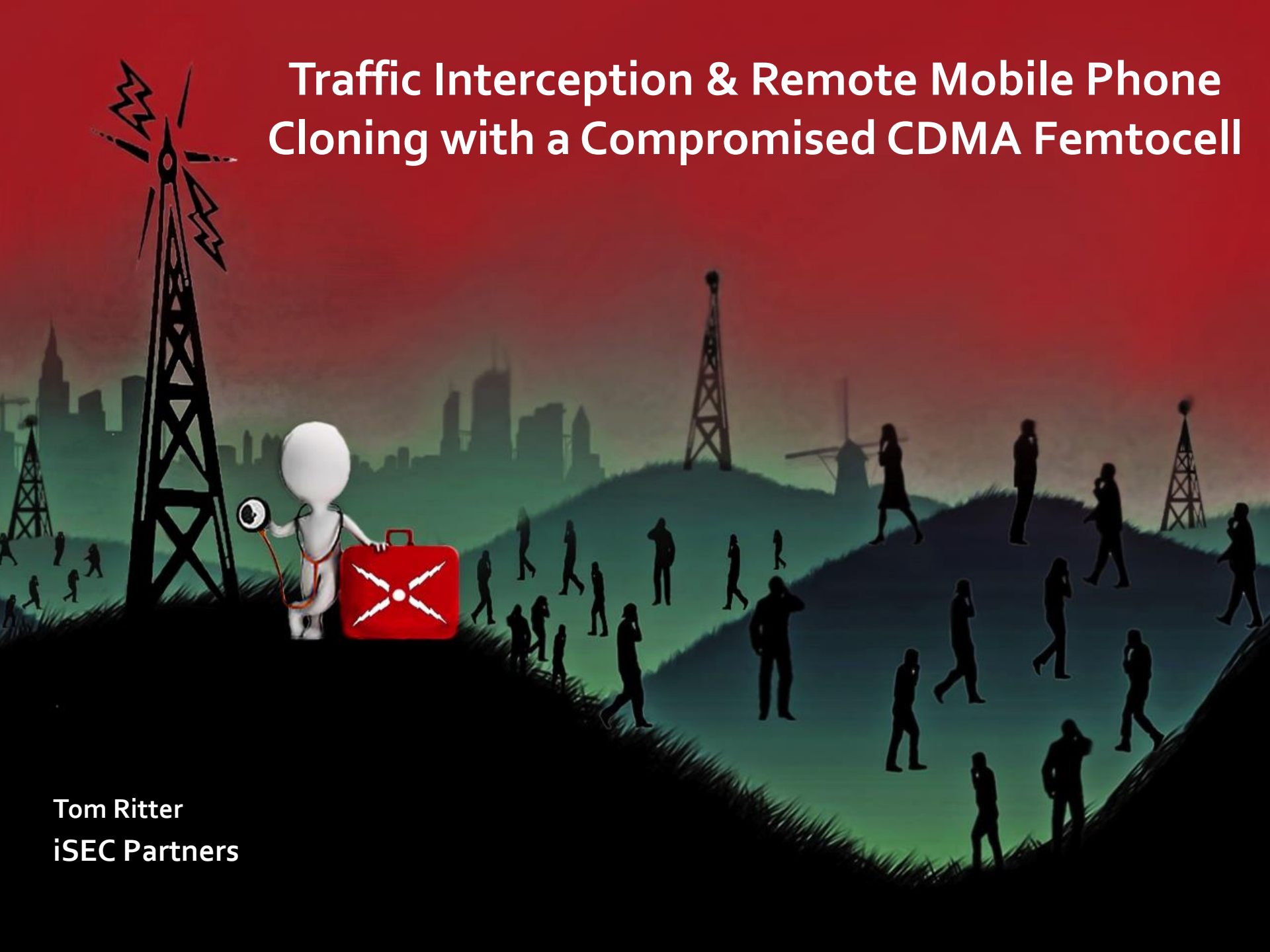
Traffic Interception & Remote Mobile Phone Cloning with a Compromised CDMA Femtocell



Tom Ritter
iSEC Partners

Full Disclosure

iSECpartners
part of nccgroup

- Disclosed vulnerabilities to the carrier early December
- They worked extremely hard, over Christmas, to prepare a patch
- All vulnerabilities disclosed in this presentation have been patched
- We do have architectural concerns around femtocells

Prior Art

iSECpartners
part of nccgroup

- BH 2011 "Femtocells: a Poisonous Needle in the Operator's Hay Stack"
  - SFR Femtocell (2nd biggest operator in France)
- THC: Vodafone (2010/2011)
- RSAXVC & Doug Kelly (Bsides KC 2011)
  - Rooting
  - Cable construction
- "Do It Yourself Cellular IDS" (Black Hat 2013)

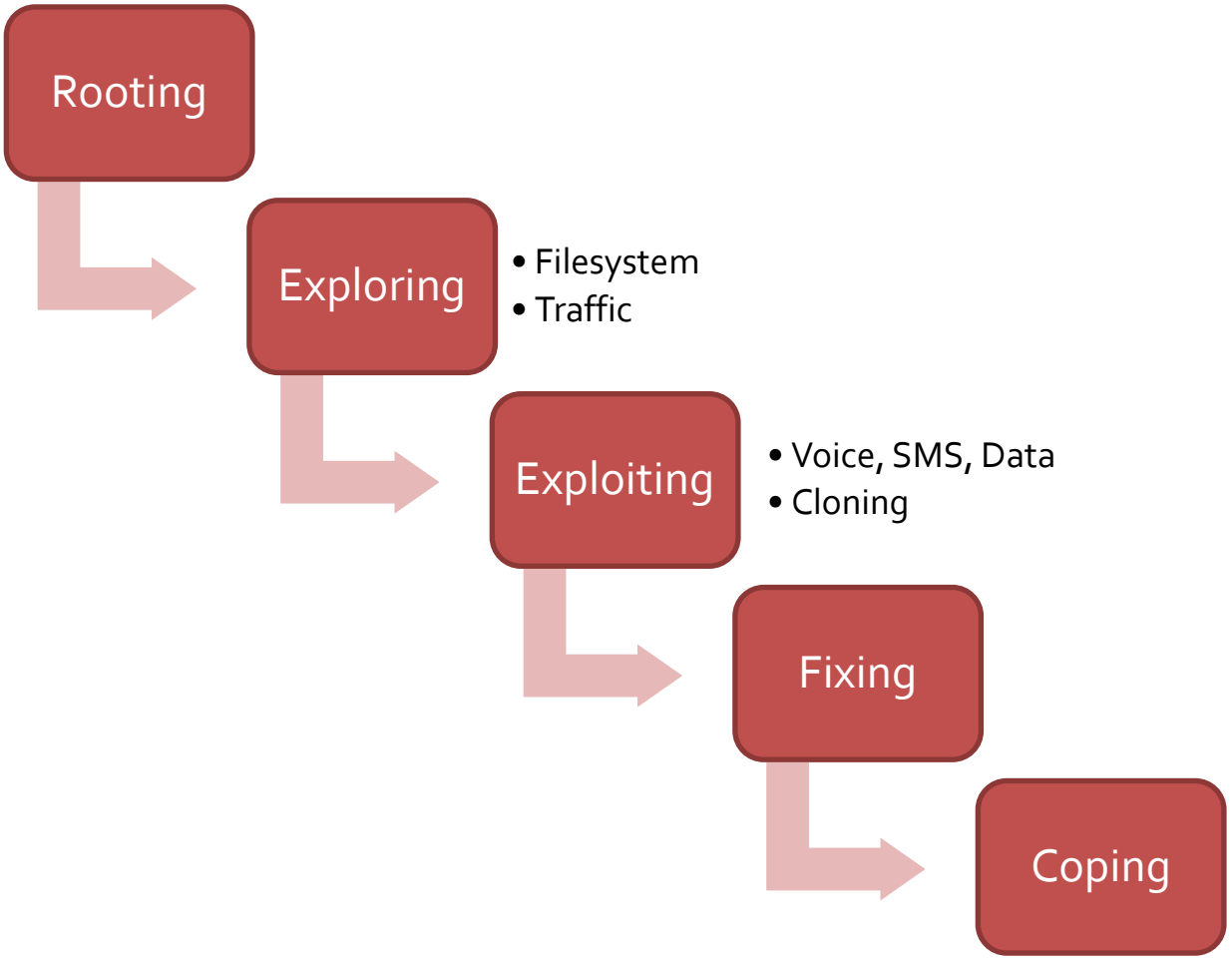
Our Focus

iSECpartners
part of nccgroup

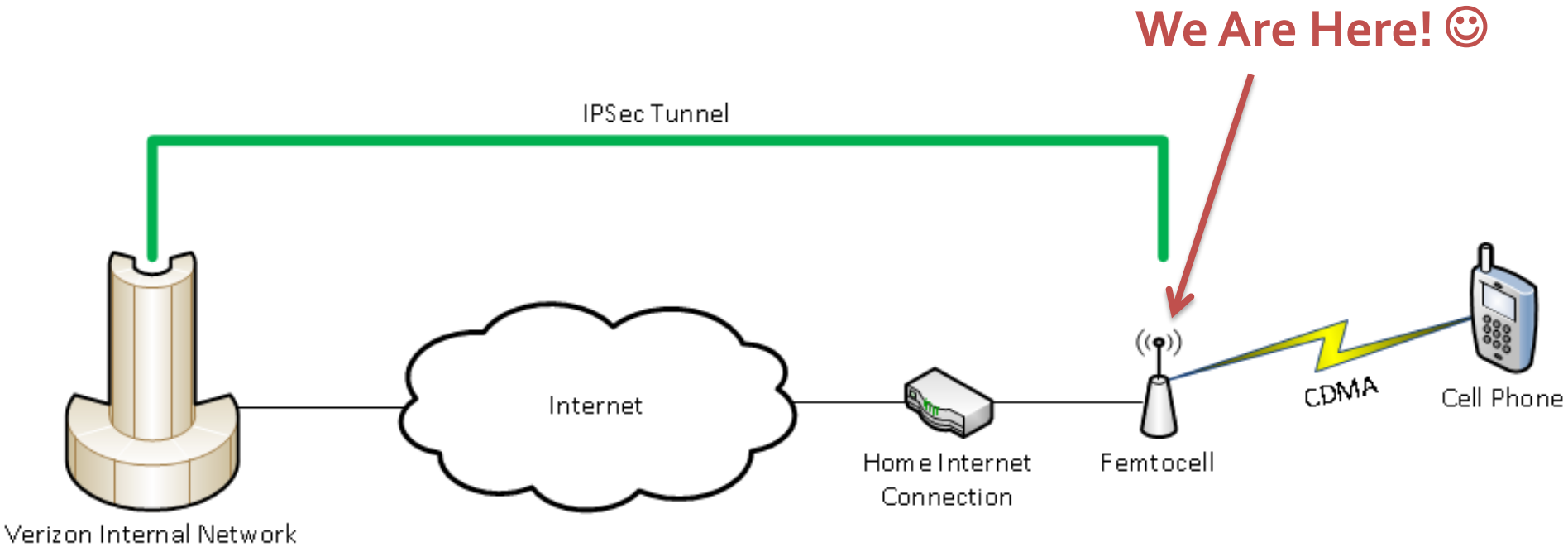
- North American Carrier
  - 3G
  - CDMA
- Customers affected
  - Roughly 1/3 of the population of the US
- Phone Calls & SMS
- MMS, Data Man-In-The-Middling, SSL Stripping
- Cloning

