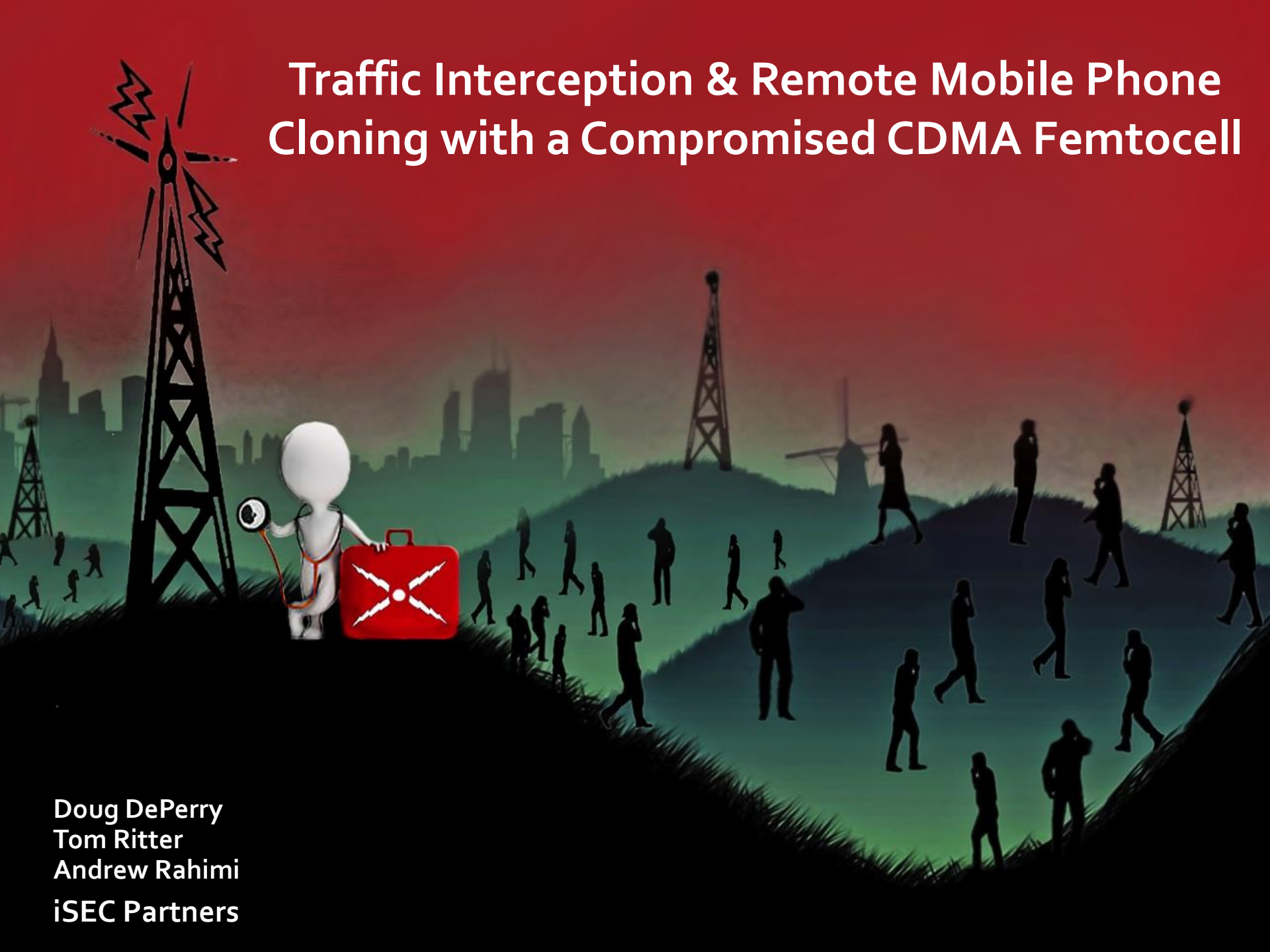
Traffic Interception & Remote Mobile Phone Cloning with a Compromised CDMA Femtocell



Doug DePerry
Tom Ritter
Andrew Rahimi

iSEC Partners

- The specific method used to access the device that makes the demonstration possible has been resolved by Verizon Wireless through a security patch.
- The Network Extenders being used to conduct the demonstration do not have the security patch installed.
- Verizon Wireless gave iSEC permission to use the network extenders to conduct the demonstration in consideration of iSEC bringing the issue to the attention of Verizon Wireless.

No User Interaction

iSECpartners part of nccgroup

- This is ***not*** like joining an open WiFi network
- Your phone associates ***automatically*** with no* indication
  - You might be on ours right now. ☺
- We don't hack phones… at least not today

