Internet Surveillance: Building Our Own Trojan Horse

Susan Landau
Distinguished Engineer
Sun Microsystems Laboratories

The Changes since 9/11

- TSA airport screenings
- Restrictions on visas.
- ID cards: RealID and PIV.
- Wiretap laws.

Wiretap Laws

- USA PATRIOT Act (2001).
- U.S.: Communications Assistance for Law Enforcement Act (CALEA) extended to VoIP (2003-).
- U.S.: Protect America Act (2007).
- Two-week extension to Protect America Act (2008).
- (Cyber Initiative (2007)).

Wiretap Law

- Title III: covers criminal cases (1968).
- Foreign Intelligence Surveillance Act (FISA): covers surveillance for foreign intelligence (1978).
- Communications Assistance for Law Enforcement Act: requires digitally-switched telephone networks to be built “wiretap accessible” (1994).
- Protect America Act: “updates” FISA to warrantless wiretapping of foreign communications over fiber optic cables (2007).
- Cyber Initiative (2008).

What risks do we face?

- Serious risks --- nuclear explosions in cities (including dirty bombs).
- Small risks, e.g., terrorists blowing up buses and trains.
- Natural disasters --- 2005 Hurricane Katrina and the 2004 Indian Ocean earthquake tsunami.
- 1931 Yellow River Flood, 1887 Yellow River Flood, 1970 Bhola Cyclone, 1556 Shaanxi Earthquake.

How efficacious are the proposed solutions?

- Wiretaps critical in kidnapping cases.
- Wiretaps used for other investigations.
- June 2006 Department of Justice *Counterterrorism Whitepaper:* 441 defendants charged with terrorism or terrorism-related activities of an international "nexus."

How efficacious are the proposed solutions?

- Wiretaps used in kidnapping cases: an average of 2-3 cases between 1968 and 1994, 4-6 in subsequent years.
- Wiretaps used for other investigations: 1968-73, 64% of cases were gambling; now it is 81% drugs. 1988-1994: arson and explosive cases: 0.
- Between 2001-2006: Yes, 441 defendants including Sheikh Abdel-Rahman, Zacarias Moussaaoui, Richard Reed. But of 335 persons prosecuted between 2001 and 2006 as "international terrorists," 123 received prison sentences, 14 of five years or more, 6 for twenty years or more.

What is the cost of the proposed solutions?

- How long will this “war” last?
- What will be the long-term costs of the proposed solutions?
- Are we looking at long-term risk for short-term gain?
- Use of surveillance previously limited to times of war.

The Real Question: how well do these work?

- Enabling law enforcement and national security investigations

versus

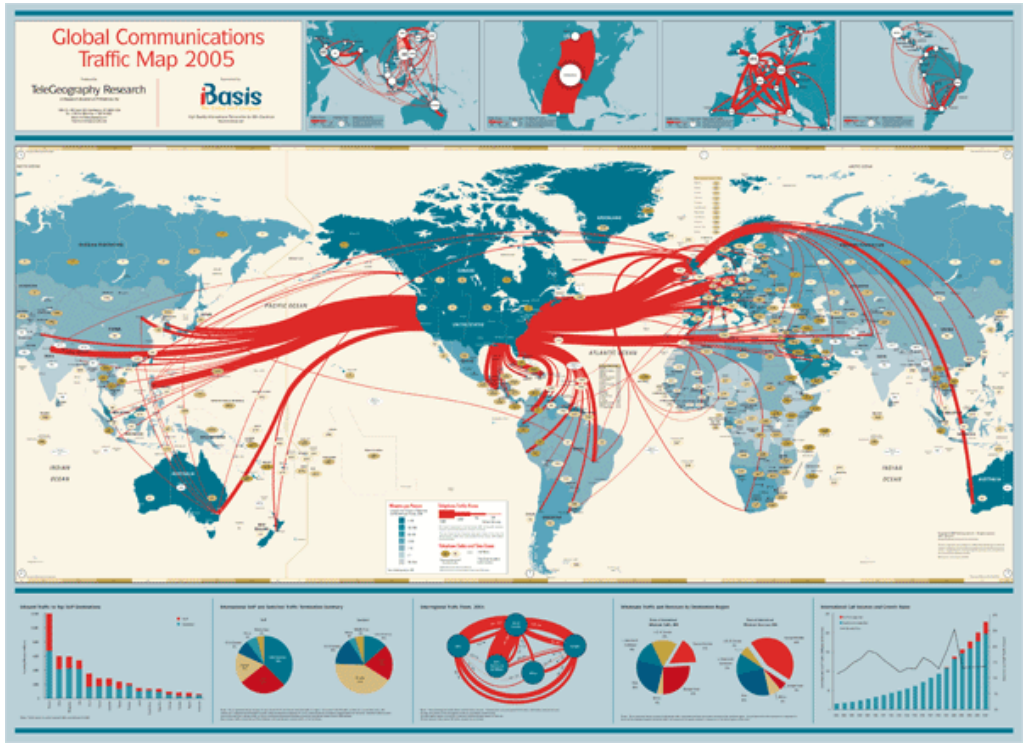
- Hardening communication systems.