Agenda

iSECpartners
part of nccgroup



General Architecture



Rooting the Femtocell(s)

SCS-26UC4
(Older)

SCS-2U01
(Newer)

SCS-2U01 Hardware

- Faraday FA626TE ARM v5TE processor
  - on Samsung UCMB board
- OneNAND flash memory
- Lattice FPGA
  - Presumably for DSP
- GPS antenna
- CDMA antenna
  - 2G/3G
- Ethernet
- HDMI Port

Console Port

- HDMI port

Custom Cable

- USB FTDI + HDMI =

Wireless Signal Range

- Approximately 40’
- Environmental factors
- Adjust signal strength
- Amplify

No User Interaction

iSECpartners
part of nccgroup

- This is ***not*** like joining an open WiFi network
- Your phone associates ***automatically*** with no* indication
- We don't hack phones… at least not today

Console Access!

iSECpartners
part of nccgroup

- Physical Access to the Device
- Connected a console cable…

- SCS-26UC4
  - Startup delay: "Press any key to interrupt boot"
- SCS-2U01
  - Magic sysreq + i

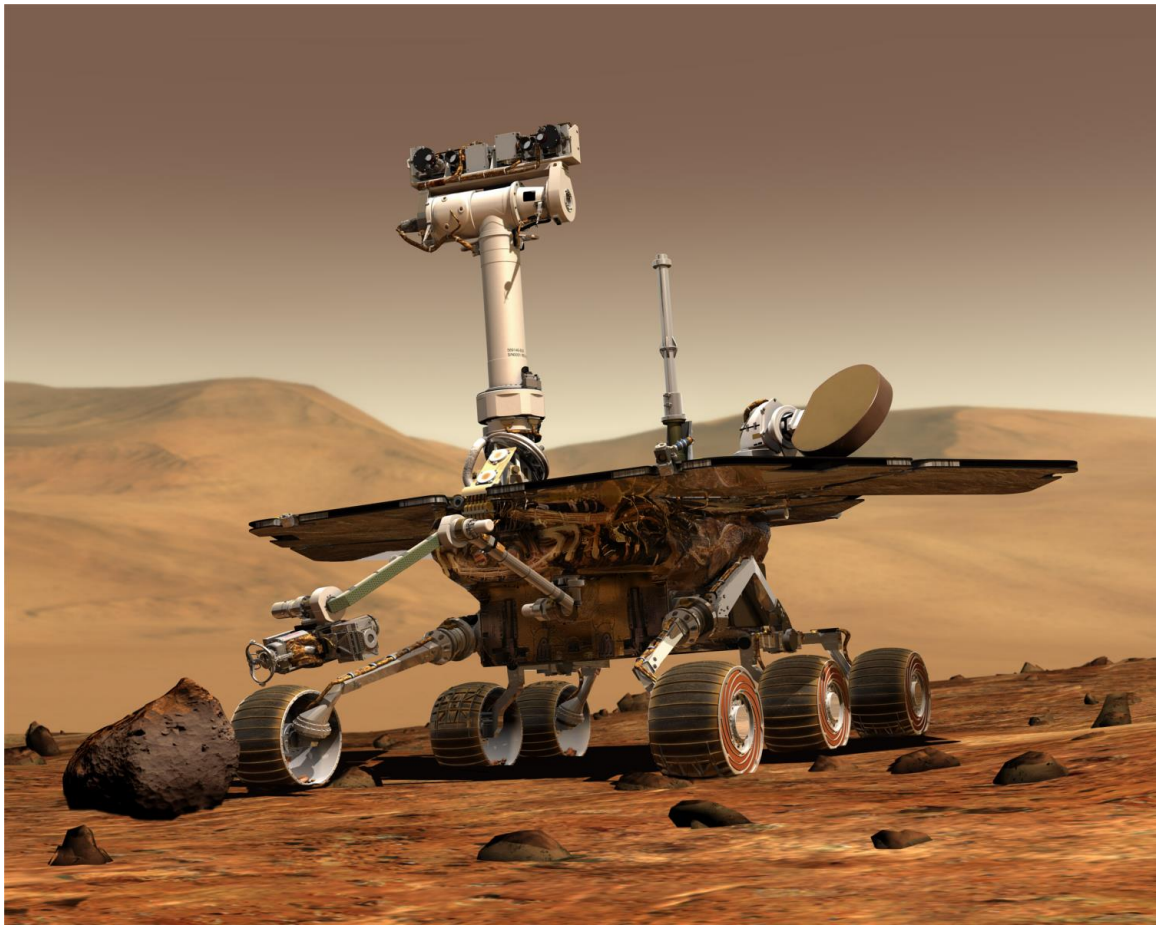
Console Access: Patched

iSECpartners
part of nccgroup

These mechanisms to obtain root no longer work

(But may be useful on other embedded devices)

Exploring the Femtocell



Filesystem

iSECpartners part of nccgroup

- MontaVista Linux 5, 2.6.18
  - (Released Sept, 2006)
  - Custom kernel, drivers, software
- /mnt/onand
  - Custom application binaries
  - uimhx, cmbx, cdhx, agent, vpn
- Keys, passwords, etc
  - /etc/shadow
  - /app/vpn/quicksec.xml

I am root, but…

iSECpartners
part of nccgroup

- Difficult to work in terminal console
- No easy way to edit files
  - No text editor
  - Reduced to find/replace inside of files using 'sed'
- No remote access via SSH
  - Config file & firewall prevent it

- Find/Replace to edit the SSH configuration, drop the firewall, log in remotely

Be Persistent

iSECpartners
part of nccgroup

- Filesystem is pulled from firmware every single time
  - Any changes disappear on reboot
  - Have to edit firmware and reflash?
- Until we noticed…
  - Persistent filesystem location
  - /mnt/onand

Be Persistent

- Read every single startup script until…

That's the part of the filesystem we can persist in!

```
if [ -f /mnt/onand/.ubirc ]; then
   echo 'DEBUG MODE STARTUP is TARTTING....'
   . /mnt/onand/.ubirc
```

Be Persistent

iSECpartners part of nccgroup

- .ubirc
  - Presence of this file == debug mode
- We use it to run scripts
  - Patch SSH configuration for remote access
  - Drop the firewall

Let's go after the data

iSECpartners
part of nccgroup

- We're persistent
- Call me Eve
- Let's go find the packets!
  - QuickSec VPN client
    - Packaged as a Netfilter kernel module
    - Literally steals packets out of Netfilters and handles them itself…
    - Packets don't show up in normal capture tools like tcpdump
    - Not Open Source

It's Just Engineering

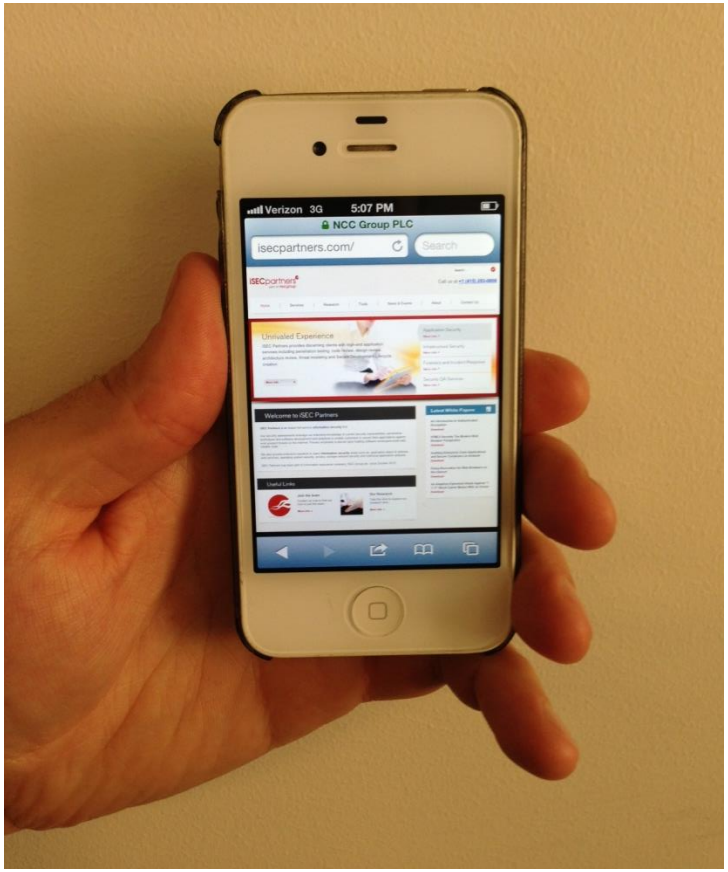
I want packets!

