

Security Implications of the Public Switched Telephone Network, with Q&A

Disclaimer: I work for a Midwestern telephone company as the senior network engineer. I run the world's largest and most popular free telecommunications database at <http://www.telcodata.us/>

During this talk, I officially speak for neither.

Additionally, I will not answer questions, on or off the record, that in my sole judgment may materially assist you in competing against either company. I am contractually prohibited from helping you compete with my employer. It's nothing personal.

Quick Disclaimer

- My experiences are for obvious reasons limited primarily to the United States regulatory environment
- However, Canada (and several Caribbean nations) participate in the North American Numbering Plan, and utilize the same SS7 networks, toll free and local number portability infrastructure and technology (in fact, many US switches are (well, were!) made by Nortel in Canada, and are largely the same equipment as Canada)
- Thus there may be circumstances where my information is not entirely 100% accurate for the Canadian market (specifically around tandem homing, ratecenters, and local call routing), but generally the information is applicable for both. Areas where they differ are subtle, and for the layman may be irrelevant, in fact.
- Where can I learn more about numbering and routing? <plug type="shameless"><http://www.telcodata.us> is a free resource (with paid downloads available) that can help you learn more about numbering, routing, and tandem homing. My apologies for the Canadian data being more limited, that's a factor of your regulatory requirements here that don't force the incumbent carriers to disclose quite as much as they have to in the US.</plug>

What are the threats?

- Technical
 - Telecommunications fraud (international arbitrage)
 - Network Compromise through misconfigured PBX hardware
 - Misuse of system to perform DoS/DDoS against someone on the PSTN
- Social Engineering
 - Caller ID Spoofing
 - Impersonation of internal staff
- Interception of call content or metadata
 - Sniffing of call signaling traffic
 - Sniffing of audio payload traffic
 - Good old fashion wiretapping

What are the big problems?

- Carriers trust each other.
 - Once you get onto the carrier to carrier wholesale interconnections, pretty much any security goes out the window
- Call completion is legally mandated
 - While I can offer a customer a service that provides them things like “blocking of known robodialers”, I have to offer it as a separate service you can subscribe to (though I don’t have to charge extra for that). Blocking calls generally is a no-no.
- Formats are often unvalidated
 - I can call my friends using a source # of “911” and many of them will have their phones freak out and go into “emergency callback mode” afterward for two minutes, locking out data. And the caller ID says “Emergency 911”
 - Calling from the numbers that come in your phone book, like how Sprint PCS in the USA adds their customer service # to everyone’s phonebook. I can call from that, and you’ll think I’m probably calling from Sprint.
 - I can call your desk from a 4 digit number, and it may be indistinguishable from an internal extension call. Grab a phone list from a large corporation, call someone using the internal extension of someone from finance, and good chances exist you might be able to get them to “verify the number on their corporate amex so you can update your records”. Yikes!

What are the big problems? (continued)

- “Canadian CNAM”
 - Yep, I just came to Canada and blamed Canada. In the US, there’s a distributed database, updated only by carriers, that defines your caller id with Name data. This is essentially non-spoofable. It’s also another way we engage in arbitrage, paying each other fractions of a cent for these lookups. Of course!
 - In Canada, it’s carried with each call in the GenericName parameter in SS7.
 - In the US, if you want caller ID with name from Canadian callers, you enable support for “Canadian CNAM” or “Trust caller id with name when sent”
 - Problem is you can *often* send it in the Facilities IE of a PRI, or in a SIP setup, and it gets trusted similarly for that reason, and you can do things like “US GOVERNMENT” as your caller ID and it’s trusted when it shouldn’t be, even on domestic calls with invalid source numbers.
 - SIP Interconnect is making this commonplace too. Comcast for example requires any phone company exchanging intercarrier traffic over SIP to send the caller id with name data in the SIP “From” and/or Remote-Party-ID or other similar fields.

Intercarrier Compensation issues

- Carriers engage in massive arbitrage that sometimes basically amounts to fraud on a regular basis
 - If you can connect to my customers on a wholesale basis, I'm legally required to charge all carriers the same rate for carriage to my end customer. So how is it you're using a third party to complete calls to me rather than go direct, when we're in the same area? How can it be economical to send calls through a middleman when you can go direct? What is that middleman doing to get the calls to me to make them cheaper? (yes, just keep whistling with your eyes shut and point at the other carrier)
 - MCI/Worldcom fraud incident: MCI passed domestic US calls to their canadian subsidiary, then back into the US to make them appear international when they were actually in-state calls (in-state calls often have the highest intercarrier compensation rate)
 - We fight each other over fractions of a cent times a million transactions (think *Office Space* or *Superman 3*). When we see fraud between each other, we let our finance teams and lawyers argue about it. They do cost/benefits analysis to see if it's worth it. In the meantime, I still see legitimate traffic taking illegitimate paths and I can do nothing to stop it.