Communications Assistance for Law Enforcement Act (CALEA)

- Law originally applied to telephone services, not "information services."
- 2003-2006 expansion of law to "easy" case of VoIP.
- 2006: attempt to expand the law to all cases of real-time communications.
- 2007: Request for "expedited rulemaking" to require broadband access providers to provide call-identifying information on packet activity for all online applications.

The Protect America Act: What and Why

- Warrantless wiretapping permitted as long as one end of communication "reasonably believed to be outside U.S."
- "Update" to FISA.
- Location difficult to obtain in real time.
- Law expired in January 2008.
- Renewal??



Circuit Switched v. Packet Switched --- 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 use digital transmission and time-division multiplexing.

Circuit Switched v. Packet Switched --- 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.

Looking at applying CALEA to VoIP, what's important about VoIP?

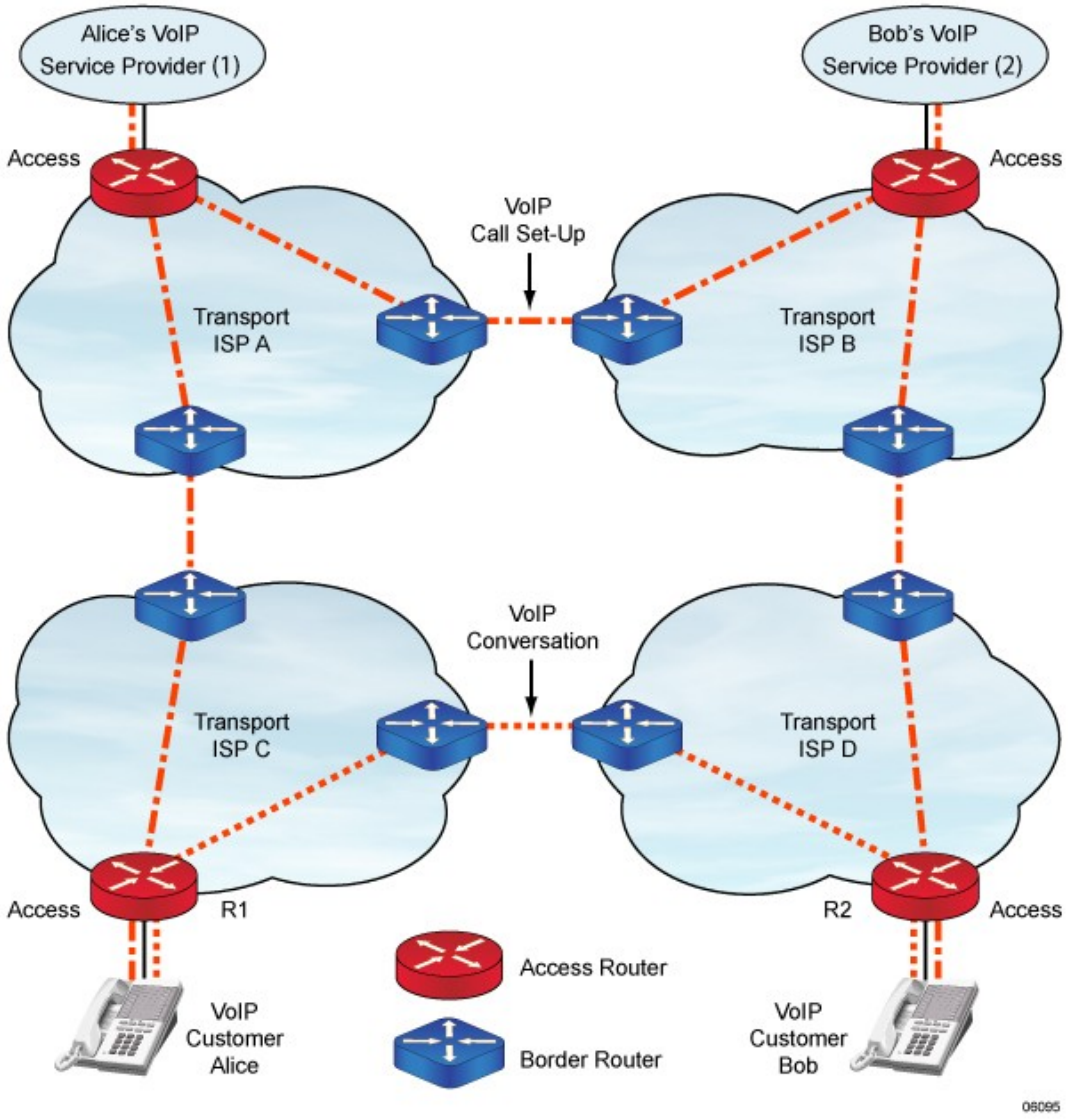
- Variety of VoIP models.
- Mobility.
- Ease of creating new identities on the Internet.

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 Wiretap Mobile Communications?

- 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
06095

What's the Problem? I

- Physical security of the switching/routing equipment into which wiretaps are inserted --- can't be predicted in advance. For example,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.

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.

This is not just theory: the Problems with DCS 3000:

- Auditing system primitive: no unprivileged userids, passwords rather than token-based or biometric authenticators.