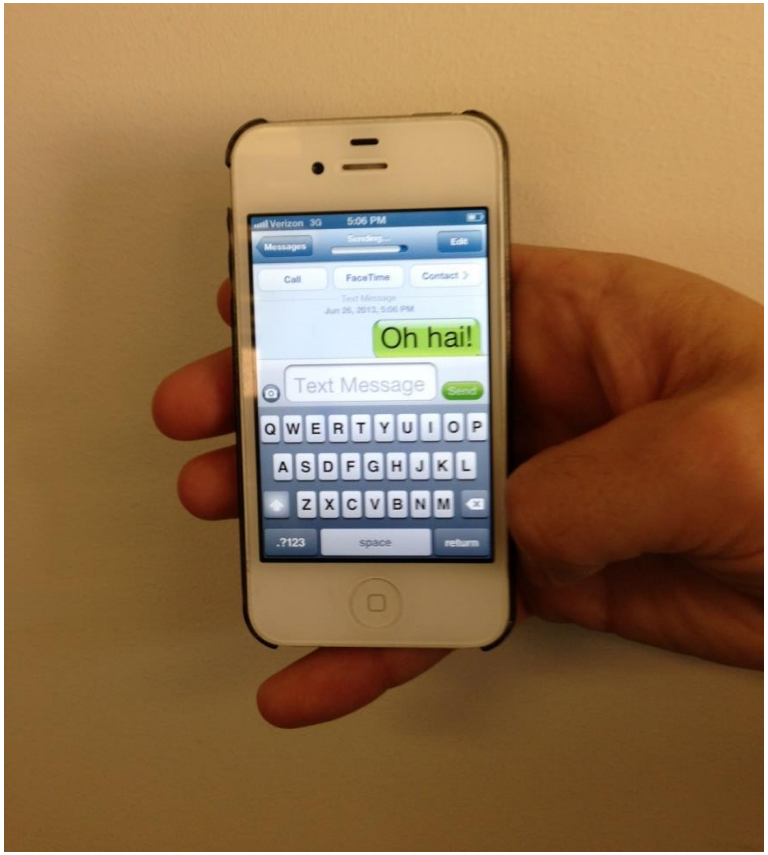
iSECpartners
part of nccgroup

- Custom kernel module
  - Priority is tricky
  - Incoming/Outgoing
    - Must be above & below quicksec to get the plaintext before encryption and after decryption
- Custom Userland app
  - Display data in real-time
  - Log to pcap
- Cross-compiling is fun*
  - *fun like a hernia

iSECpartners
part of nccgroup

Voice, Texts, and Data





Voice: Lots 'o packets

iSECpartners part of nccgroup

- Its mostly UDP, lots and lots of UDP
- Strange Ports
  - This is hard.

Source	Destination	Protocol	Length	Info
10.208.110.101	10.190.140.253	UDP	62	Source port: awg-proxy Destination port: sua
10.190.140.253	10.208.110.101	UDP	153	Source port: sua Destination port: awg-proxy
10.208.110.101	10.190.140.253	UDP	72	Source port: awg-proxy Destination port: sua
10.190.140.253	10.208.110.101	UDP	65	Source port: sua Destination port: awg-proxy
10.208.110.101	10.190.140.253	UDP	98	Source port: awg-proxy Destination port: sua
10.190.140.253	10.208.110.101	UDP	73	Source port: sua Destination port: awg-proxy
10.208.110.101	10.190.140.253	CLASSIC-S	62	Message: Set Active Destination Request
10.190.140.253	10.208.110.101	UDP	55	Source port: sua Destination port: awg-proxy
10.208.110.101	10.190.140.253	UDP	62	Source port: awg-proxy Destination port: sua
10.190.140.253	10.208.110.101	UDP	153	Source port: sua Destination port: awg-proxy
10.208.110.101	10.190.140.253	UDP	72	Source port: awg-proxy Destination port: sua
10.190.140.253	10.208.110.101	UDP	65	Source port: sua Destination port: awg-proxy
10.208.110.101	10.190.140.253	UDP	100	Source port: awg-proxy Destination port: sua
10.190.140.253	10.208.110.101	UDP	73	Source port: sua Destination port: awg-proxy
10.208.110.101	10.190.140.253	CLASSIC-S	62	Message: Set Active Destination Request
10.190.140.253	10.208.110.101	UDP	55	Source port: sua Destination port: awg-proxy
10.190.140.253	10.208.110.108	UDP	50	Source port: 6115 Destination port: a1-bs
10.208.110.108	10.190.140.253	UDP	46	Source port: 65310 Destination port: 6115
192.168.2.4	66.174.71.40	ISAKMP	122	INFORMATIONAL
66.174.71.40	192.168.2.4	ISAKMP	122	INFORMATIONAL
10.190.140.253	10.208.110.105	UDP	50	Source port: a1-bs Destination port: a1-bs
10.190.140.253	10.208.110.101	UDP	48	Source port: sua Destination port: awg-proxy
10.208.110.101	10.190.140.253	UDP	48	Source port: awg-proxy Destination port: sua
10.208.110.105	10.190.140.253	UDP	46	Source port: 65294 Destination port: a1-bs
10.190.140.253	10.208.110.101	UDP	190	Source port: sua Destination port: awg-proxy
10.208.110.101	10.190.140.253	UDP	90	Source port: awg-proxy Destination port: sua
10.190.140.253	10.208.110.101	UDP	65	Source port: sua Destination port: awg-proxy
10.190.140.253	10.211.28.212	UDP	59	Source port: 64534 Destination port: 53518
10.190.140.253	10.211.28.212	UDP	59	Source port: 64534 Destination port: 53518
10.190.140.253	10.211.28.212	UDP	59	Source port: 64534 Destination port: 53518

Voice: Force Decode as RTP

iSECpartners part of nccgroup

both.pcap [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 10.191.12.248 and ip.addr eq 10.211.28.212) and (udp.port eq Expression... Clear Apply Save

No.	Source	Destination	Protocol	Length	Info
1069	10.191.12.248	10.211.28.212	RTP	56	PT=DynamicRTP-Type-97, SSRC=0xFC14, Seq=180,
1070	10.211.28.212	10.191.12.248	RTP	76	PT=DynamicRTP-Type-97, SSRC=0xABADFBF0, Seq=
1071	10.191.12.248	10.211.28.212	RTP	56	PT=DynamicRTP-Type-97, SSRC=0xFC14, Seq=181,

```
⊞ Frame 1070: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
⊞ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
⊞ Internet Protocol Version 4, Src: 10.211.28.212 (10.211.28.212), Dst: 10.191.12.248 (10.191.12.248)
⊞ User Datagram Protocol, Src Port: 38368 (38368), Dst Port: 64532 (64532)
⊟ Real-Time Transport Protocol
```

```
⊟ Real-Time Transport Protocol
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: DynamicRTP-Type-97 (97)
    Sequence number: 1
    Timestamp: 3166485852
    Synchronization Source identifier: 0xabadfbf0 (2880306160)
    Payload: 754059680002de68bc07dc42330e032f22c8cb42c5c0
```

Voice – Codec?

RFC 3558:

Value	Rate	Total data frame size
0	Blank	0 (0 bit)
1	1/8	2 (16 bits)
2	1/4	5 (40 bits; not valid for EVRC)
3	1/2	10 (80 bits)
4	1	22 (171 bits; 5 padded at end w/ zeros)
5	Erasure	0 (SHOULD NOT be transmitted by sender)

Voice – Codec?

iSECpartners
part of nccgroup

Decoding EVRC speech codec

2

I want to decode the EVRC speech codec. I have checked the ffmpeg library but it seems like, EVRC is not being currently supported by ffmpeg.

Is there any alternate library which can be used to decode EVRC data?

2

Or if anybody have some algorithm or decoding mechanism or code snippet to do so, please let me know.

Thanks Nitin

audio | ffmpeg | decoding | cdma

share | edit | close | flag | protect

asked Apr 30 '12 at 8:06
Nitin Goyal
95 • 1 • 9

No Answers!

Voice – Codec?

iSECpartners
part of nccgroup

1

+500

There are some files claimed to be EVRC code here (on chinese sites):
http://www.codeforge.com/article/67387

Same file on pudn.com:
http://en.pudn.com/downloads95/sourcecode/comm/voice_compress/detail389385_en.html

It can be not so easy to download full 0.5 MB archive (registration required), but it looks like working

This answer has been awarded bounty worth 500 reputation by Tom Ritter

There are so3 and so68 implementations in the archive
ftp://ftp.3gpp2.org/TSGC/Incoming/SWG11/Software_Published_in_TIA/evrc_rel-B_mps_software/Software_Distribution_vB-1.0_for_C.S0018-B_v1.0_EVRC_MPS.zip

so3 sources look similar to some files from evrc.rar:

