Wiretapping and Surveillance II

Wiretapping Meets the Computer Age

- We've all seen pictures of traditional wiretaps — the guys with the earphones in the van, the wires with alligator clips, etc.
- Those images are fairly realistic — but times have changed
- Today's phone system is not compatible with the old way of doing things

Loop Extenders

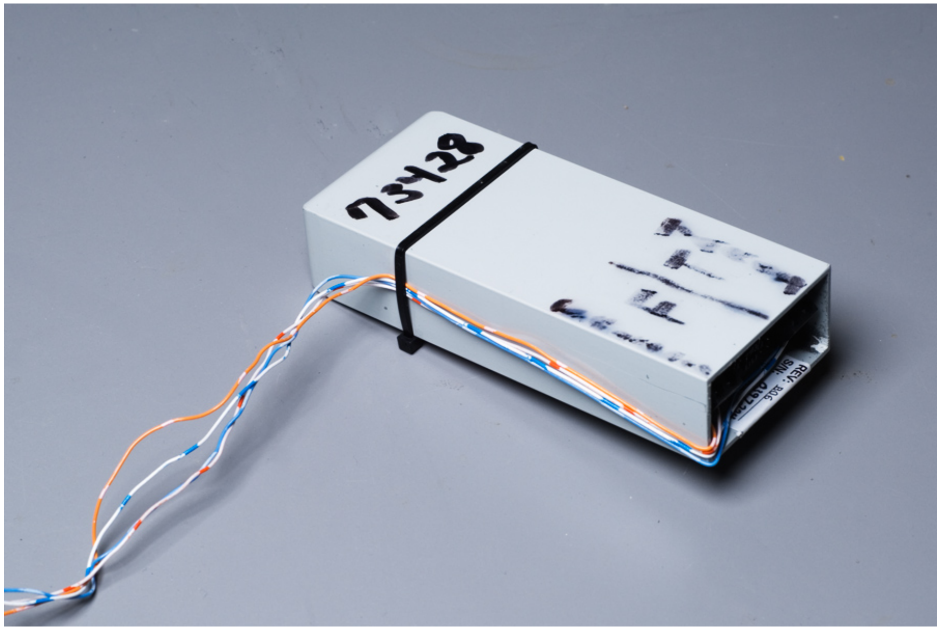


Photo © Matt Blaze; used by permission

- Attach one set of wires to the target's line.
- Attach the other set to an unused "friendly pair" to run the signal back to the central office.
- Listen in from the comfort of an office environment — no more cold vans...

Pen Registers

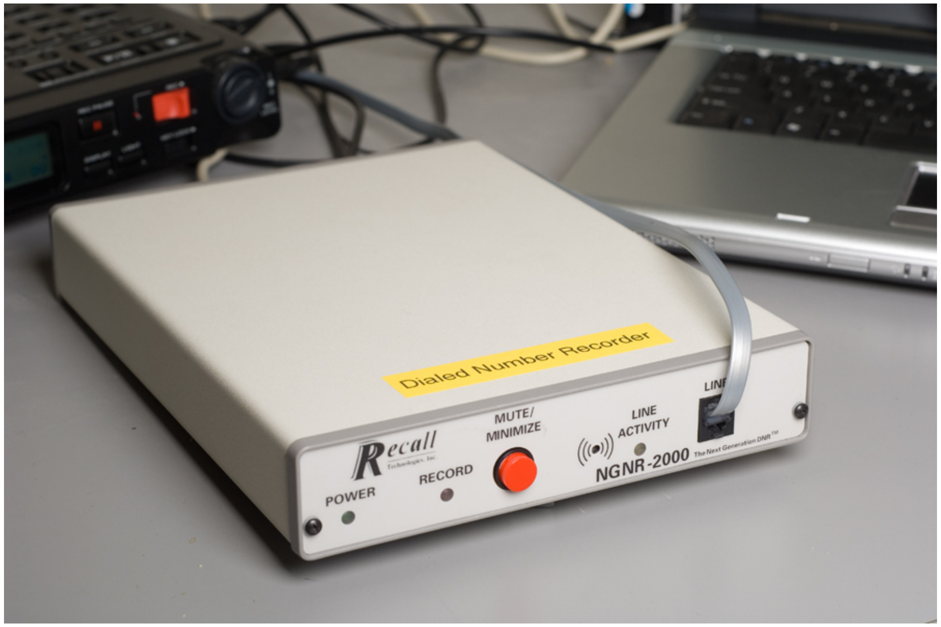


Photo © Matt Blaze; used by permission

- Note the phone jack on the front — it's designed to plug in to a standard phone line
- It just listens to dialing tones and records them
- The "minimize" button suggests that it's part of a general wiretap setup

The Full Setup

Photo © Matt Blaze; used by permission

- The recorder is hooked to the dialed number recorder
- A laptop controls everything

What’s the Problem?

- By the early 1990s, it was obvious (at least to the FBI) that traditional twisted-pair, hard-wired telephones were obsolescent
- They were right — while plenty of twisted pair phones remain, the growth is in cell phones, VoIP, etc.
- How do you tap such phones?