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
  - Concerns shared by…

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

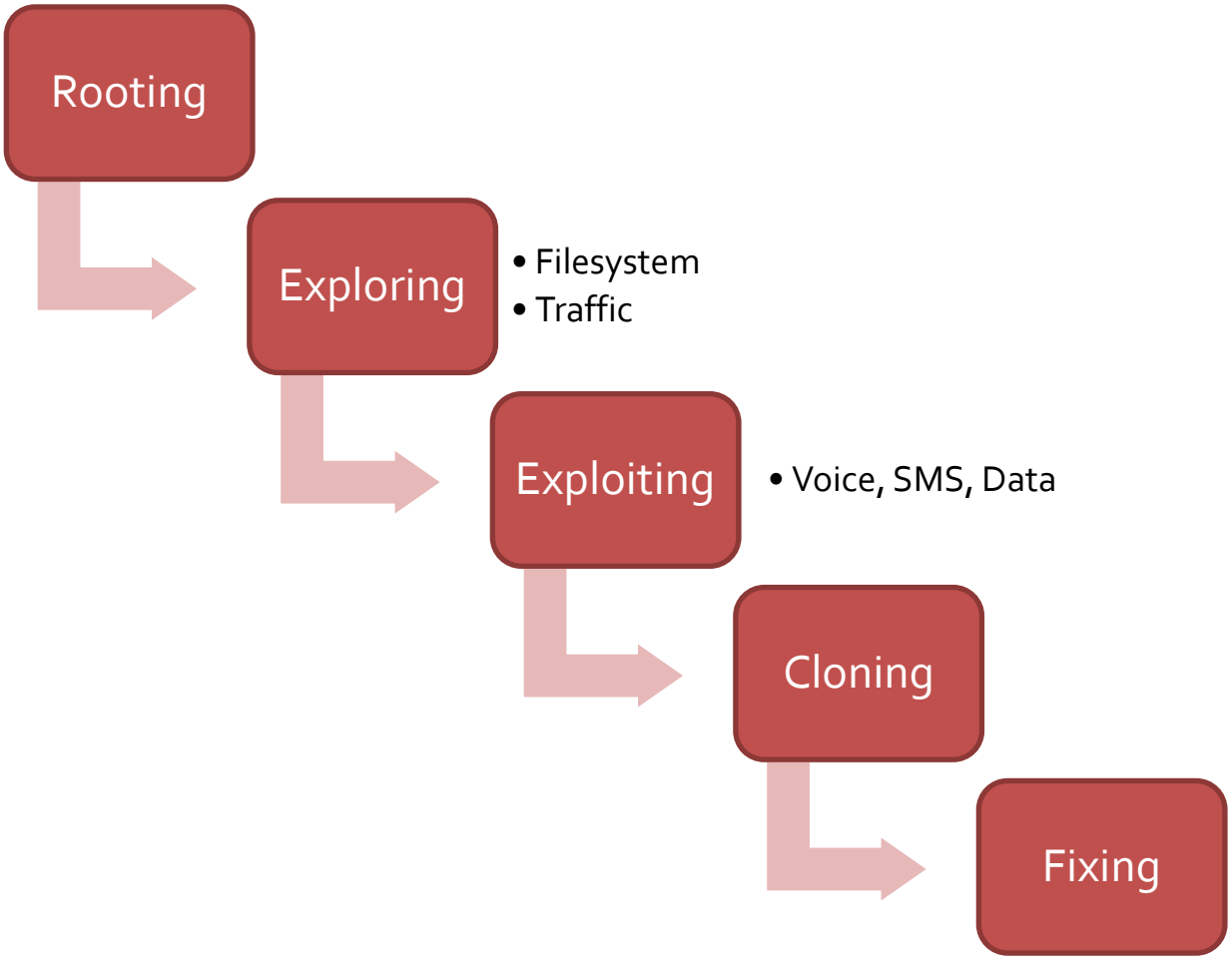
Our Focus

iSECpartners part of nccgroup

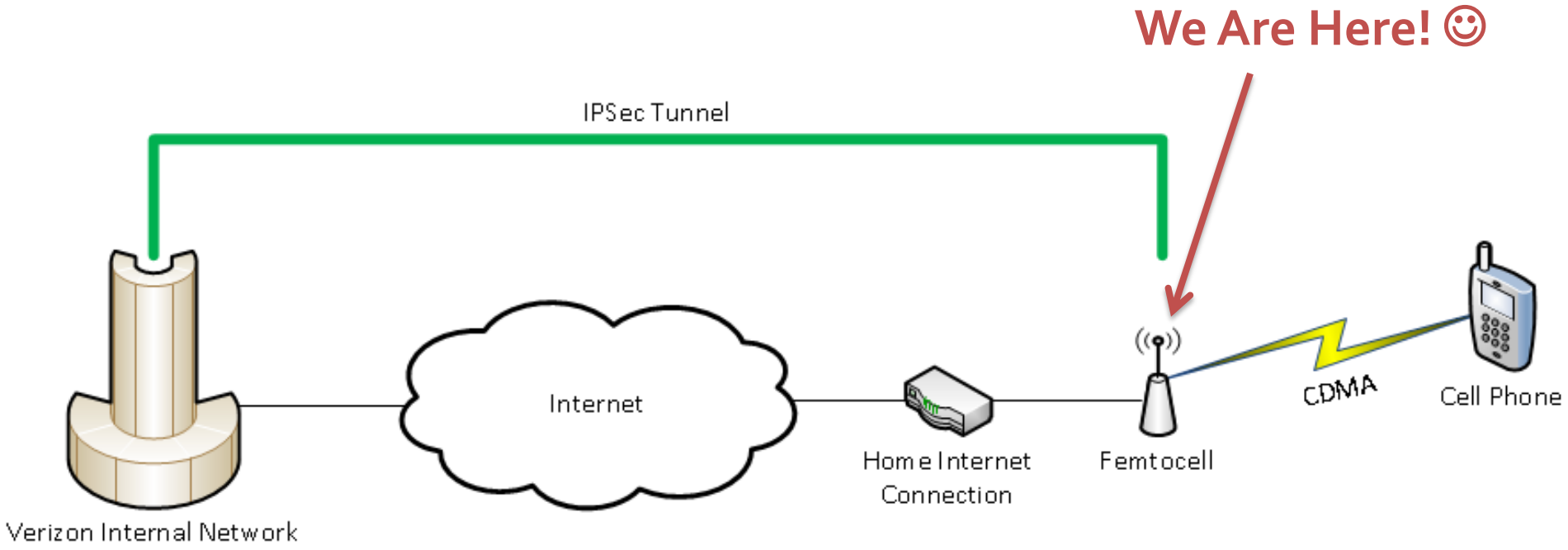
- North American Carrier
  - 3G
  - CDMA
- Customers affected
  - Roughly 1/3 of the population of the US
- Phone Calls & SMS
- MMS, Data Man-In-The-Middling, SSL Stripping
- Cloning

Agenda

iSECpartners part of nccgroup



General Architecture



Rooting the Femtocell(s)

SCS-26UC4
(Older)

SCS-2U01
(Newer)

Rooting the Femtocell(s)

SCS-26UC4
(Older)

Bonus!