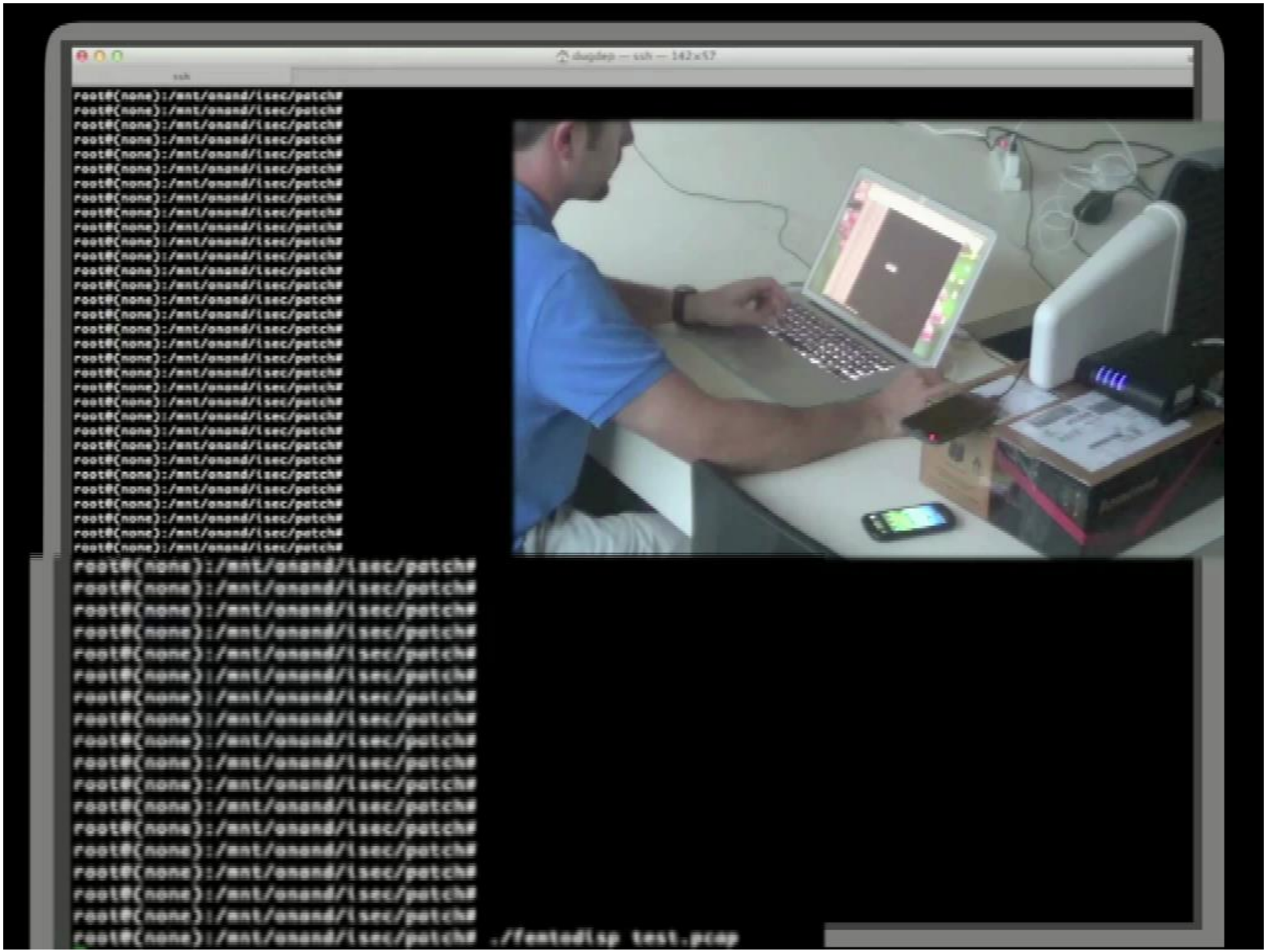
```
/*     Enhanced Variable Rate Codec - Master C code Specification       */
/*     Copyright (C) 1997-1998 Telecommunications Industry Association. */
```

and so68 (EVRCB_FX) is for EVRC-B (both encoder and decoder):

```
EVRC-B vocoder fixed point c-simulation can be compiled using the standard GNU
c++ compile tools like g++, make, etc.

/*  EVRC-B - Enhanced Variable Rate Coder - B Speech Service Option for  */
/*  Wideband Spread Spectrum Digital System                              */
/*  C Source Code Simulation                                             */
```

Voice!



SMS

- These specs suck
  - But we figured it out
- 7-bit Words, ugh

```
#######################
Looks like an outgoing SMS from:
MIN: 908433[redacted]
ESN: 80 BE[redacted]
packet number = 619
#######################


#######################
sent a text message to:
Phone: 401[redacted]
Message: Hello
SMS ID: 1
packet number = 624
#######################
```

SMS

smscap2.pcap [Wireshark 1.8.3 (SVN Rev 45260 from /releases/wireshark-1.8.3)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: udp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Info
553	74.76	10.189.17.43	10.208.110.101	cdma_sms	
554	74.86	10.208.110.101	10.189.17.43	cdma_sms	CDMA SMS From: [redacted] SMS: Test Cap Message 3

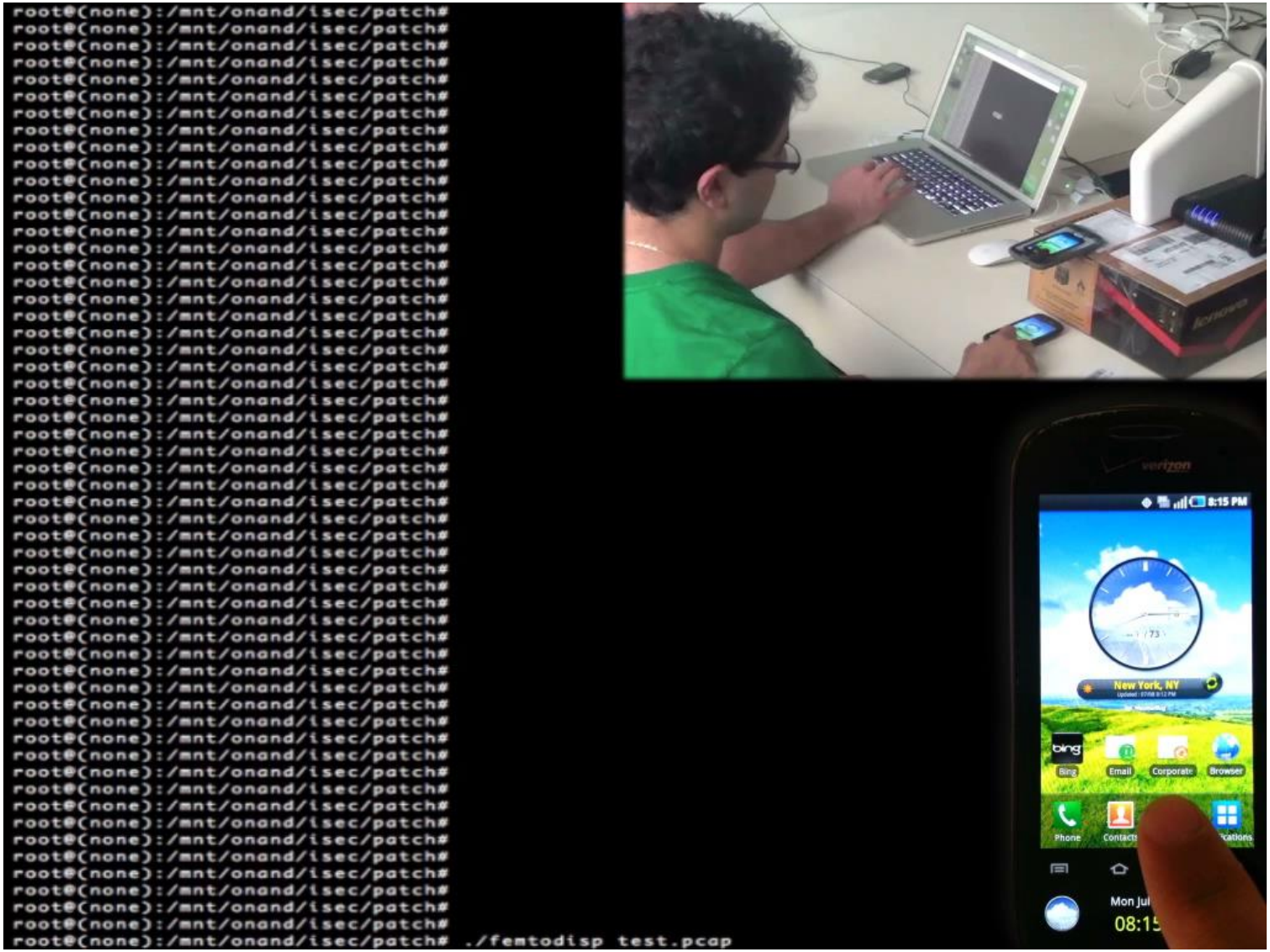
```
0001 0... .... .... = Encoding: 2
.... .000 1001 0... = Number of Characters: 18
.... .... .... .101 = Initial Character: 5
User Data: Test Cap Message 3
```

```
User Data Tag: 1
User Data Length: 18
0001 0... .... .... = Encoding: 2
.... .000 1001 0... = Number of Characters: 18
.... .... .... .101 = Initial Character: 5
User Data: Test Cap Message 3
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 62 00 00 40 00 3a 11  ab 6e 0a d0 6e 65 0a bd   .b..@.:. .n..ne..
0020  11 2b 0c cd 36 b1 00 4e  98 74 00 06 00 00 00 05   .+..6..N .t......
0030  20 0e 12 01 01 00 39 03  00 53 35 03 00 00 02 10    .....9. .S5.....
0040  02 02 07 02 a6 a2 0e 1e  a8 80 06 01 04 08 21 00   ........ ......!.
0050  03 [redacted] 4c bc fa 20 87 87 82 09   ..q .... L.. ....
0060  b9 79 f3 c3 9f 2a 06 60  03 06 12 11 07 13 14 35   .y...*.` .....5
```