Enter CALEA

- In 1994, Congress passed CALEA: *Communications Assistance for Law Enforcement Act*
- It required a standardized interface to tap calls, from the comfort of their own offices
- Applied to any “entity engaged in providing commercial mobile service” or “a replacement for a substantial portion of the local telephone exchange service” (P.L. 113-414(103)(8)(B))
- Did not apply to “entities insofar as they are engaged in providing information services” (P.L. 113-414(103)(8)(C))
- It now applies to ISPs, despite that last clause. . .

Lawful Intercept

- Most other industrialized nations have passed similar laws
- The generic concept is known as “lawful intercept”
- All major manufacturers of phone switches and IP routers support it
- Precise rules for access are different in each country

What’s the Trouble?

- “It’s only a software change”

☞ But phone switch software is *very* expensive

- Congress authorized some money for switch upgrades, but not nearly enough
- The system required complex software — and that’s *always* a recipe for trouble

They Were Warned. . .

- “It’s too complex”
- “It’s vulnerable to remote hacking”
- “The real bad guys will use crypto”
- Guess what happened?

Pen Register Complexities

- Under CALEA, what is a pen register supposed to capture?
- Dialed digits? Which dialed digits?
- Digits before you hit “Send” on your cell phone? How?
- Digits dialed after the call is established? Sometimes right, sometimes not — how can you tell?

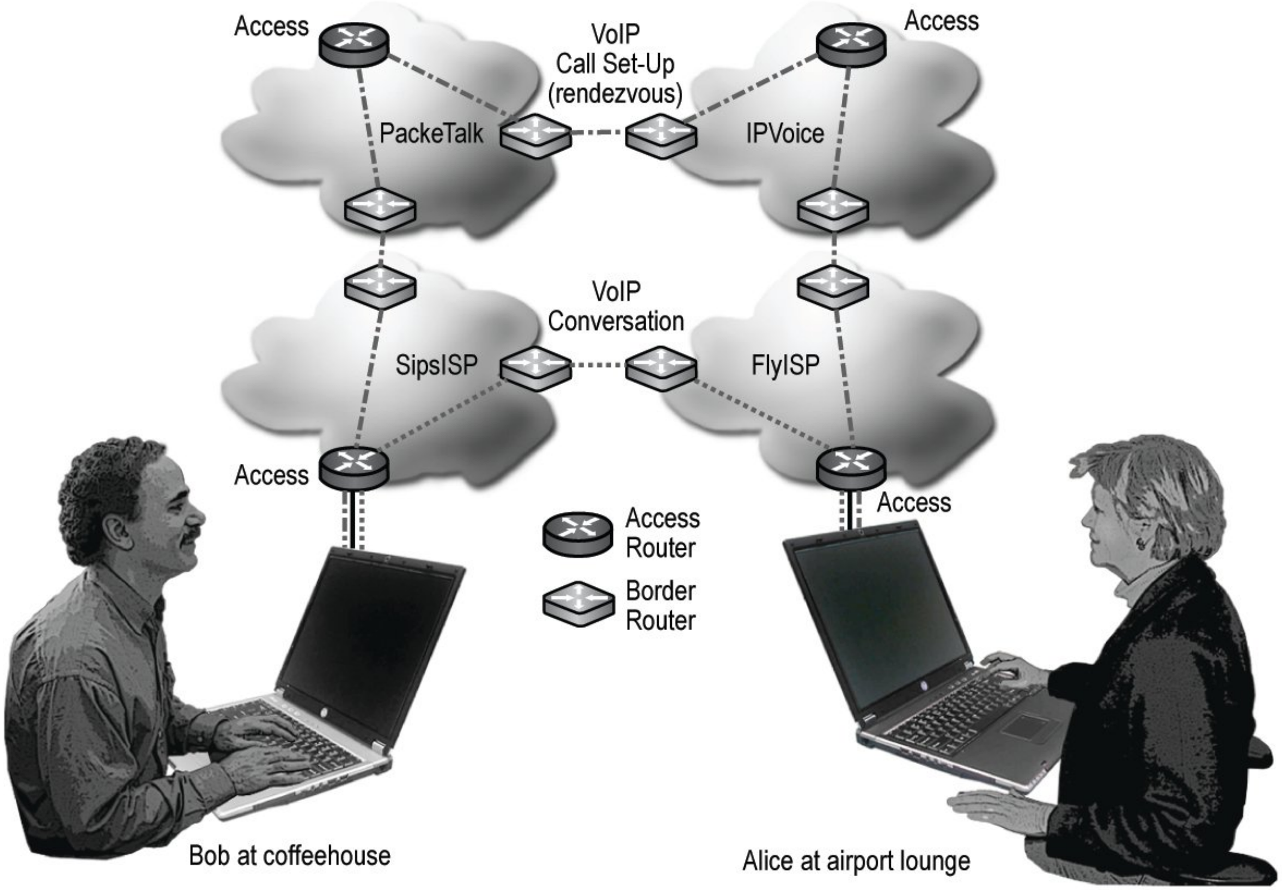
Yesterday’s Answers to Today’s Technology

- It used to be easy to captures digits as dialed, so the FBI wanted that ability to remain
- They ignored the fact that today’s devices just aren’t built that way
- Maybe the devices could be modified to do it if needed, but then taps would be detectable
- They tried to adapt to prepaid calling cards — but ignored other tone response systems: “For new reservations, press 1; for existing reservations, press 2; for the FBI guy who’s listening to you, press 3”?