SCS-2U01
(Newer)

SCS-2U01 Hardware

iSECpartners part of nccgroup

- 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

iSECpartners part of nccgroup

- HDMI port

Custom Cable

iSECpartners part of nccgroup

- USB FTDI + HDMI =

Wireless Signal Range

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

Console Access!

iSECpartners part of nccgroup

- SCS-26UC4
  - 57600 8 N 1
  - Uboot delay: “Press any key to interrupt boot”
  - Root shell
  - Run /etc/init.d/rc 5
  - Root on fully functional device
- SCS-2U01
  - 115200 8 N 1
  - Magic sysreq + i
  - Root login
  - Run /etc/init.d/rc 5
  - Root on fully functional device

Console Access: Patched

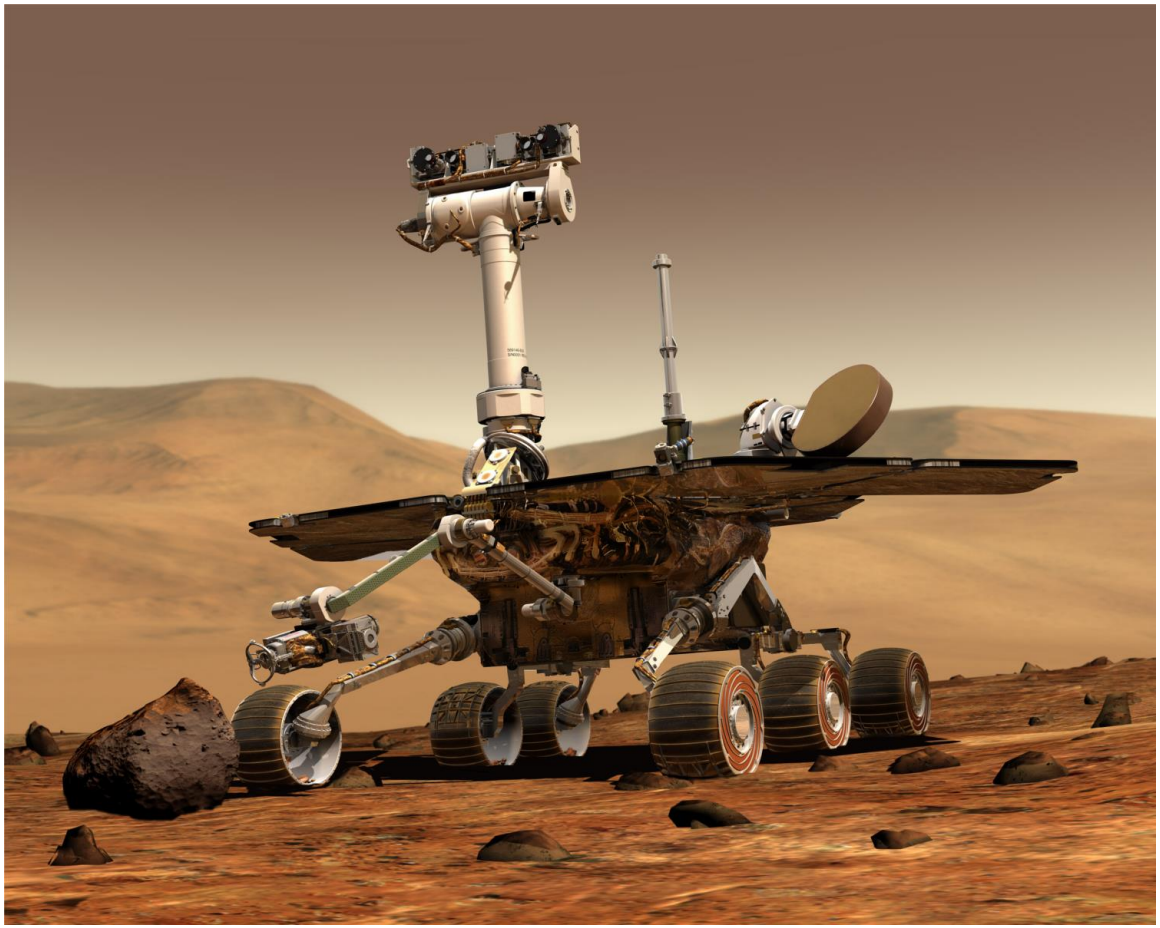
iSECpartners part of nccgroup

These mechanisms to obtain root no longer work

(But may be useful on other embedded devices)

iSECpartners
part of nccgroup

Exploring the Femtocell



Filesystem

iSECpartners part of nccgroup

- MontaVista Linux 5, 2.6.18
  - 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

- This terminal console sucks
  - Can't really do anything
- Let's patch
  - No easy way to edit files
    - ugh, sed
  - SSHD
    - PKI-only, no RootLogin
    - Edit SSHD.conf
  - Flush iptables

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 sshd
      - Allow interactive root login
    - Flush iptables
    - exec /bin/bash

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

iSECpartners
part of nccgroup

It's Just Engineering

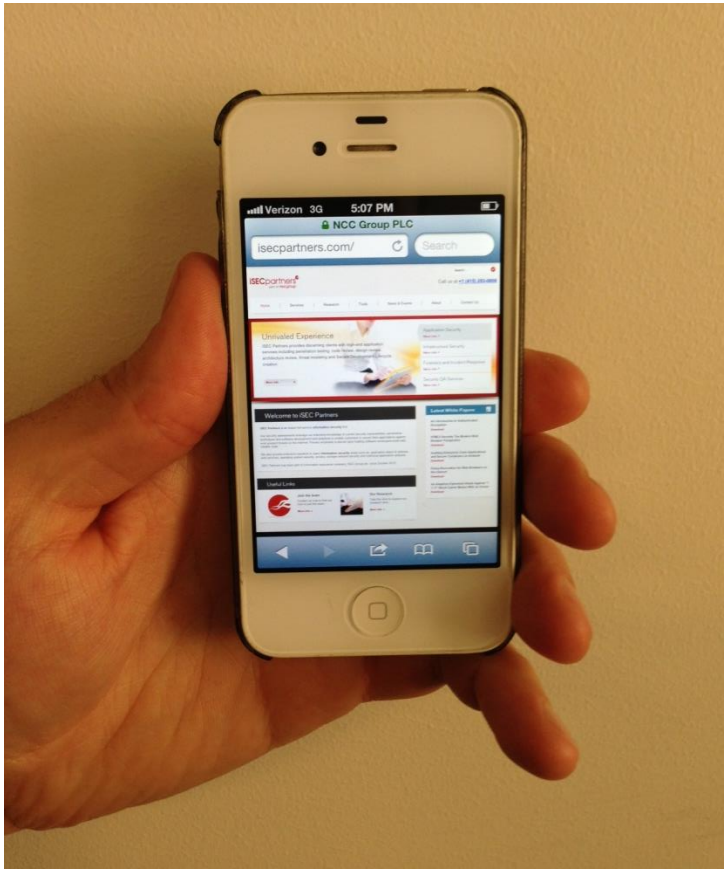
I want packets!