User Data (cdma_sms.user_data), ... P... Profile: Default

SMS

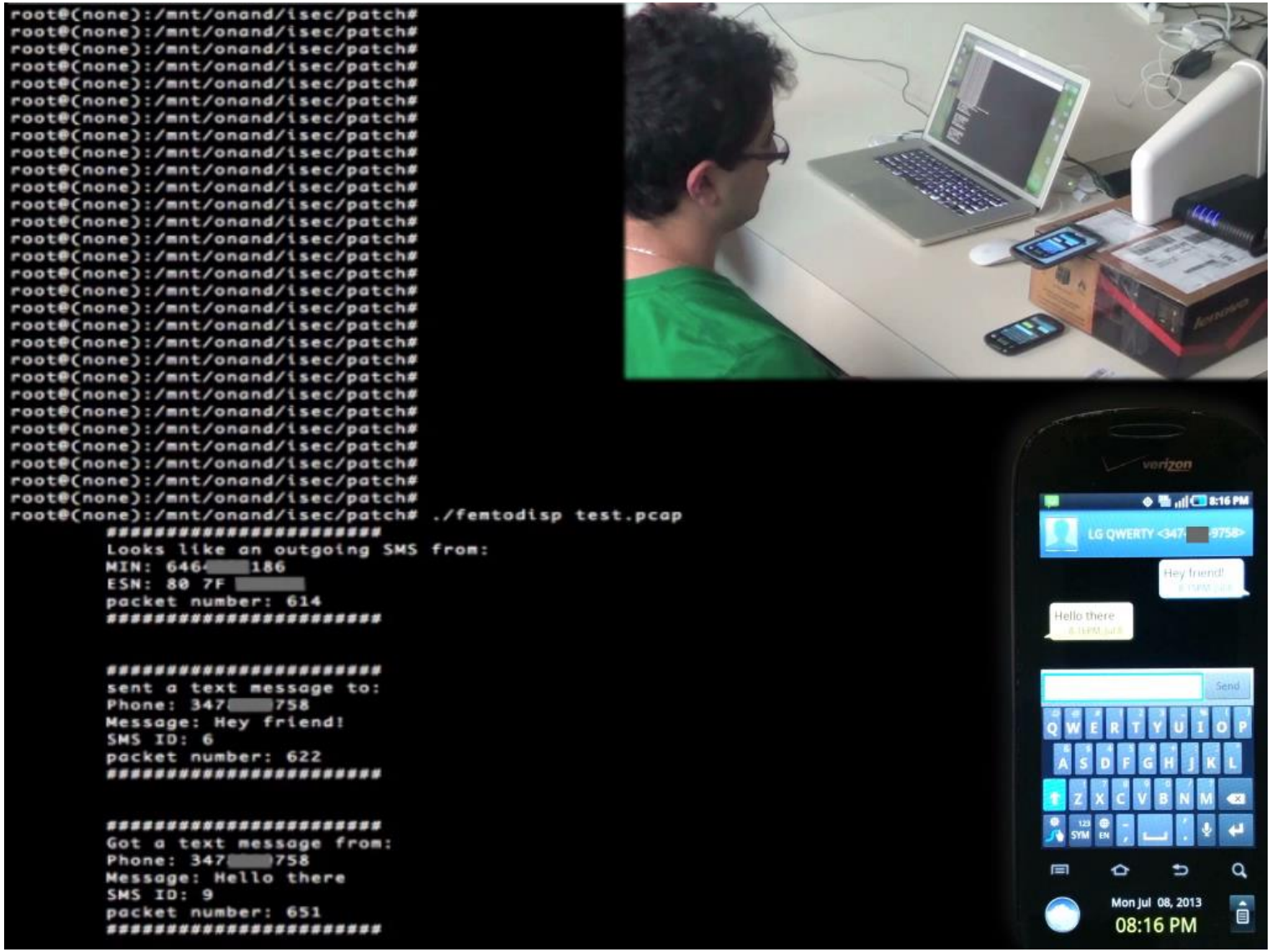

root@(none):/mnt/onand/isec/patch#
./femtodisp test.pcap
verizon
8:15 PM
New York, NY
bing
Bing
Email
Corporate
Browser
Phone
Contacts
Mon Jul
08:15

Data

iSECpartners
part of nccgroup

- Plaintext! Praise the Lord: beautiful, decoded, plaintext
- Easiest thing to do with data: View It.

MMS


root@(none):/mnt/onand/isec/patch# ./femtodisp test.pcap
Looks like an outgoing SMS from:
MIN: 646 186
ESN: 80 7F
packet number: 614
sent a text message to:
Phone: 347 758
Message: Hey friend!
SMS ID: 6
packet number: 622
Got a text message from:
Phone: 347 758
Message: Hello there
SMS ID: 9
packet number: 651
verizon
8:16 PM
LG QWERTY
Hey friend!
Hello there
Send
Mon Jul 08, 2013
08:16 PM

Data

iSECpartners
part of nccgroup

- Plaintext! Praise the Lord: beautiful, decoded, plaintext
- Easiest thing to do with data: View It.
- Second easiest thing to do with data: Drop It.

iMessage

- And when you Denial of Service some data services, they fail over insecurely…

Data

iSECpartners part of nccgroup

- Back to the Data. It is plaintext.

- However: Lots of encapsulation
  - If we're lucky: IP, GRE, PPP, HDLC, IP…
  - If we're not: IP, GRE, PPP, HDLC & then IP segmented across GRE packets

Data Traffic

iSECpartners
part of nccgroup

10isecpartners.pcap [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Expression... Clear Apply Save

No.	Source	Destination	Protocol	Info
121	https > 52227 [SYN, ACK] Seq=0 Ack=0 Win=14180 L			
107	55308 > http [ACK] Seq=0 Ack=1 Win=6940 Len=0			
139	33046 > http [ACK] Seq=0 Ack=1 Win=6940 Len=0			
139	PPP Fragment			
139	PPP Fragment			
139	PPP Fragment			
139	PPP Fragment			
171	PPP Fragment			
170	10.191.12.248	10.208.110.109	PPP	171 PPP Fragment

- Frame 166: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits)
- Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 10.191.12.248 (10.191.12.248), Dst: 10.208.110.109 (10.208.110.109)
- Generic Routing Encapsulation (CDMA2000 A10 Unstructured byte stream)
- PPP In HDLC-Like Framing
- Data (89 bytes)

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 7d 00 00 40 00 40 2f  a9 5e 0a bf 0c f8 0a d0   .}..@.@/ .^......
0020  6e 6d 30 80 88 81 e5 25  d8 c3 00 00 00 1d 00 01   nm0....% ........
0030  00 50 50 18 1b 1c 7a 68  00 00 47 45 54 20 2f 20   .PP...zh ..GET /
0040  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ..Host:
0050  77 77 77 2e 69 73 65 63  70 61 72 74 6e 65 72 73   www.isec partners
0060  2e 63 6f 6d 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .com..Co nnection
0070  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 55 73   : keep-a live..Us
0080  65 72 2d 41 67 65 6e 74  3a 20 4d                   er-Agent : M
```

Frame (139 bytes) | PPP Fragment (89 bytes)

File: "C:\Users\tom\Documents\work\femto... | ... | Profile: Default

- Frame 166: 139 bytes on wire (
- Ethernet II, Src: 00:00:00_00:
- Internet Protocol Version 4, S
- Generic Routing Encapsulation
- PPP In HDLC-Like Framing
- Data (89 bytes)