The Problem with VoIP

- VoIP calls can be tapped at two layers, the voice layer and the IP layer
- The IP layer knows nothing of telephony concepts like phone numbers
- If the signaling channel is encrypted, the ISP can't even look at it
- This means that a voice-layer tap should be done — but that doesn't work

Running VoIP



(Picture by Nancy Snyder)

Tapping VoIP

- The ISP and the VoIP provider may not be the same
- The voice path isn't the same as the signaling path
- The ISP will be local — but the VoIP provider can be anywhere

Skype Makes it Harder

- Skype uses a peer-to-peer signaling network; there are no trusted nodes on whom the FBI can serve a court order
- The actual signaling path can vary from call to call
- Skype uses a strongly-encrypted voice path — *no one* can tap it
- The technology used is fundamentally incompatible with the model used by CALEA

Tapping IP is Hard Enough

- Connections are broken up into packets
- Packets can and do take different paths through the network
- It isn't easy to predict how any given packet will be routed, though different packets from the same connection tend to follow the same path
- Most inter-ISP paths are asymmetric, for sound network engineering reasons
- Conclusion: the only good place to tap IP is at the edge

Enter Carnivore

- Carnivore was an FBI system designed to tap Ethernets
- It was capable of pen register or full content wiretaps
- It listened to DHCP and otherwise decoded protocols to be (relatively) smart about what it monitored
- Subject of an independent review — but that review was criticized as superficial and incomplete
- Example: the review team didn't look for problems such as buffer overflow

Exit Carnivore

- Because of the publicity the name attracted, the FBI renamed Carnivore to “DCS-1000”
- A few years ago, it was discontinued entirely
- Commercial software and/or ISP capability had gotten good enough

Hacking

- What if someone hacks into the wiretap platform?
- Could they delete data? Insert false data? Modify data?
- Could they use the lawful intercept mechanism to spy on someone else?

The Athens Affair

- Vodaphone Greece bought a phone switch with (legally mandated) lawful intercept capability
- Someone — just whom has never been established — installed binary patches into the phone switch to (ab)use this mechanism
- The attacker tapped about 100 cell phones belonging to senior government officials, including the Prime Minister
- One phone number on the list belonged to someone at the American embassy
- A copy of every call was relayed to another cell phone number
- These were prepaid phones, bought over the counter for cash
- A key person was found dead, an apparent suicide, just after the attacks was detected

What Happened?

- Writing the intercept software took a great deal of skill
- Planting it took a very sophisticated hacking attempt or cooperation from an insider
- Various log books were destroyed
- There was good “tradecraft”
- Was it an intelligence agency? Which one?

Other Hacks?

- “Israeli companies, spies, and gangsters have hacked CALEA for fun and profit, as have the Russians and probably others, too” (*I, Cringely*, July 10, 2003)
- Major wiretap scandal in Italy: “A team of security consultants ostensibly hired to test the security of Telecom Italia’s security systems allegedly used Trojan horse malware and illegal wiretap techniques to spy on targets including Carla Cico, chief exec of Brasil Telecom, the Kroll investigative agency, and journalists Fausto Carioti and David Giacalone of Italian newspaper *Libero*.” (*The Register*, April 14, 2008)
- More?

We Told You So

- CALEA wiretaps appear to be *more* expensive than conventional ones
- As a result, they're used much less often than predicted
- The predicted security problems have indeed appeared

But. . .

- The FBI was right in their prediction: conventional phones would go away
- For various other reasons, some of the newer phone technologies are of more interest to the mob and other targets
- You need sophisticated technology to tap these calls, but the sophisticated technology is *inherently* buggy

What about Crypto?

- The FBI claims they’re running into encrypted files and conversations
- Except for Skype, evidence of trouble is at best scant
- They’ve almost always been able to “go around the crypto”
- Example: notes on desks with passwords

Hacking the Endpoint

- Various police agencies around the world have endorsed "remote search" capability
- The FBI has a rumored program called "Magic Lantern"
- Translation: they hack into your computer

Legal Hacking?

- Will firewalls become illegal?
- Or are there hidden back doors installed by Microsoft et al.?
- If so, who has the knowledge and keys to use them? Law enforcement? Which country's?

Cryptographic Key Escrow

- The Clinton administration once proposed “key escrow” — the government would have a back-up key to let them read any traffic encrypted with a special “Clipper” chip
- Other, similar, mechanisms were proposed as well
- None caught on, despite intense lobbying
- Some of these mechanisms had serious security flaws

Complexity

- On behalf of law enforcement (and intelligence agencies), we have added complex mechanisms to already-complex systems
- Some of these mechanisms have created very serious vulnerabilities
- This was not only predictable but predicted
- The government went ahead anyway…
- But — are their concerns legitimate? Are there better solutions?