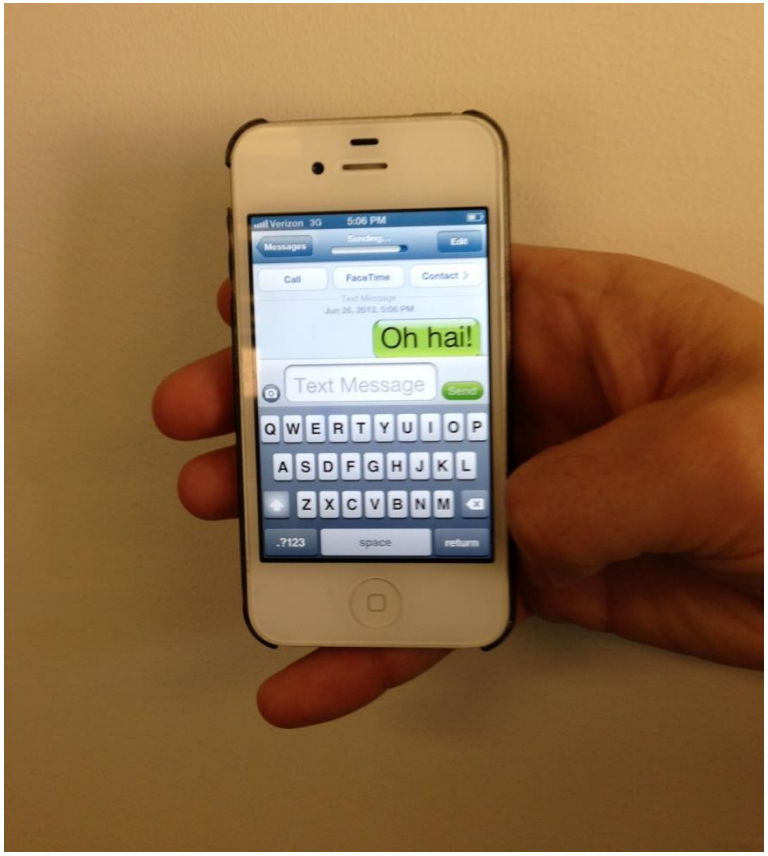
iSECpartners part of nccgroup

- 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





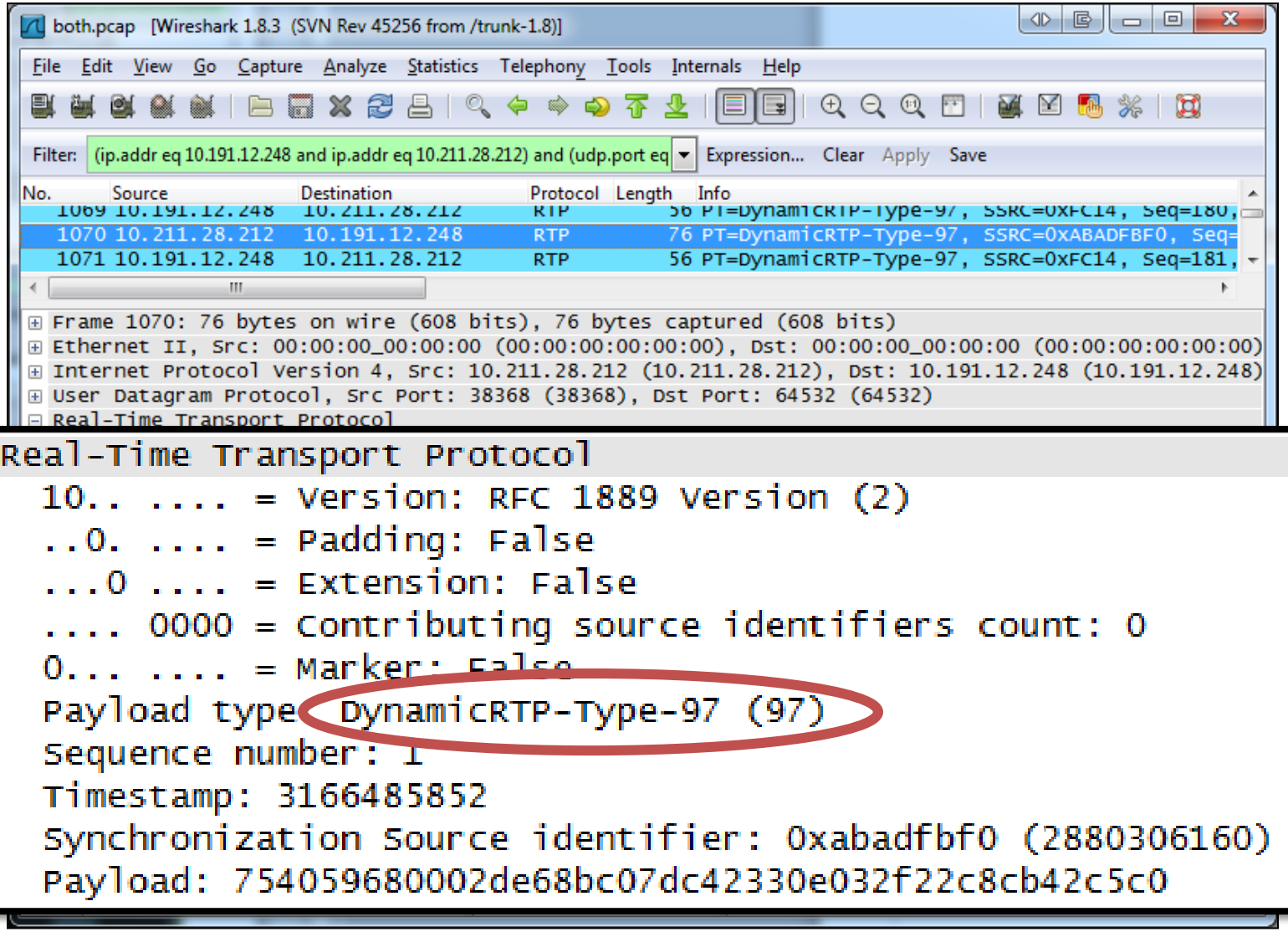
Voice: Lots 'o packets

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



Voice – Codec?