```
........ ......E.
.}..@.@/ .^......
nm0....% ........
.PP...zh ..GET /
HTTP/1.1 ..Host:
www.isec partners
.com..Co nnection
: keep-a live..Us
er-Agent : M
```

Data Middling

iSECpartners
part of nccgroup

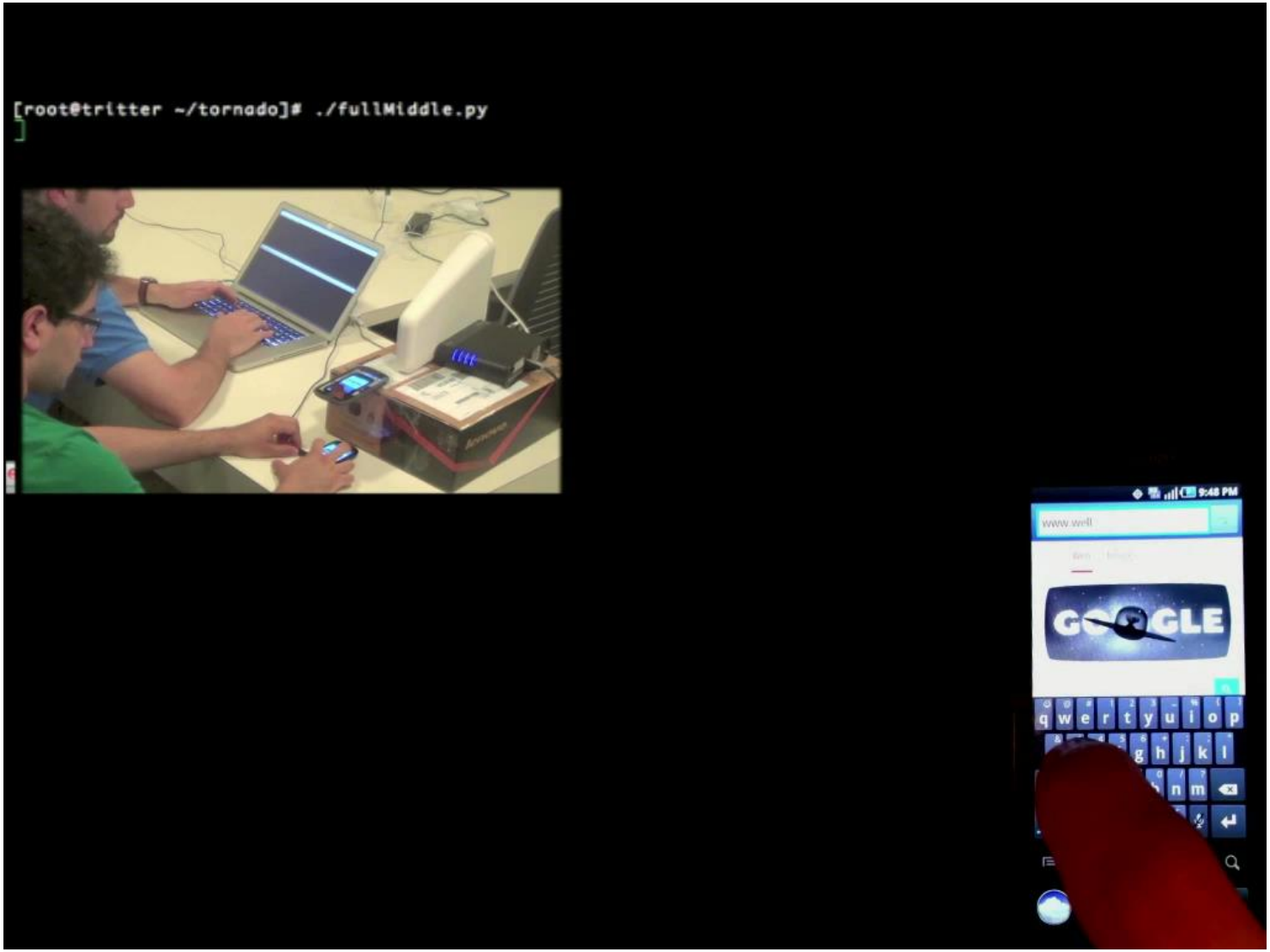
- Goal: Edit a Webpage, as simply as possible
  - (Change HTTPS Form Action - > HTTP)
- Going to require editing the inner TCP checksum
  - Which requires decoding and re-encoding
  - And editing the PPP checksum
  - And hopefully doesn't change the size

Data Middling

iSECpartners
part of nccgroup

- And then we found out… the carrier applies transparent compression to all traffic on port 80
- Everything you send to them is proxied
  - These setups are often used in transparent logging, censorship, and MITM attacks
  - We have no evidence of these activities
  - This is not the only carrier doing this
  - But it is something we had to work around

Data Middling Video



Miniature Cell Towers

- Eavesdropping is cool and everything but…
- Impersonation is even cooler.

Cloning

CDMA Terminology

iSECpartners part of nccgroup

- No SIM Cards needed here

	GSM	CDMA
Device ID	IMEI	ESN (Now MEID)
Subscriber ID	IMSI	MIN
User Phone #	MSISDN	MDN

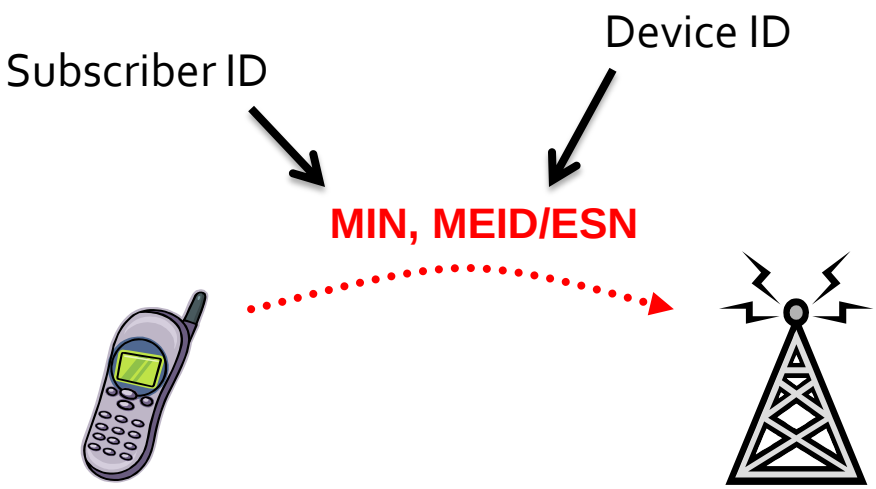
- Unlike the IMSI, the MIN is just a 10 digit phone number, sometimes the same as your actual phone number

CDMA Terminology

- ESN (Electronic Serial Number)
  - CDMA-specific ID number: "11 EE 4B 55"
- MEID (Mobile Equipment Identifier)
  - ESNs ran out! MEID is successor
  - Pseudo ESN used for backwards compatibility with handsets using MEIDs: "80 11 EE 4B"

Cloning basics – Real Towers

- Every time you make a call, MIN and MEID or ESN sent unencrypted to the tower to identify you
- That used to be it, and cloning was rampant



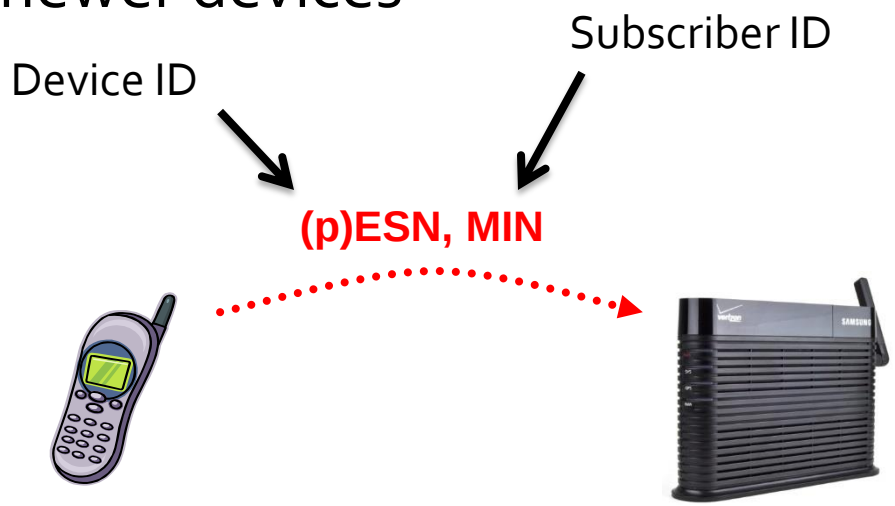
Enter the CAVE

iSECpartners
part of nccgroup

- CAVE (Cellular Authentication and Voice Encryption)
- Every phone has a secret *A-Key*, which generates two derivative keys used to authenticate every call and message, as well as encrypt voice traffic over the air
- The *A-Key* is never shared over the network, but the derivative keys are used for every call

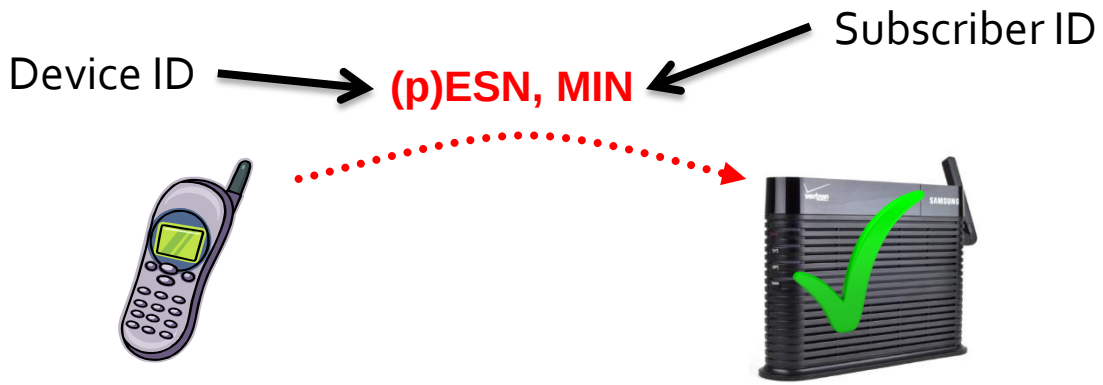
Connecting to a Femtocell

- The femtocell acts just like any other tower, except it doesn't actually require the MEID
- ESN is used with older devices, and pESN is used instead of MEID on newer devices



Remember Your Failure At The CAVE…

- The femtocell does not use MEIDs for authentication at all, only the (p)ESN and MIN
- And most importantly, the femtocell ***didn't require CAVE!***
- This means that a "classic" clone with just the (p)ESN and MIN would work - as long as the attacker's clone is connected to a femtocell
- We just need the (p)ESN and MIN of our victim



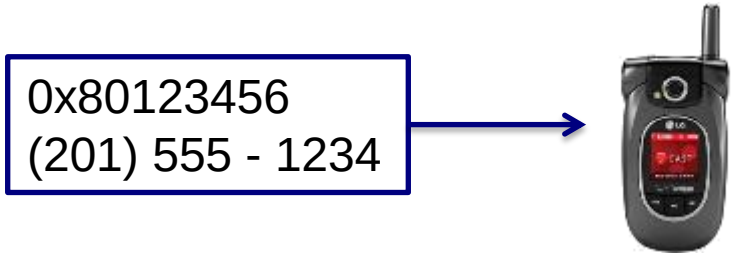
The Perfect Clone

- (p)ESN/MIN values are passed through the femtocell in a registration packet whenever ANY phone comes within range
- This allows cloning ***without physical access to phone***