- Outdated hashing algorithm (MD5) in 2007 document.
- Single shared login, rather than login per user.

The Protect America Act: Dangers Lurk

- Apparent removal of security and privacy role of communication carriers.
- Placement of system properly within the U.S. rather than at borders.
- Likely to be made of pieces previously used abroad.
- Call Detail Records, built for network development purposes, now has new “customers.”

The Protect America Act: Risks

- Risk of exploitation by opponents.
- Lack of two-person (two-organization) control.
- Lack of inherent technical minimization of traffic.
- Domestic traffic penetrating into a system built for foreign surveillance traffic.

What are the type of threats we face?

What are the type of threats we face?

- Threats from non-state actors.

What are the type of threats we face?

- Threats from non-state actors.
- Threats from state actors.

What are the type of threats we face?

- Threats from non-state actors.
- Threats from state actors.
- Threats from insiders.

Threats from Non-State Actors

- “Loop carrier” disabled Worcestor Airport tower communications (1998).
- Attack on sewage treatment plant in Maroochy Shire, Australia released thousands of gallons of untreated sewage (2000).
- Slammer worm disabled safety monitoring system at Davis-Besse nuclear power plant (2003).
- Penetration into Harrisburg water filtration plant for distribution of spam, etc. (2006) ...

Threats: Attacks from State Actors

- 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

Threats from Insiders

- Historically the most dangerous type of threat

Threats from Insiders

- Historically the most dangerous type of threat
- They know your systems, they know your vulnerabilities, they know your audit methods, ...