iSECpartners part of nccgroup

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

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

+500

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                                             */
```

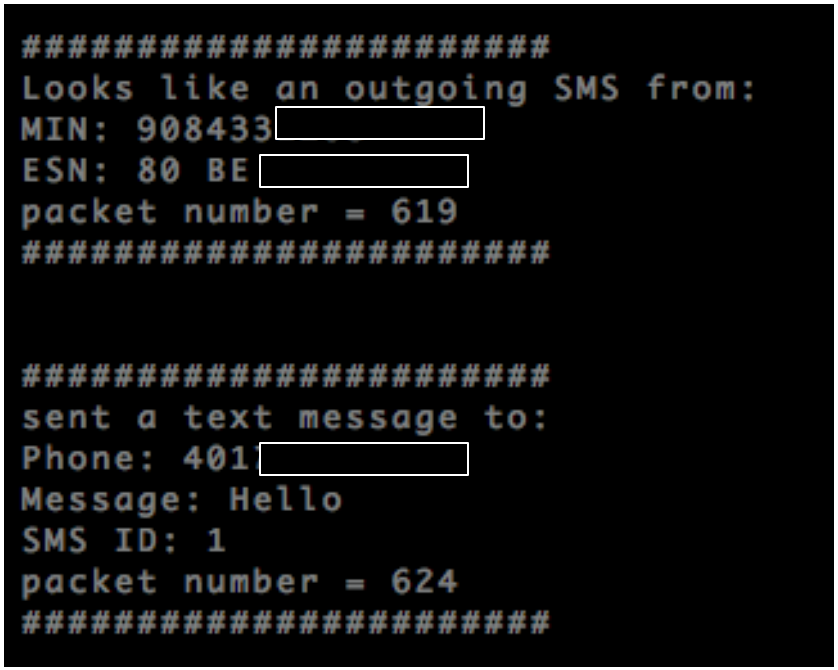
Voice!

iSECpartners part of nccgroup

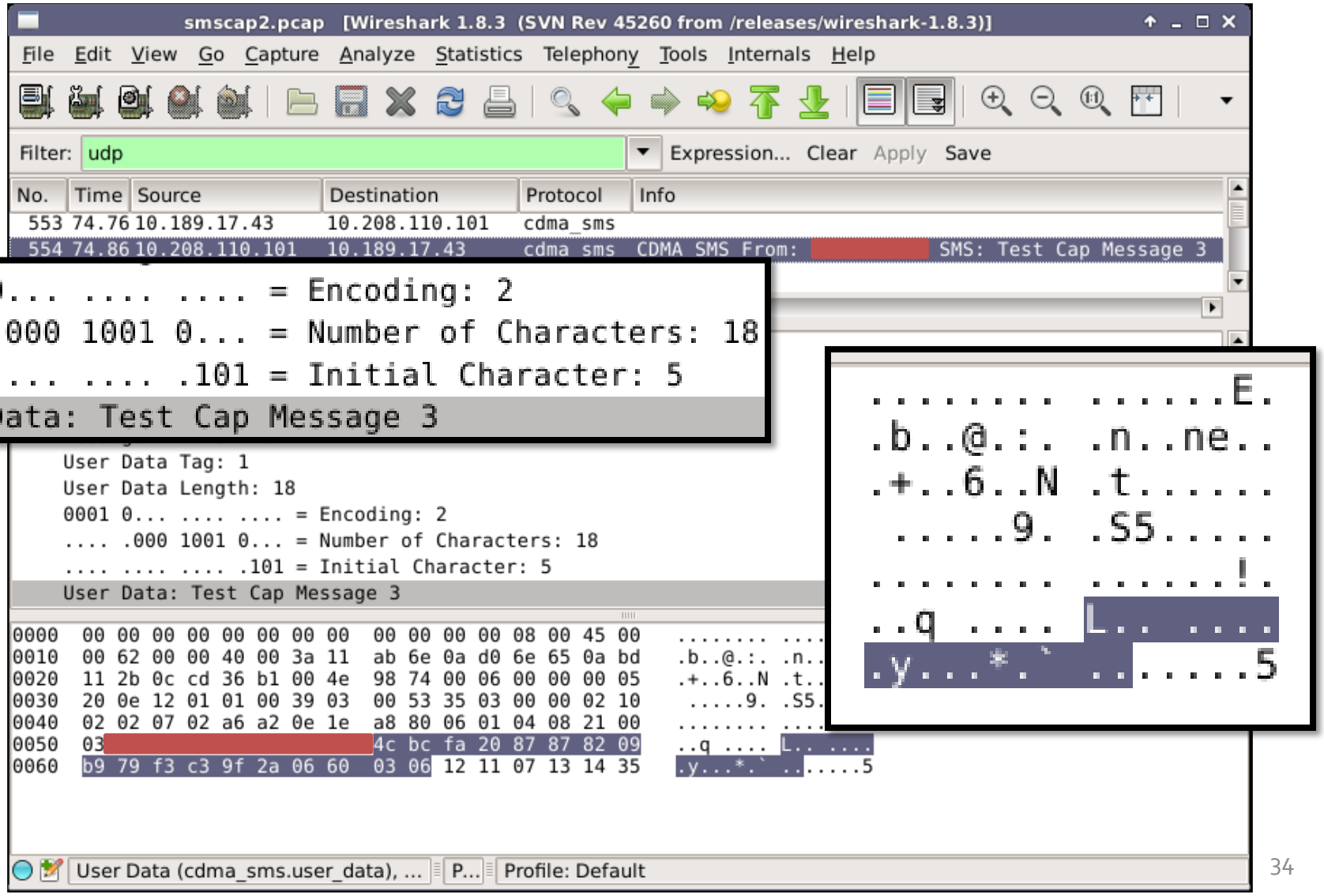
http://www.youtube.com/watch?v=3FyNB4QmY1Q

SMS

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



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: 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 ....
0010 00 62 00 00 40 00 3a 11 ab 6e 0a d0 6e 65 0a bd .b..@.:. .n..
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 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

iSECpartners part of nccgroup

http://www.youtube.com/watch?v=R-4fkJiVeE4

Data

iSECpartners part of nccgroup

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

MMS

iSECpartners part of nccgroup

http://www.youtube.com/watch?v=uuwsMsvGAYo

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…

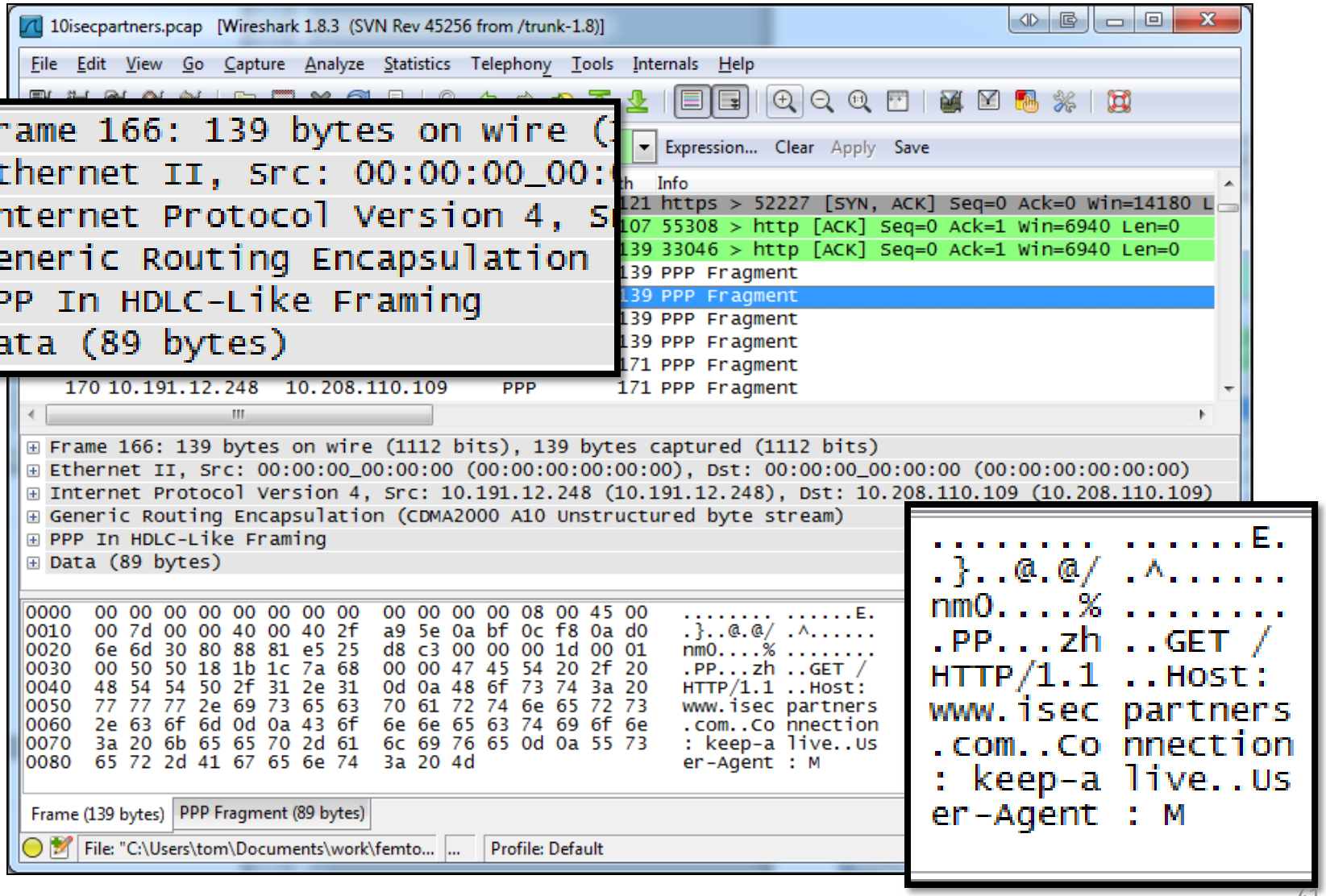
Data

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



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
- TCP Checksum is at the beginning (GRE frame N)
- PPP Checksum is at the end (GRE frame N+3? 4?)