```
#########################
MIN is: 908   1208
ESN is: 80 BE
packet number = 18
#########################
```

The Perfect Clone

Step 1: Victim phone falls in range of rooted femtocell with sniffer



Step 2: MIN and ESN are collected and cloned to a target device

Step 3: Target device is associated with a stock femtocell

Step 4: Clone attained; calls and SMS can be made on behalf of original phone

Simplest Cloning Scenario

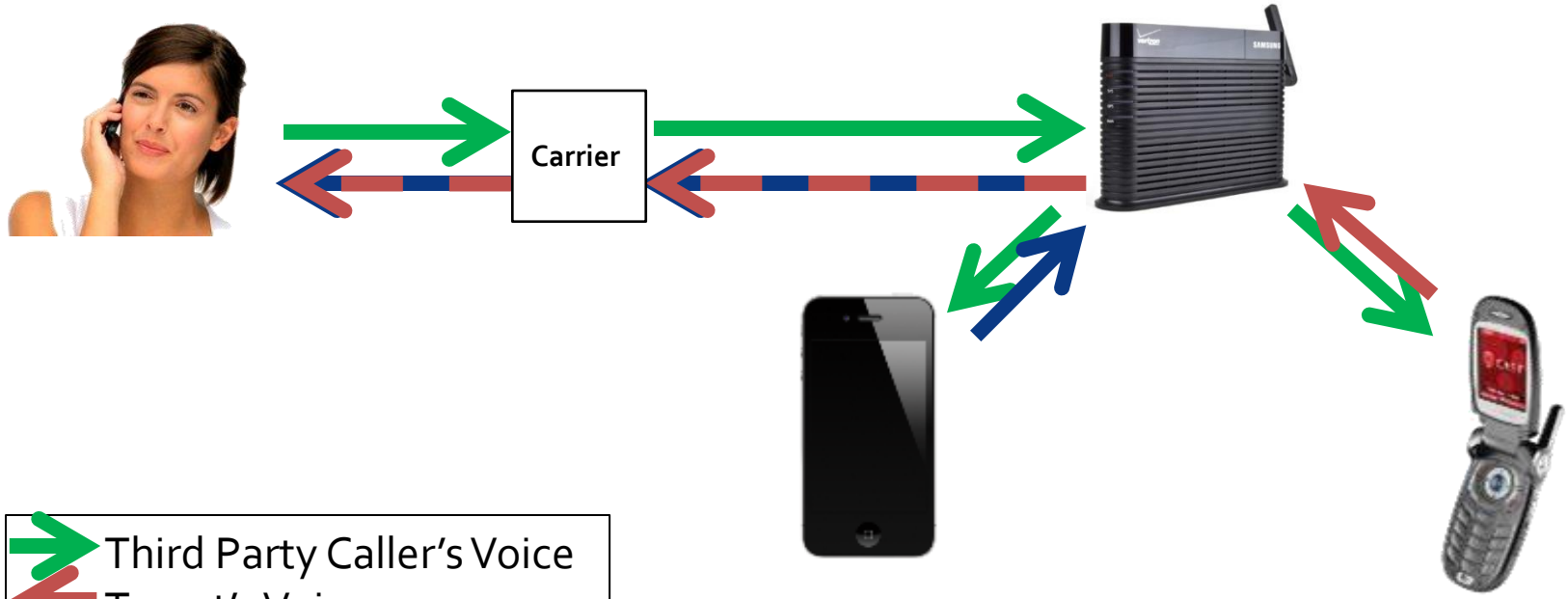
iSECpartners
part of nccgroup

When the VICTIM phone is turned off or jammed

- Everything works
  - Incoming Call
  - Outgoing Call
  - SMS

More Complicated Scenarios

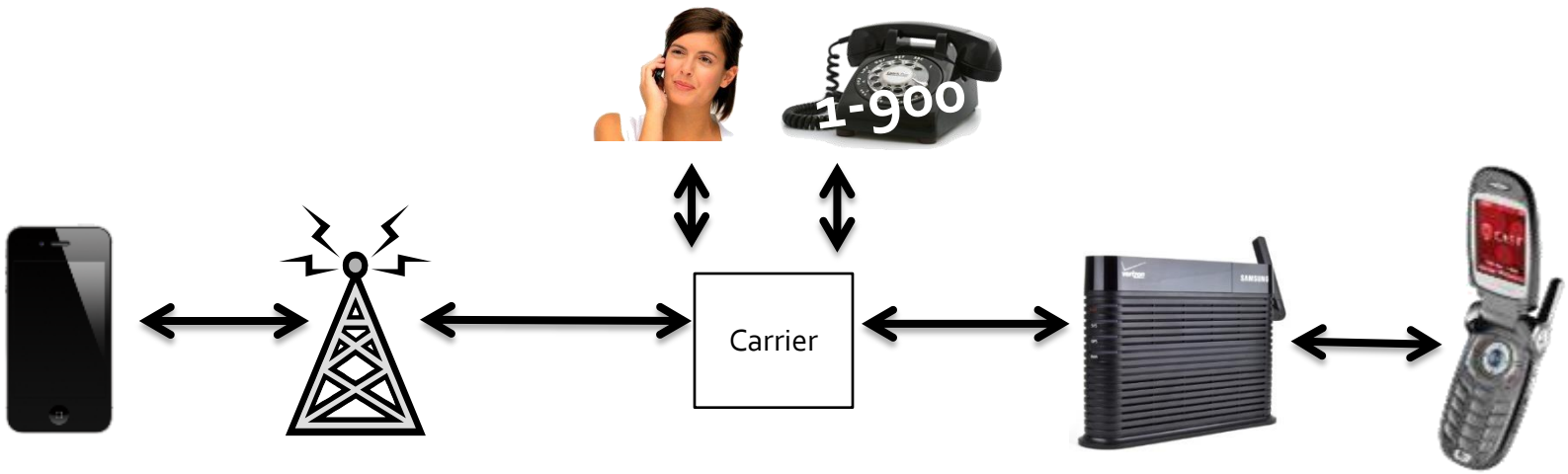
Two-and-a-half-way call



Third Party Caller's Voice
Target's Voice
Victim's Voice

More Complicated Scenarios

Two calls at once, no impact to the victim



Cloning Data

- Much more difficult
- Need more keys
  - Valid NAI
  - HA
  - AAA

Cloning Video

iSECpartners
part of nccgroup

Cloning: Patched

iSECpartners
part of nccgroup

The requirement for CAVE Authentication to be enabled takes place on the Carrier Network (not the femtocell).

Accordingly, it was patched without requiring any software updates to the femtocell.

Femtocells are a Bad Idea

Major US Carrier Comparison

iSECpartners
part of nccgroup

Carrier	Technology	Femtocell?
Verizon	CDMA	Yes
Sprint	CDMA	Yes
AT&T	GSM	Yes
T-Mobile	GSM	No

Short Term Mitigations

- Harden the femtocell hardware and software

- That might help except…

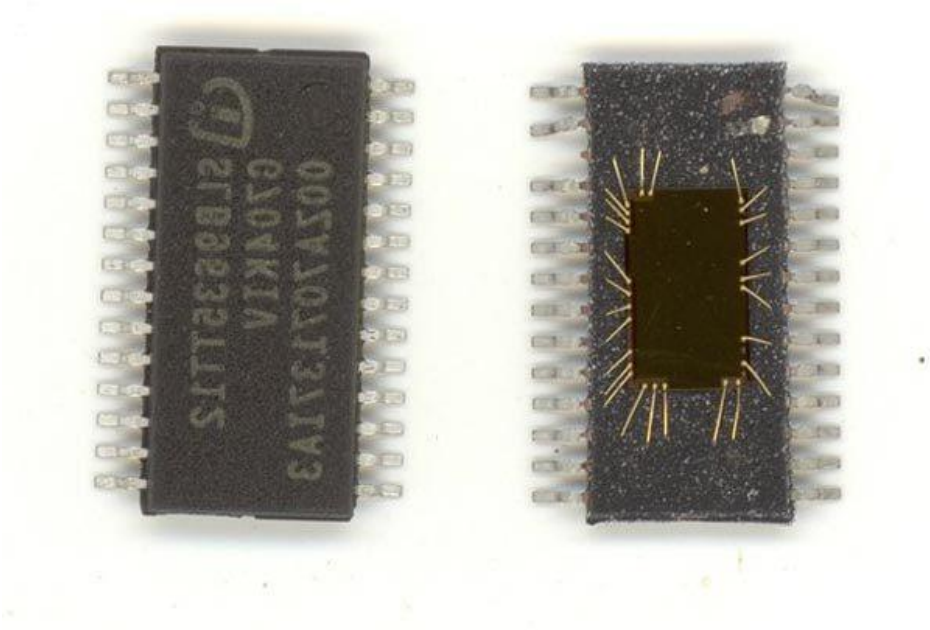
Root is always possible

iSECpartners
part of nccgroup

"If an attacker has physical control over your computer…
it's not your computer anymore."

Root is always possible

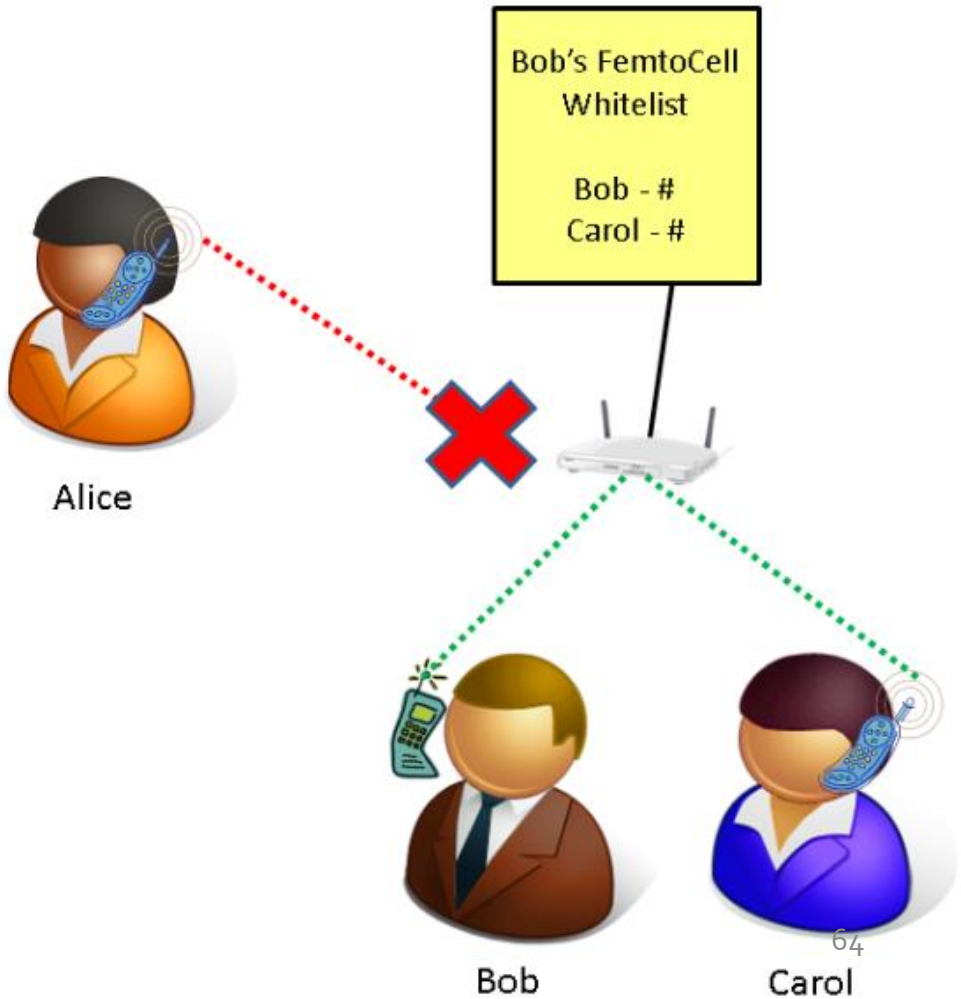
- We got in through a serial port
- JTAG / UART ports?
- Reflash firmware?
- Glitching Attacks?



Short Term Mitigations

Require phone registration

- Capability currently exists



Femtocell Handset Registration

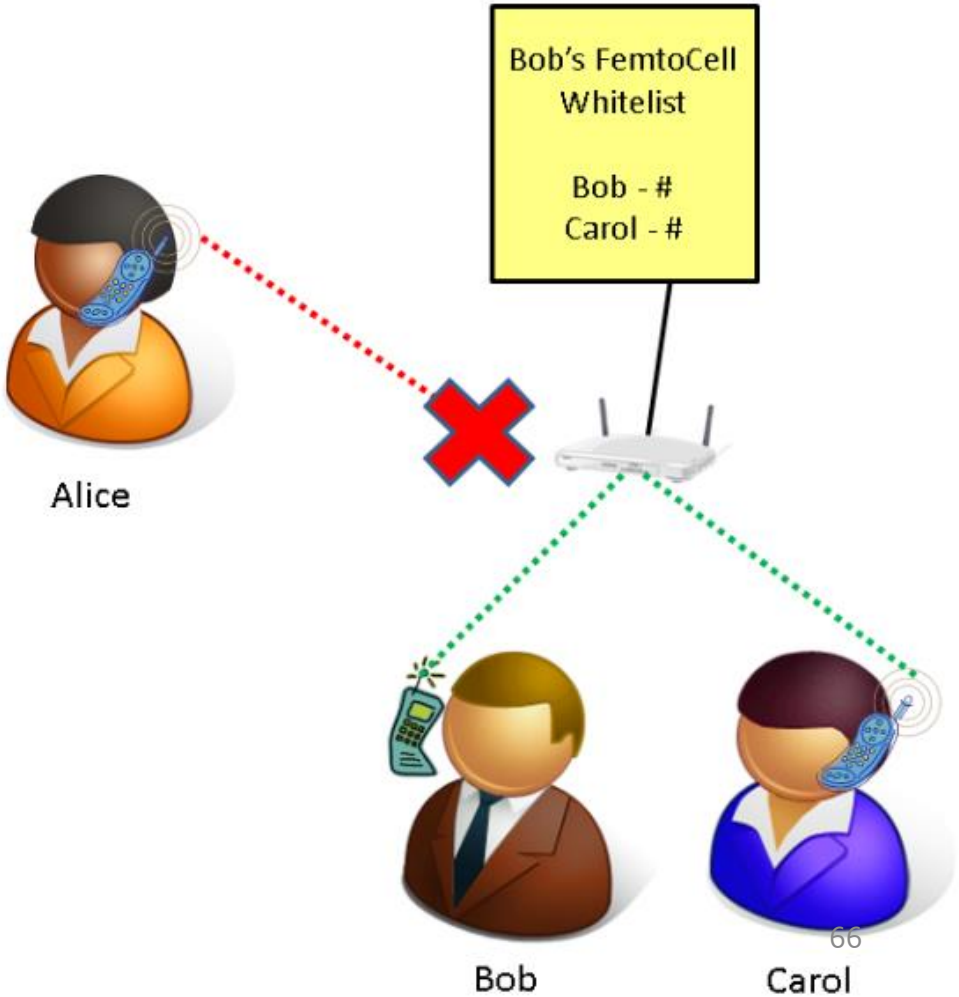
iSECpartners part of nccgroup

Vendor	Tech	Femtocell	Requires Registration
Verizon	CDMA	Yes	**No** Optional per Femtocell
Sprint	CDMA	Yes	**No** Optional per Femtocell
AT&T	GSM	Yes	**Yes!**
T-Mobile	GSM	**No!** Wi-Fi Calling	N/A