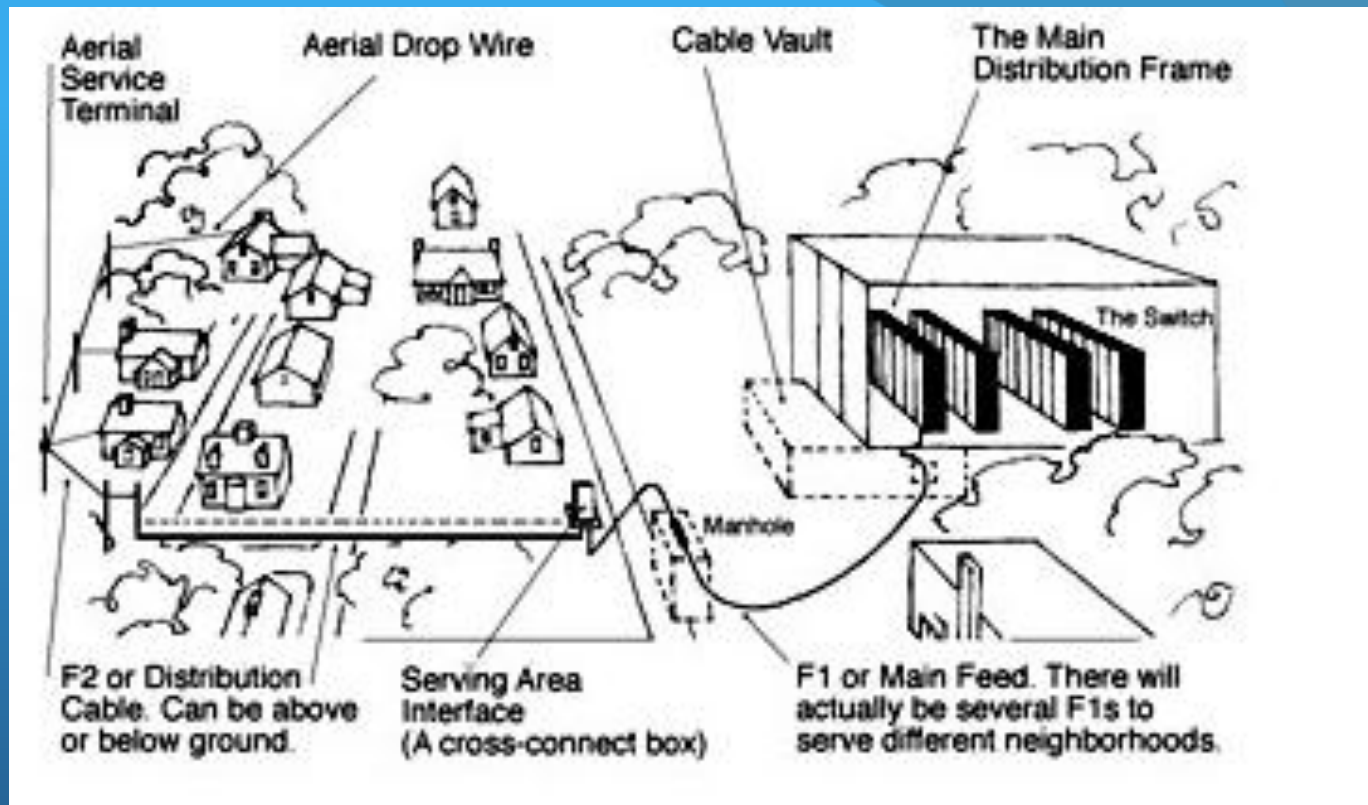
What does this mean to me?

- As your carrier, I'm used to seeing calls coming into my network for you, my customer, through pretty much any unorthodox ways you can think of.
- Even if I think the originating carrier is engaging in fraud to lower their call completion costs into my network, I have to complete the call to you anyway.
- Effectively, there's no way for me to firewall garbage that comes in the carrier side
- That means ultimately, you can't trust what your caller ID says, or that the call even comes from the same general area you think it does.

How does the phone network function generally?

(Not a silly question, I promise!)

Local Loop - Outside Plant



Credit: <http://www.privateline.com>

Cross connect boxes and service terminals are generally unlocked (as in they entirely lack locking mechanisms besides the customary 9/16" socket wrench to keep kids out). It is easy to listen in at these points, it's equally easy to double splice your line onto a disused pair (aka a Bridge Tap) and monitor your line from elsewhere in the neighbo(u)rhood.

POTS Network Interface Device (a/k/a Demarc)

Used to provide a demarcation point between your wiring and the phone company's wiring



T1 Network Interface Device (Outdoors)

The door contains the smartjack.

These posts contain the low level DSX1 signal you're accustomed to seeing as a T1 line, and are safe to observe/touch/whatever. They operate at roughly -3v to +3v typically.

There is a transmit and receive pair.





T1 Smartjack (Used internally and externally, converts HDSL2/HDSL4 to and from T1 signalling)

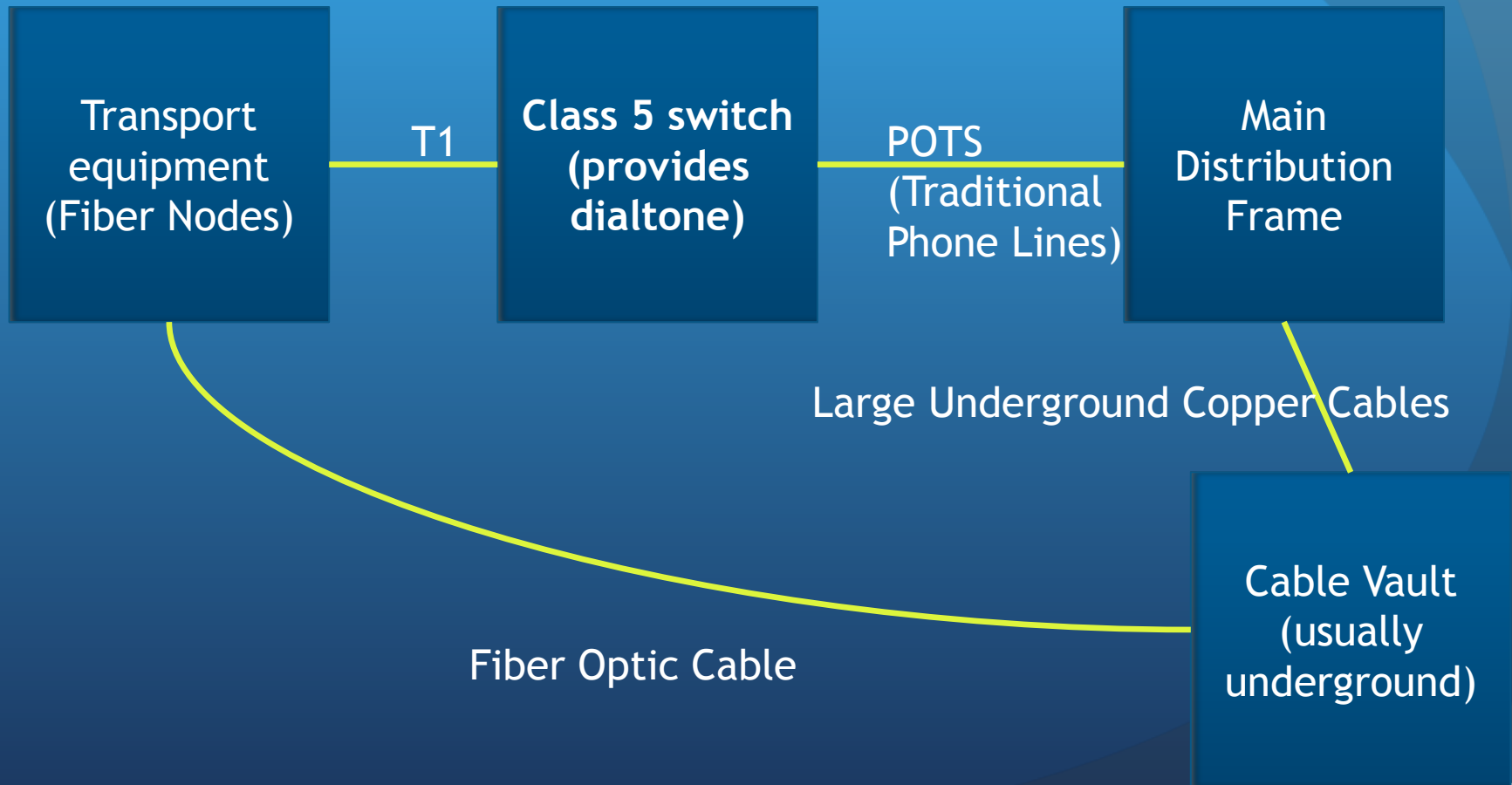
These are powered from the central office or remote terminal typically using roughly 130v DC on the pair. Tread with care, it really hurts if you touch that.

