, California.
- At 4:46 AM PST, they struck the United States Army Space and Strategic Defense installation in Huntsville, Alabama

Nathan Thornburgh, Time Magazine, August 25, 2006

What's the Real Problem?

- People call people, not IP addresses.
- If you're trying to do VoIP on a fixed line directly to large ISP: Easy. Anything else: HARD.
- The proposed expansion of CALEA is worse. It would cover: any real-time communications, any WiFi provider of more than 300', and would force a “point-of-presence” requirement for applications used in U.S.

Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP

Steven Bellovin, Columbia University
Matt Blaze, University of Pennsylvania
Ernest Brickell, Intel Corporation
Clinton Brooks, NSA (retired)
Vinton Cerf, Google
Whitfield Diffie, Sun Microsystems
Susan Landau, Sun Microsystems
Jon Peterson, NeuStar
John Treichler, Applied Signal Technology

June 13, 2006

Security Implications of Applying the Communications Assistance for Law Enforcement Act to VoIP

- http://www.itaa.org/news/docs/CALEAVOIPreport.pdf

Susan Landau
susan.landau@sun.com