Short Term Mitigations

Require phone registration

- Capability currently exists
- Protects against untargeted dragnets
- Does not protect against isolation attacks

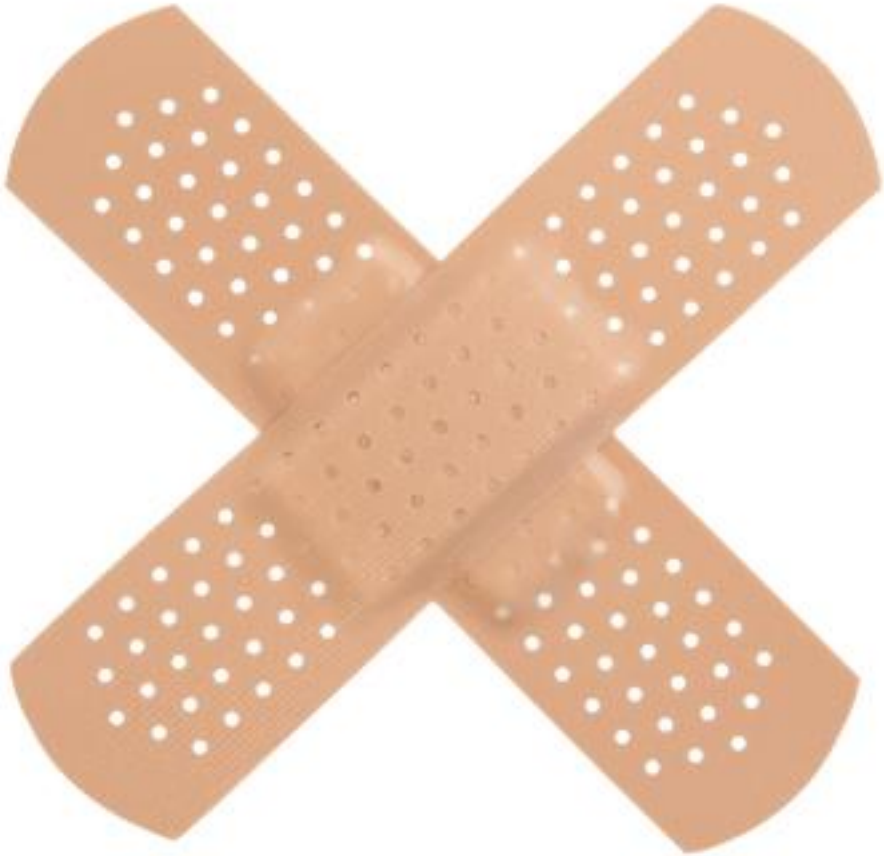


Long Term Mitigations

iSECpartners
part of nccgroup

- Get rid of 'em
- WiFi Calling
  - IPSec or SSL Tunnel
- End-to-End encryption
  - OSTel & CSipSimple/Groundwire
  - RedPhone
  - ZRTP

Fixes & Bandaids



Mitigation Summary

iSECpartners
part of nccgroup

- Short Term
  - ~~Harden femtocell~~
  - Require registration
- Long Term
  - No femtocells
  - Move to WiFi Calling
  - End-to-end Encryption

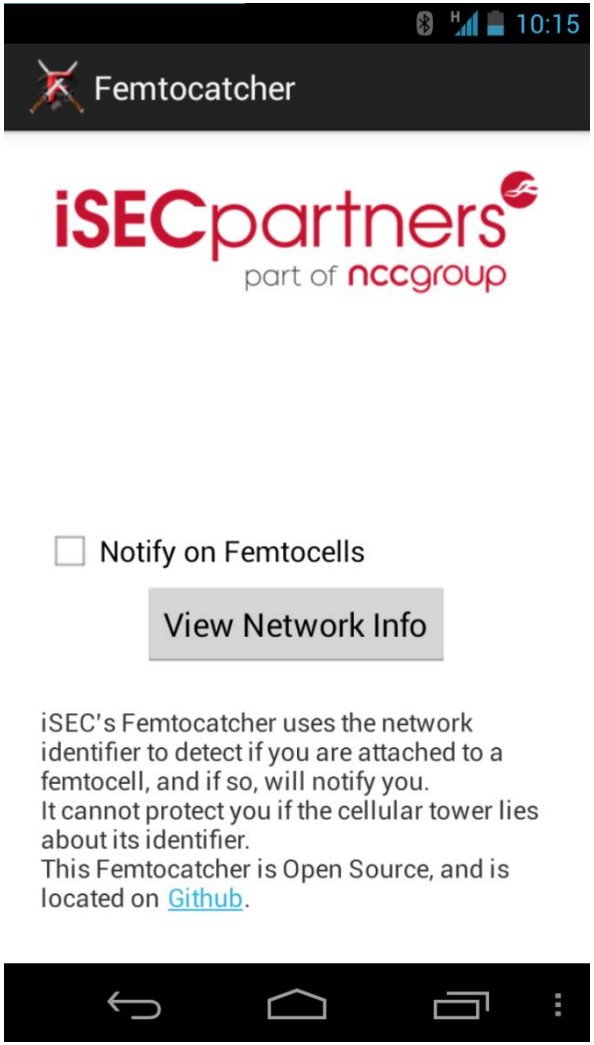
What Can I Do?

iSECpartners
part of nccgroup

- How do I know if I'm connected to a femtocell?
- Android - some phones display an icon when connected to a femtocell
  - Phones that Verizon modified
  - Not Stock Android, Not Third Party ROMs
- iPhone – No visual indicator
- All - Short beep at beginning of phone call (easy to miss)
- But somewhere, there's code written to detect them

Announcing FemtoCatcher

- Detects femtocells and puts you in airplane mode
- http://github.com/isecpartners/femtocatcher
- Thanks immensely to Mira Thambireddy



Coping

As a Business Owner

iSECpartners
part of nccgroup

- Cellular sniffing is possible
  - Physical Security
  - Security Procedures
- High-Value Processes should be reviewed
  - Two factor auth
  - Caller ID

When You Rely on Cellular

iSECpartners
part of nccgroup

- The network is untrusted
  - People will sniff your protocol
  - People will perform active attacks on your service
- You cannot rely on obscurity

As a Telecom

iSECpartners
part of nccgroup

- Your network does not extend to femtocells
  - They cannot be treated as a trusted computing device
  - They will attack you

Thank You & Questions?

iSECpartners
part of nccgroup

- Tom Ritter
  - Principal Security Engineer at iSEC Partners
  - tritter@isecpartners.com

- Thanks to
  - Doug DePerry
    - Senior Security Engineer at iSEC Partners
    - doug@isecpartners.com
  - Andrew Rahimi
  - RSAXVC & Doug Kelly
  - Davis Gallinghouse, Tim Newsham
  - Mira, Michael, Pratik, Peter Oehlert, Joel Wallenstrom, and really all of iSEC