Threats from Insiders

- Historically the most dangerous type of threat.
- They know your systems, they know your vulnerabilities, they know your audit methods ...
- Kim Philby, Aldrich Ames, ...

These Attacks are not Hypothetical --- Vodafone Greece:

- Between June 2004 and March 2005, more than one hundred phones belonging to members of the Greek government --- including the Prime Minister --- were wiretapped.
- Wiretapping software activated.
- Vodafone had not bought wiretapping package --- and thus logging software not installed on system.
- Rootkit hid activity of updates, etc.
- Discovered when SMS went awry.

These Attacks are not Hypothetical: Telecom Italia

- Massive alleged wiretapping at Telecom Italia.
- Former Chief of Security arrested.
- Targets included many public figures: magistrates, politicians, sports players, referees.
- Motive: blackmail?

Contrasting Notions of Security

- Two notions of computer security: “traditional” computer security, and “cyber-security.”
- Traditional computer security protects against attacks against availability, integrity, and confidentiality of computer systems.
- Cybersecurity protects against attacks by networked systems, attacks on critical infrastructure, and attacks on networked information systems.

Contrasting Threats and Protection Models

- Traditional computer security protects the machines through reducing vulnerabilities and providing defense in depth.
- Cybersecurity “checks the road” --- who is out there, what are they doing, why are they doing it. This is a different threat model and a different model of security. This “protection” can introduce vulnerabilities.

What risks do we face?

- Serious risks --- nuclear explosions in cities.
- Small risks, e.g., terrorists blowing up buses.
- Natural disasters --- 2005 Hurricane Katrina and the 2004 Indian Ocean earthquake tsunami.
- 1931 Yellow River Flood, 1887 Yellow River Flood, 1970 Bhola Cyclone, 1556 Shaanxi Earthquake.

Frank DeMarco

"Tidewater Muse"

What risks do we face?

- Hurricane Katrina: > 1800 dead.
- Indian Ocean earthquake tsunami: 283 thousand.
- 1931 Yellow River Flood: 1-2 million dead.
- 1887 Yellow River Flood: 1-2 million dead.
- 1970 Bhola Cyclone: 500K-1 million dead.
- 1556 Shaanxi Earthquake: 830 thousand dead.
- 1839 Indian Cyclone: 300 thousand dead.
- ...

What Does Society Need (in Terms of Communications Security)?

- Securing civilian communications.
- Enabling secure communications in cases of national/international disaster, natural or otherwise.
- Enabling successful investigations of criminal and terrorism cases.

Enabling Secure First-Responder Communications

- What communications worked during 9/11 and Katrina?
- What was easy to use after the disaster?
- What are the types of disasters in which we will need such communication systems?
- What are we protecting against? What should we be developing for?
- Secure ad-hoc communications networks are important in the civilian infrastructure --- just as they are in the military.

Securing Civilian Communications

- Securing personal and business communications.
- Securing communications that use the Internet as a backbone.
- Securing communications that use private networks with Internet protocols.

Tools for Investigations

- Different environment than 1968, 1978: credit cards, frequent-flyer numbers, frequent-buyer cards; data mining is an industry.
- Storage of transactional data (data retention requirements in Europe).
- Different communications environment: an increasing majority of citizens broadcast their location.
- CCTV.

Terrorism Investigations: not criminal cases

- Deterrence --- jail --- may not be an answer.
- Different situation in U.S. compared to U.K., France, and Germany.
- Lessons from West Bank and Northern Ireland.
- Community building: Extensive surveillance networks may not be the answer --- “The whole deal here is to engender the trust that one afternoon may allow one of those Islamic leaders to say to the sergeant, 'You know, I am worried about young so-and-so.' ”

Ian Blair, London Police Comm.

The Long View

- [T]he terror threat will be with us for a long time. It's a new, maybe generational challenge and we have to learn to manage it as we devise better strategies, as we find out who's trying to attack us and prevent it.

  Representative Jane Harman
  December 8, 2007.

Susan Landau
susan.landau@sun.com