These are controllable inband to allow for all sorts of fun stuff, and that serial port is typically unpassworded and allows for additional control over the circuit. (There is a common idea in the telecommunications industry that the risks of mean time to repair being increased outweigh the risks of leaving the device unprotected. Many devices such as smartjacks, DS3 multiplexers and similar equipment lack passwords entirely or are set to defaults for this reason. Sounds risky but generally the tradeoff IS best practice, even with security in mind). Large equipment and wiring vaults are often completely insecure if you have a 9/16" socket wrench.

Serious transport gear however is generally better protected.

When you see this, the signal is actually traveling over HDSL on the copper lines (which runs at roughly 2mb, and allows for better distance, forward error correction, etc) and being translated back to T1 at your site. 99.9% of T1 circuits are delivered this way.

General Central Office Layout



Cable Vault

LOG IN or JOIN

The Big Story: Samsung Galaxy S4 review



Photo: The Verge - "Into the vault: the operation to rescue Manhattan's drowned internet"
<http://www.theverge.com/2012/11/17/3655442/restoring-verizon-service-manhattan-hurricane-sandy>

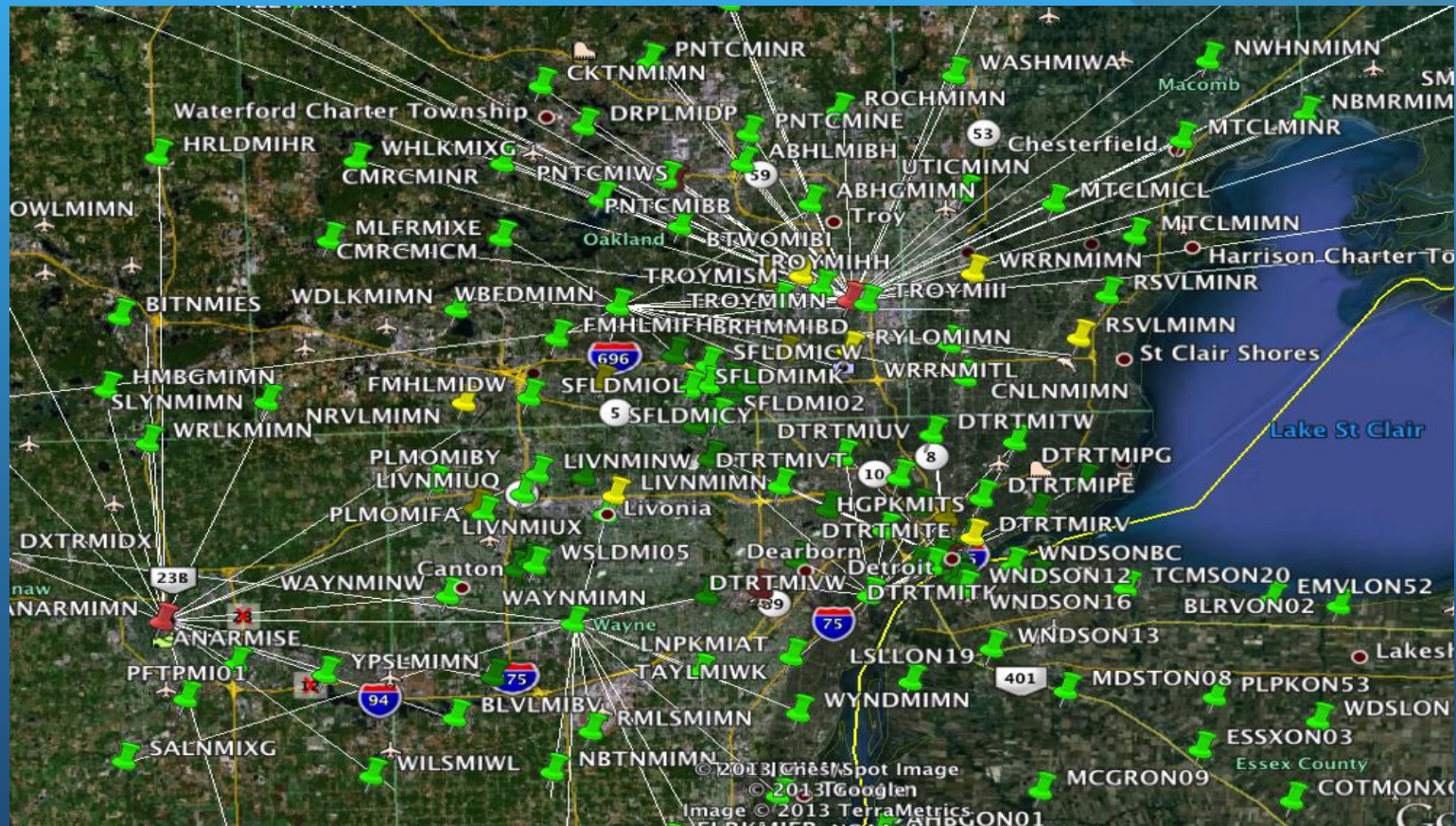
Manholes



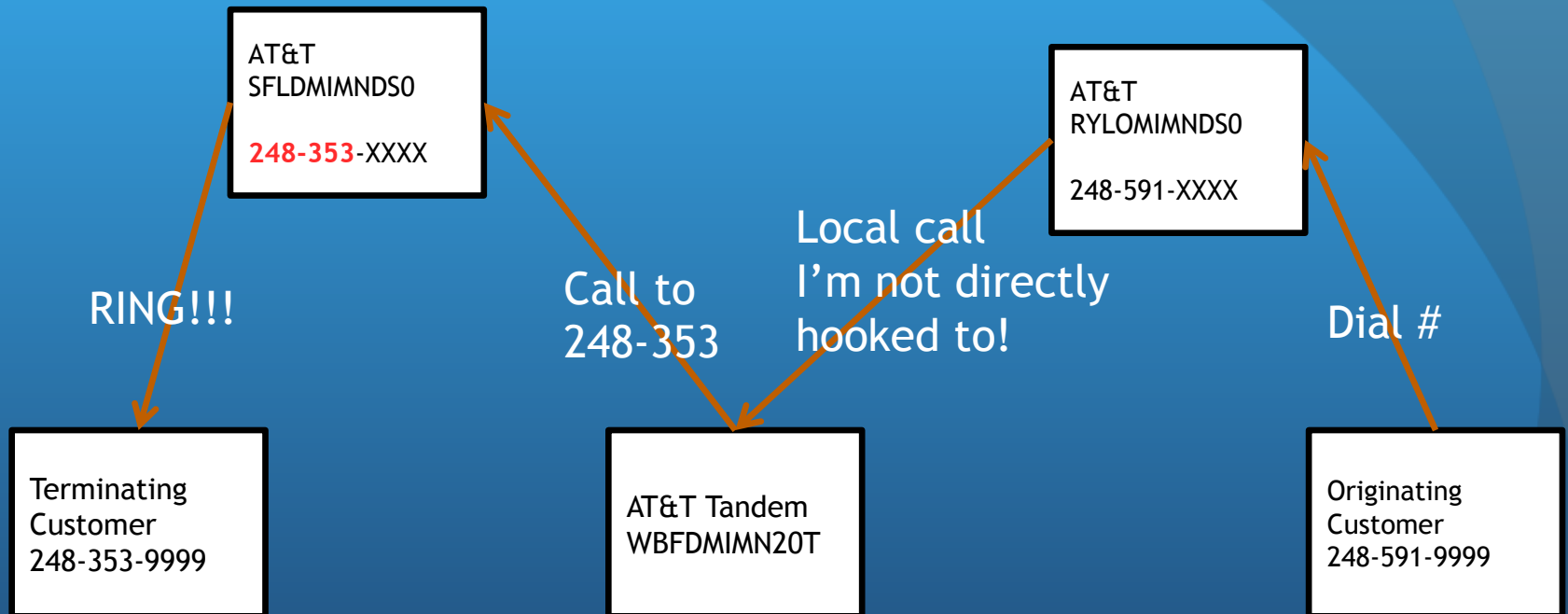
Photo: The Verge - "Into the vault: the operation to rescue Manhattan's drowned internet"
<http://www.theverge.com/2012/11/17/3655442/restoring-verizon-service-manhattan-hurricane-sandy>

The Tandem Network

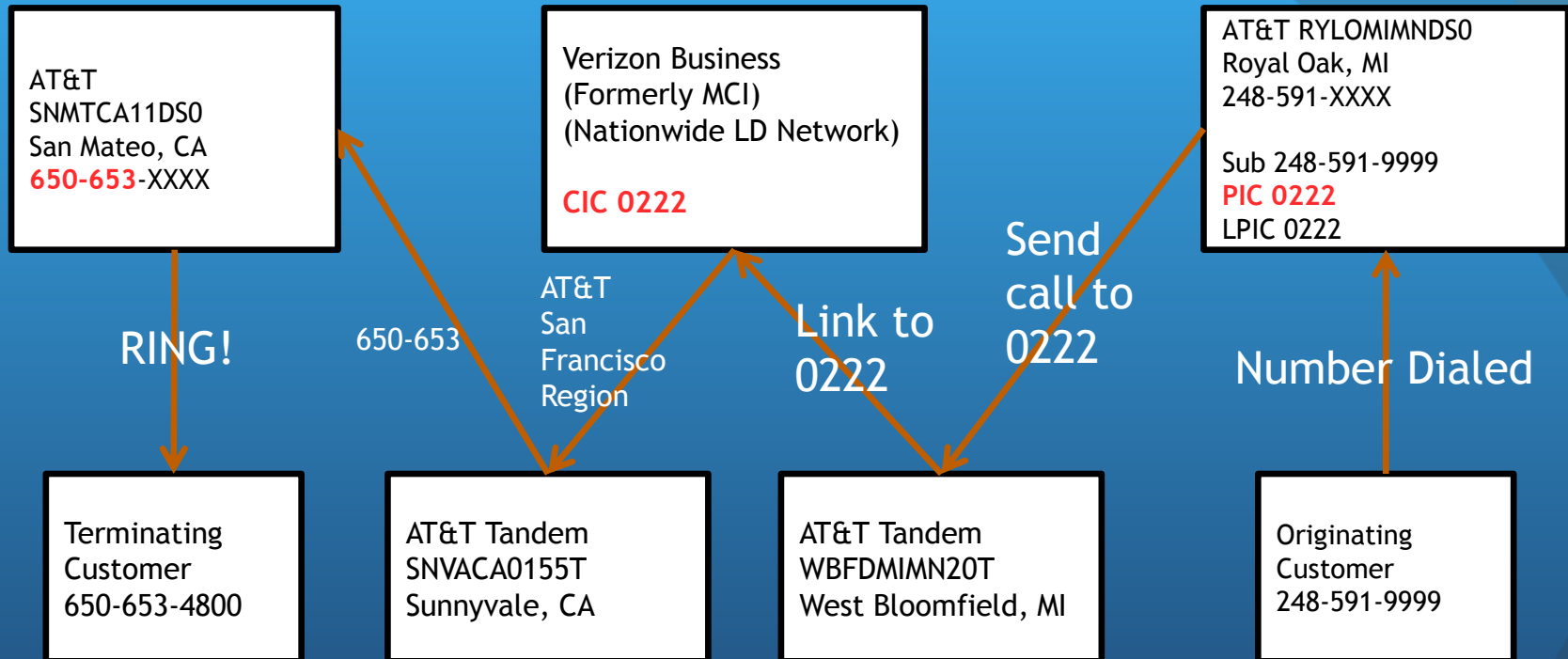
(How phone companies interconnect)