- Oh, and the frames may be out of order

Data Middling

iSECpartners part of nccgroup

- Try 1:
  - Do it inline, in the kernel
  - Nope: Carrier applies transparent compression to all traffic on port 80
  - Can't collect packets to decompress, edit, and recompress, can't only edit one packet at a time
- Try 2:
  - Change the request to HTTP 1.0 (No Compression)
  - Nope: Carrier Ignores it

Data Middling

iSECpartners part of nccgroup

- Try 3:
  - DNS Hijack, send everyone to our server
  - Nope: Carrier does transparent proxying on port 80, then does own lookup based on Host header
- Try 4:
  - DNS Hijack AND rewrite all connections to port 80 on our IP to port 81, and back again
  - Nope: Corner Cases. If they happen 2% of the time, on a normal webpage, it's dozens of packets.

Data Middling

iSECpartners part of nccgroup

- Try 5:
  - DNS Hijack, rewrite all connections to port 80 on our IP to port 81, and back again, AND Redirect people to 8080
  - Success!
  - The corner cases don't occur on the small 301 redirect
  - We can proxy the real webpage to users, ferrying their cookies and form posts, and:
    - Strip SSL
    - Rewrite URLs to port 8080

Data Middling Video

iSECpartners part of nccgroup

http://www.youtube.com/watch?v=2xjhtDobO8c

Miniature Cell Towers

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