Local Call Routing



Long Distance Call Routing

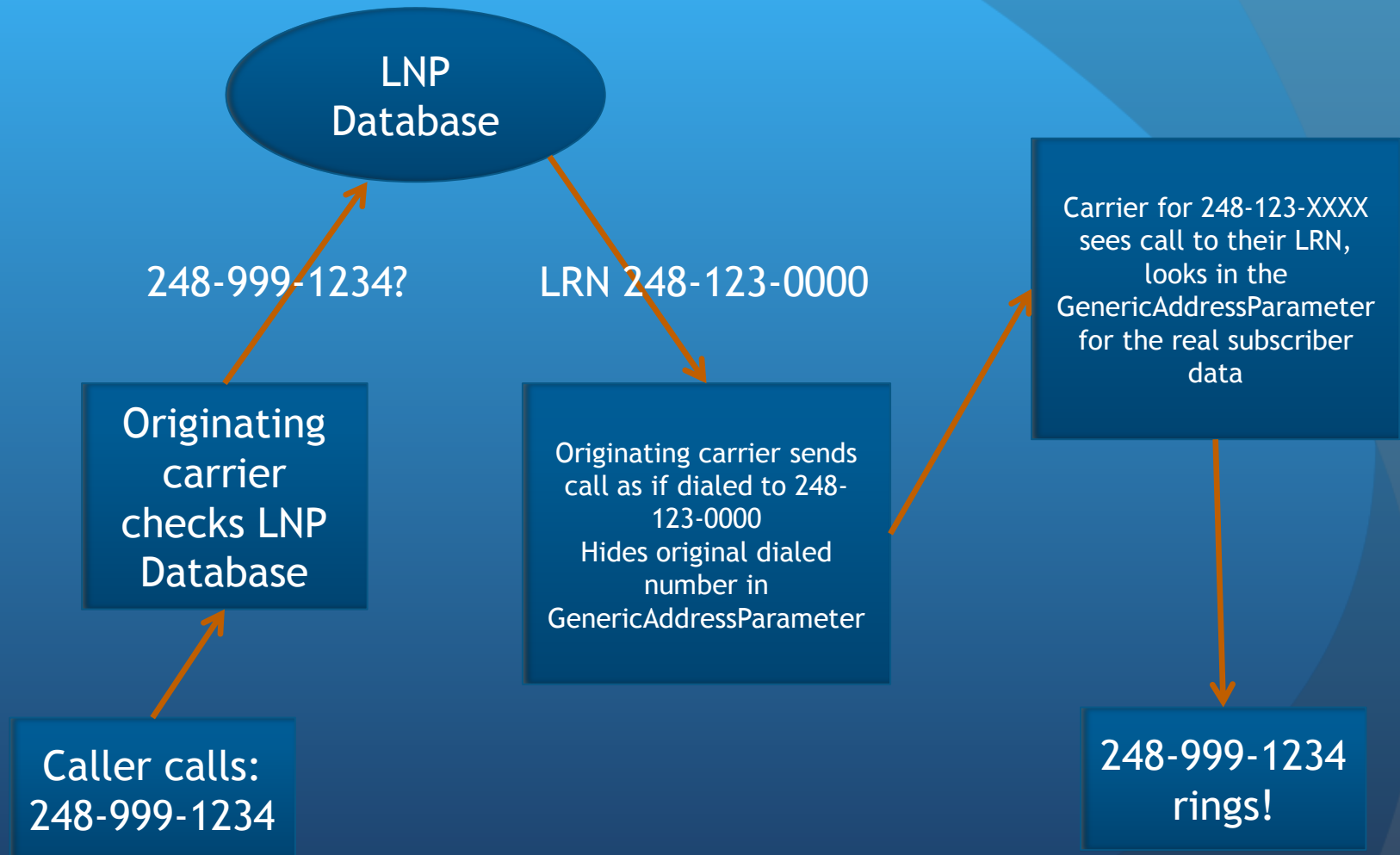


Customer is subscribed to Verizon Business for Long Distance

Local Number Portability

- Customer with working phone number decides to change phone company. Places order with new company, provides bill information for old provider
- New provider (winning carrier) coordinates the port out with the old carrier (losing carrier)
- Winning Carrier builds subscription in NPAC requesting the number be routed to them
- Losing Carrier (optionally) builds matching subscription acknowledging portout.
- Winning Carrier prepares service for activation
- Winning Carrier Presses “Activate” button in NPAC interface, SV Broadcast goes out to all LSMS databases immediately informing them of new carrier information
- (Losing Carrier also sends a records release to the 911 network allowing the winning carrier to claim the 911 record and update as necessary)
- Old carrier disconnects service and issues final bill.

Local Number Portability



Local Number Portability

- Works like an unencrypted VPN Tunnel in a way. The call is retargeted at a special phone number that means “This call is to a number ported to your phone switch”
- The intermediate network simply sees a call to the LRN and routes accordingly (it need not know about LNP at all!)
- The switch that owns the LRN’s NPA-NXX prefix knows this special number means “ported call inbound” and knows to look in the GenericAddressParameter field for the actual number that was called.

It's all about the Benjamins

- So I've mentioned how carriers commit fraud (or just have honest misconfiguration that's difficult to fix) how does this come into play for you?
 - Caller ID Spoofing - "CallingPartyNumber" field is not validated and essentially can't be. If a carrier lets it into the network, there's no way to tell the veracity for sure. (yes, there's a presentation indicator that says the number is user specified or not, but that's not even consistently set)
 - International Arbitrage
 - International calling dictated (regulated is a strong word here) by ITU (which is a treaty organization).
 - The rates for one country calling another are set in an international tariff
 - The rates, when published, are non negotiable and are payable under treaty, with no method for declaring the records fraudulent as long as the calls took place.
 - This is ripe for abuse in banana republics that have high rates because they are connected only by satellite, for instance.
 - Revenue share used to be common in USA, still very common in these very small areas.
 - If someone sets up a revenue sharing number, there's no recourse. It's not even technically illegal. Your carrier must pay those even if the customer's phone system was hacked and dialing revenue share numbers.
 - What IS illegal? Well, your stuff getting hacked is illegal in your country, but what about if someone in Turkey gets money from East Timor via a third party carrier in Pakistan when your PBX gets hacked? Who has jurisdiction? How are you going to get records to prove it?

In case you think I'm kidding about how open they are

Value-Added, IVR and Tele... x interpremium.net/Domestic x
interpremium.net/Domestic%20Premium%20rate.pdf

02

Call TV PRN solutions

Available in Australia, Austria, Belgium, Croatia, Czech Republic, Finland, France, Germany, Greece, Hungary, Italy, Netherlands, Poland, Portugal, Slovakia, Spain, Sweden, Switzerland, Tunisia, UK



03

National Number

Available in Australia, Austria, Belgium, Czech Republic, France, Germany, Greece, Hungary, Ireland, Italy, Norway, Poland, Portugal, Spain, Sweden, Switzerland, UK



Our solutions have been specially designed to meet any need. No matter where you are and what service you require, we can come up with a solution tailored for you. Pay-per-minute and pay-per-call solutions.

Payouts vary from €0.15 to €1.50 ppm/ppc. Fast payment terms. SIP-forwarding or PSTN-forwarding to any other DID possible.

contact@interpremium.net

When you want money to get away somewhere nice, just get someone to call Liberia a few million times. Note the amount of revenue they are sharing with you... The reasons for abuse are very clear

Special Promotions

Grenada - \$ 0.035/min !!!

45 days EOM

test number: +14734026600

Grenada - \$ 0.15/min !!!

Every 500

test number: +14739016600

UK - £ 0.06/.03/.01/min !!!

Every 500

test number: +447021759299

Spain - € 0.035/min !!!

Every 500

test number: +34902735110

Liberia - \$ 0.14/min !!!

Every 500

test number: +231330550259

Malawi - \$ 0.07/min !!!

Every 500

test number: +265888704667

UK - £ 0.06/min !!!

40 days EOM

test number: +447589942350

UK - £ 0.06/min !!!

40 days EOM

test number: +447589972700

So how does this happen?

- Old School
 - How many people have office voicemail systems that can turn on call forwarding remotely? How many people have their mailbox password the same as their phone number or DID or extension (ie: very guessable)? (answer: LOTS)
 - Cleaning staff walks over and sets your call forwarding on at your desk.
- New School
 - How many people have misconfigured SIP access to their systems? Do you have IP extensions on your PBX that use registration? Do you lock down who can access port 5060 externally? Are your passwords secure passwords, or are they the extension of the handset?
 - How many misconfigured PBX (especially Cisco) exist?

Fixes

- Disable remote access to setting call forwarding on extensions (some systems support this, a few BY DEFAULT (yay!))
- Use secure passwords for voicemail boxes
- Ask your phone company to disable international calling if you don't use it. If you do (sparingly) ask if you can set up “validated account codes” - some carriers can do this
- (What about 900/976 blocking? There's no carriers in the US that will route 900 calls anymore except for a small embedded base in verizon business. I honestly have never routed 900-xxx-xxxx because at this point, I'm not certain where to even route it)
- Use your PBX to restrict international calling to only extensions that use it failing all else
- AND PROTECT IN LAYERS. WHY NOT DO ALL THESE THINGS?~

What about SIP?

- Great question! This is the new school, and it's quickly become the rage because there are so many who make ghastly mistakes when setting up PBXen, especially Cisco Call Manager.
- What should I do?
 - Good:
 - Set up IP access lists restricting access to port 5060/UDP to places you expect. Barring that, block the countries you don't using IANA's /8 list. Not getting SIP requests from Latin America? Drop LACNIC space.
 - Disable unused protocols or filter them. Not using H323 or SCCP? Disable them.
 - Can you get away with using SIP/TLS? Do it. It will help certain kinds of spoofing attacks you can do leveraging the SIP headers to get around your carefully crafted firewall rules. SIP/TLS support usually is godawful, but worth a try getting it working
 - Best:
 - Disable hairpinning - make sure that your phone system cannot take in a call via a SIP trunk and send it back out. Cisco dial-peer configs that say essentially "route 7xxx to call manager, route 91nxxnxxxxx to PSTN" are the worst. One misconfiguration and I can bounce a call off you from anywhere starting with a 9 in front, and you'll happily toss it to your phone company as if it was your idea. You can do this in a cisco by prepending digits when a call comes in from a trusted peer (like insert 9997 before the number they're calling) and then match on 999791NXXNXXXXXX and then strip the 9997), you can get around this by guessing the number you prepend, but it'll stop the vast majority of scammers, and help prevent you from looping misconfigured calls!
 - Custom asterisk - have your phones use one context, calls from your carrier use another. Be careful about what can call what

Call Interception

- I'm not talking about "Lawful Intercept" here - CALEA and its ilk are well known.
- How is rogue call interception done?
 - "Buttset" - a lineman's handset clipped on any part of the analogue line will let you passively listen to analog "POTS" lines.
 - In-room bug. High value targets might end up with getting their handset bugged by someone committing espionage, or a state actor.
 - Digital circuits can be intercepted too! Your PRI doesn't make you safe.
 - SIP - That SDP can have audio going anywhere. If you can get access to the sequence numbers and call-ids of an ongoing transaction, you can spoof a re-invite in dialog in both directions putting you as the SDP IP address, and you relay while recording
 - Or hack it, or sniff it, or MITM the entire thing, or or or or or. It's just UDP data in a standard RTP format you can decode with wireshark.