iSECpartners
part of nccgroup

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"
- (Phones often ALSO have an IMEI for global or 4G)

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

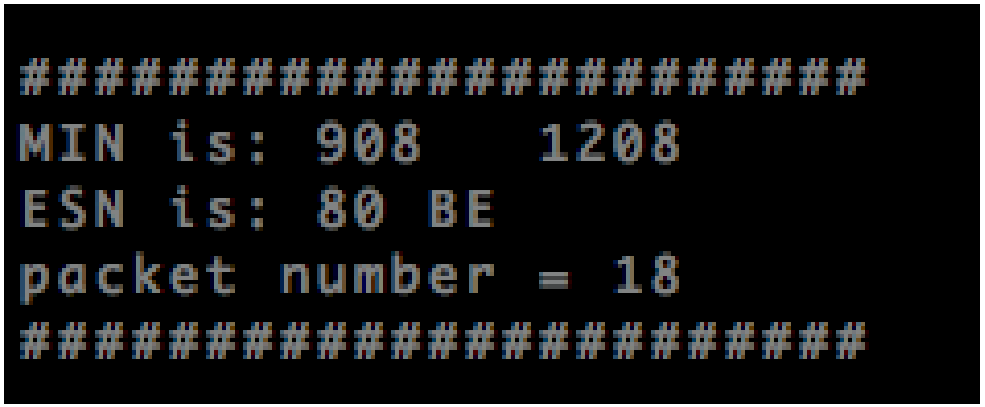
Remember Your Failure At The CAVE…

- 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

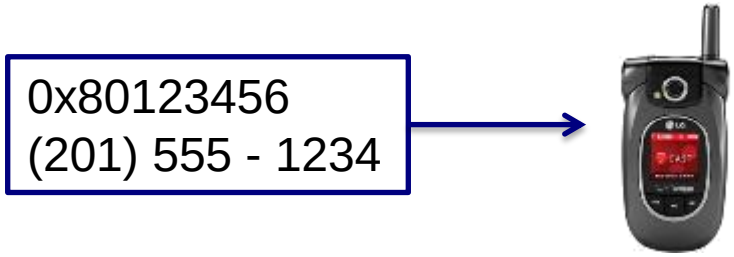
iSECpartners part of nccgroup

- (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***



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

Cloning Implications

iSECpartners part of nccgroup

- Cloning can be flakey
- Voice
  - The elusive 2.5-way call
- SMS
- Data
  - Not yet….
- Helpful definitions for our discussion:

Victim phone – the phone of a legitimate subscriber whose keys have been captured by a rogue femtocell

Target phone – the phone of an attacker that has been modified (cloned) to the legitimate victim phone

Cloning Scenario 0

When the VICTIM phone is turned off or jammed

- Everything works
  - Incoming Call
  - Outgoing Call
  - SMS

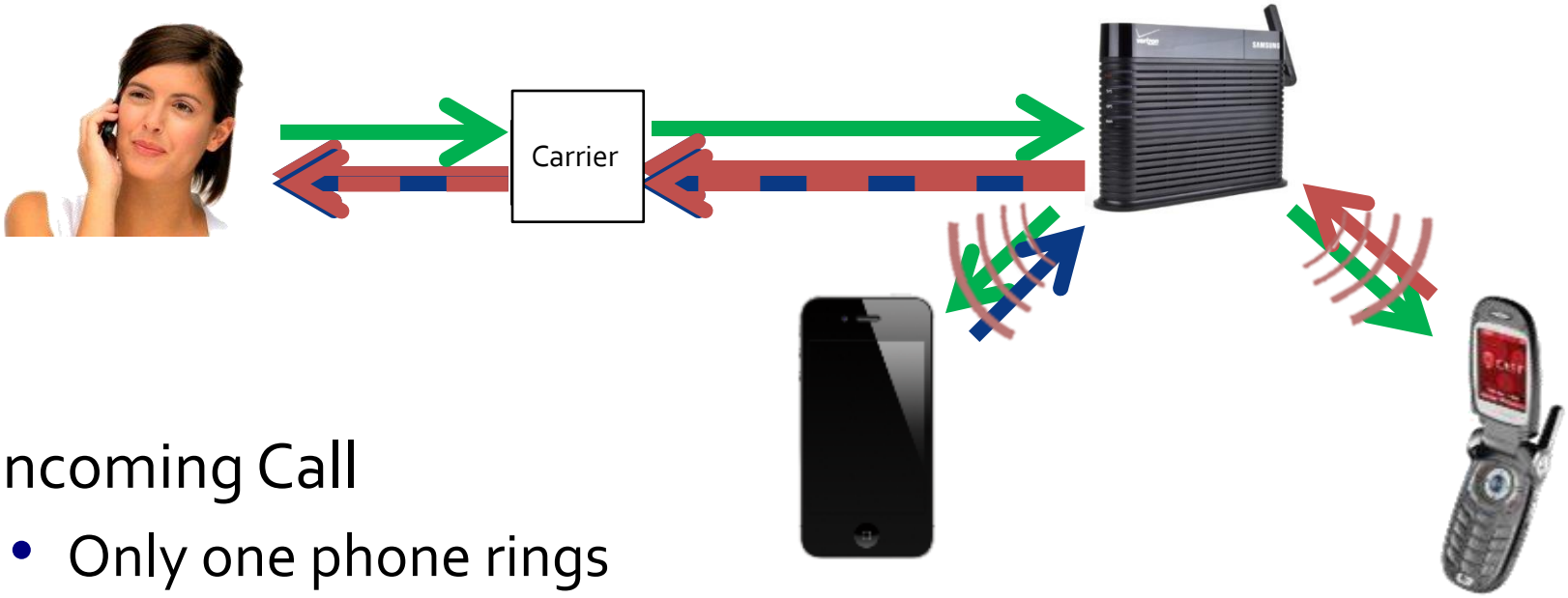
Cloning Scenario 1

When both the TARGET and VICTIM phones are associated with the femtocell.

- Outgoing Call
  - Forced drop
- SMS
  - Incoming

Cloning Scenario 1

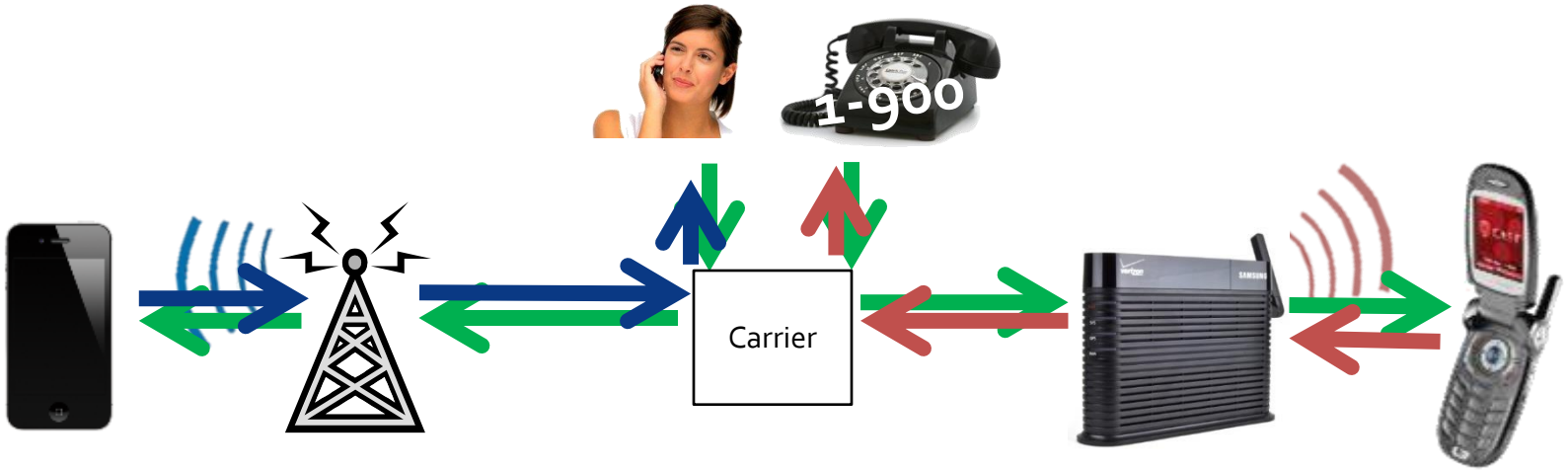