But intercepting T1 is expensive

It's not 1994 anymore. This 1970s technology (T1 is really that old!) has dozens of portable devices that can drop audio channels out, record call metadata, etc on ebay. This is just a random grab of a common model. Plug these into the monitor port of a smartjack with bantam cables, and you're good to go without making a peep.

Value-Added, IVR and Tele... x t-berd 224 | eBay x

www.ebay.com/sch/i.html?_from=R40&_trksid=p2050601.m570.l1313.TR0.TRC0.H0.Xt-berd+224.TRS0&_nkw=t-berd+224&_sacat=0

Other Industrial Test Equipment
More ▾

See all categories

Condition see all
☐ New (1)
☐ Used (55)

Price
\$ to \$ >>

Format see all
☒ All Listings (56)
☐ Auction (3)
☐ Buy It Now (54)

Item Location see all
☒ Default
☐ Within
100 mi of 48009 >>
☐ US Only
☐ North America
☐ Worldwide

Delivery Options see all
☐ Free shipping
☐ Free In-store pickup

Show only see all
☐ Returns accepted
☐ Completed listings
☐ Sold listings

More refinements...

Did you mean: **t bird 224?** (1 items)

Model T-Berd 224 10 Options!
\$75.00
or Best Offer

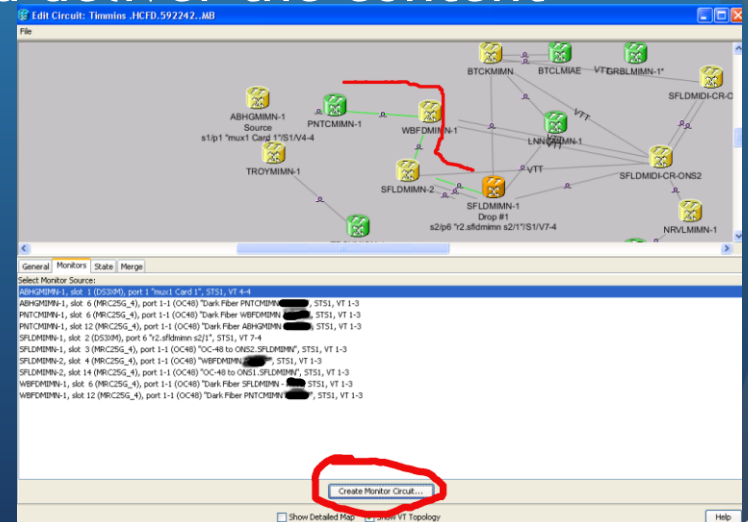
TTC / Acterna / JDSU / WG (Wandel Goltermann) T-BERD 224 PCM Analyzer
\$49.00
0 bids
2d 11h left (Monday, 3PM)

TTC T-BERD 224 PCM ANALYZER W/ 5 OPTIONS & EXTRAS! TESTED & WORKS!
\$475.00
or Best Offer

TTC ACTERNA T-BERD 224 PCM ANALYZER SS7 LOADED WITH ELEVEN OPTIONS ~ 41500 12709
\$525.00

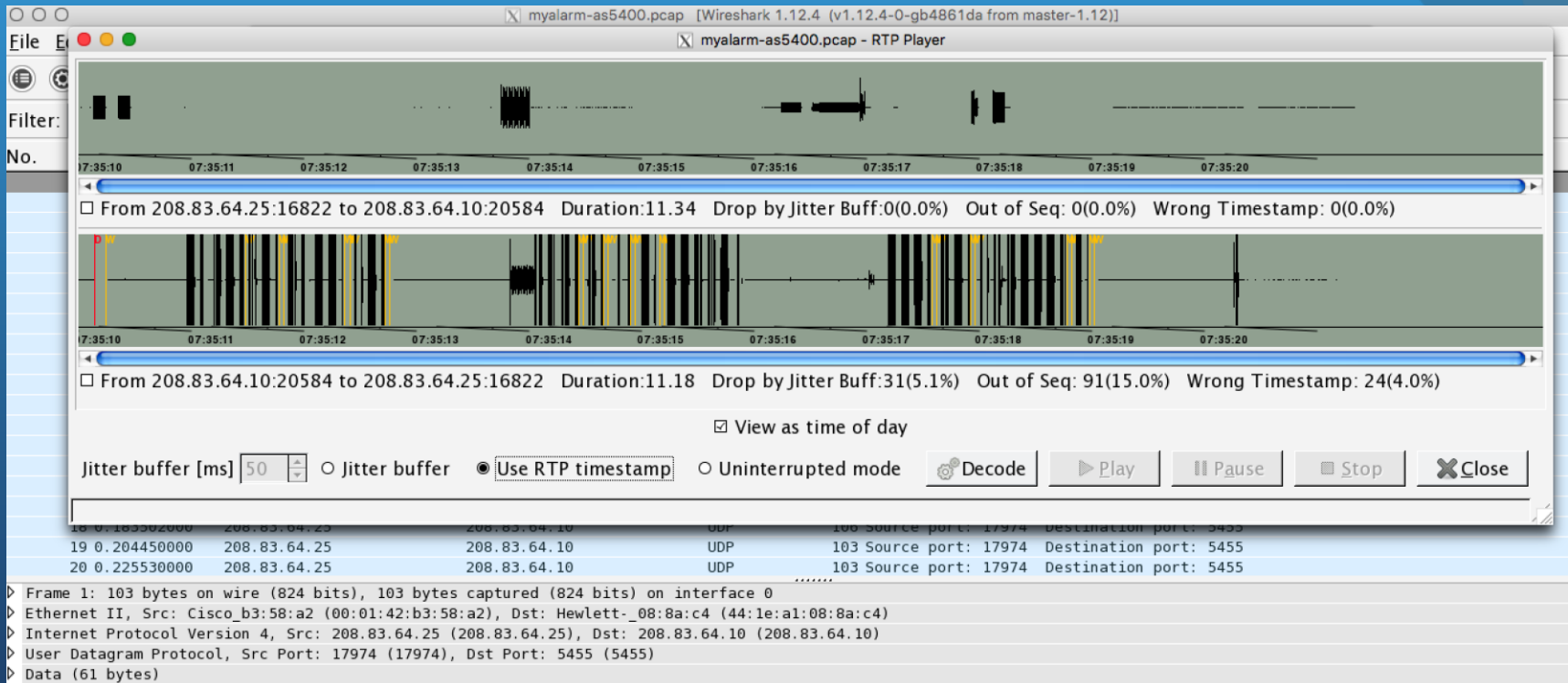
But you'd have to get to my smartjack!

- Or build a HDSL2 -> T1 -> HDSL2 rig out of commercially available parts for roughly \$300 (not telling you what you need to do this, but it's relatively trivial)
- Or make friends with a disgruntled telco tech. Where do you want me to place the wiretap at? I can monitor from any part of the circuit, and deliver the content anywhere!
- (no, I won't do this for you IRL)



SIP: It's just a ton of UDP

Even multimillion dollar telcos fling around pcap files for debugging. It just works. No fancy test sets needed.



(bonus shot, ladder view)

myalarm-as5400.pcap - Graph Analysis		
Time	208.83.64.10 208.83.64.25	Comment
68.201099000	INVITE SDP	SIP From: "2484187999" <sip:2484187999@208.83.64.10 To: <sip:8663494902@208.83.64.25
68.216558000	100 Trying	SIP Status
74.690741000	183 Sessl	SIP Status
74.821448000	RTP (g711	RTP Num packets:567 Duration:11.319s SSRC:0x180B4019
74.825270000	RTP (g711	RTP Num packets:4 Duration:0.056s SSRC:0x38EB63C8
74.892038000	200 OK SD	SIP Status
74.892393000	ACK	SIP Request
74.901589000	RTP (g711	RTP Num packets:65 Duration:1.344s SSRC:0x38EB63C8
76.265628000	RTP (telep	RTP Num packets:5 Duration:0.040s SSRC:0x38EB63C8
76.325693000	RTP (g711	RTP Num packets:14 Duration:0.259s SSRC:0x38EB63C8
76.605512000	RTP (telep	RTP Num packets:6 Duration:0.060s SSRC:0x38EB63C8
76.685623000	RTP (g711	RTP Num packets:25 Duration:0.479s SSRC:0x38EB63C8
77.191268000	RTP (telep	RTP Num packets:6 Duration:0.057s SSRC:0x38EB63C8
77.269227000	RTP (g711	RTP Num packets:14 Duration:0.256s SSRC:0x38EB63C8
77.545700000	RTP (telep	RTP Num packets:6 Duration:0.060s SSRC:0x38EB63C8
77.625774000	RTP (g711	RTP Num packets:82 Duration:1.619s SSRC:0x38EB63C8
79.265634000	RTP (telep	RTP Num packets:5 Duration:0.040s SSRC:0x38EB63C8
79.328740000	RTP (g711	RTP Num packets:8 Duration:0.136s SSRC:0x38EB63C8
79.485703000	RTP (telep	RTP Num packets:6 Duration:0.060s SSRC:0x38EB63C8
79.566867000	RTP (g711	RTP Num packets:8 Duration:0.138s SSRC:0x38EB63C8
79.725546000	RTP (telep	RTP Num packets:5 Duration:0.040s SSRC:0x38EB63C8
79.785552000	RTP (g711	RTP Num packets:10 Duration:0.180s SSRC:0x38EB63C8
79.985538000	RTP (telep	RTP Num packets:5 Duration:0.040s SSRC:0x38EB63C8
80.045653000	RTP (g711	RTP Num packets:118 Duration:2.339s SSRC:0x38EB63C8
82.405703000	RTP (telep	RTP Num packets:6 Duration:0.060s SSRC:0x38EB63C8
82.485753000	RTP (g711	RTP Num packets:13 Duration:0.239s SSRC:0x38EB63C8
82.745674000	RTP (telep	RTP Num packets:5 Duration:0.040s SSRC:0x38EB63C8
82.805686000	RTP (g711	RTP Num packets:40 Duration:0.779s SSRC:0x38EB63C8

Takeaways

- Wiretapping - if you can touch it you can own it
 - Done properly, VoIP can be MORE secure than other methods. (SIP/TLS with SRTP, rather than IPSEC VPNs, for quality's sake please!)
- Everything is a computer now. Your desk phone has a webserver inside. Vulnerabilities in things like busybox, dropbear, and small webserver projects take on a whole new light!
- Technical considerations for international fraud are increasing considerably. Determine if you REALLY need international, if so, can you get away with account codes? Lock down international to certain handsets?
- Voicemail - Still a threat all these years later - security for this shouldn't be an afterthought
- End user training - Protect your end users by training them how to identify internal calls vs external ones. Abuse this, play with it, and see what you can do. Social engineering can take on whole new levels of danger.
 - Ideally, provide a second factor of authentication in your organization to figure out internal vs external threats. Consider things like adding a factoid to your exchange GAL that people can challenge a new caller with, or some sort of companywide shibboleth that changes monthly... If your company is too big for people to recognize people, you may need a new way to authenticate internal callers.
 - Did you spend big money on a session border controller or sip proxy to work around NAT issues? UTILIZE IT to flag invalid caller ID (usually you can write a rule to do this, check your manual).
- Configure your PBX correctly and firewall it. Disable unused services
- As the barrier for entry for new carriers is lowered (see IP interconnection in the US) this situation is unlikely to get better because not everyone starting up these companies understands the risks (hopefully some of them are at least thinking about the kind of features they extend to customers, making sure SIP-I stuff is disabled toward their own customers, etc)