When both the TARGET and VICTIM phones are associated with the femtocell.



- Incoming Call
  - Only one phone rings
    - Situation normal
  - Both phones ring
    - The race is on
    - "Two-and-a-half"-way call

Cloning Scenario 2

When only the TARGET phone is associated to the femtocell and the VICTIM phone is on an actual Verizon tower



- Incoming Call and SMS
  - Most recent carrier contact
- Outgoing Call
  - TARGET call is dropped
  - Two for one!

Cloning Data

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

Cloning Video

iSECpartners part of nccgroup

http://www.youtube.com/watch?v=Ydo19YOzpzU

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.

iSECpartners
part of nccgroup

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

iSECpartners part of nccgroup

- Harden the femtocell hardware and software

- That might help except…

Root is always possible

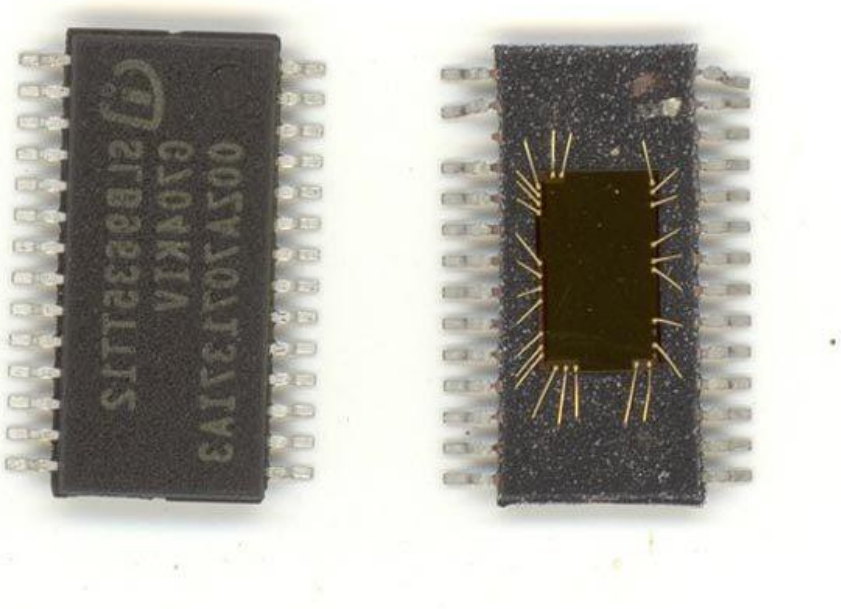
iSECpartners part of nccgroup

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

Root is always possible

iSECpartners part of nccgroup

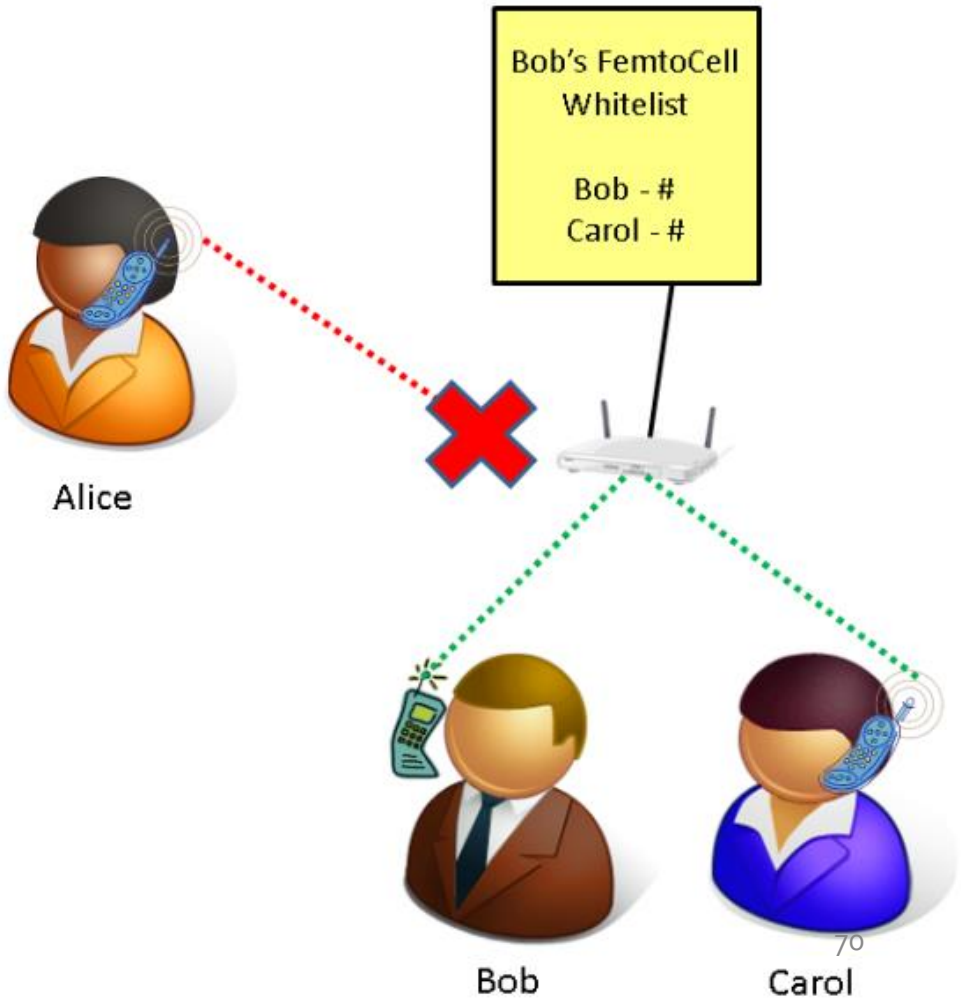
- We got in through a serial port
- JTAG / UART ports?
- Reflash firmware?
- Glitching Attacks?



Short Term Mitigations

Require phone registration

- Capability currently exists



Femtocell Handset Registration

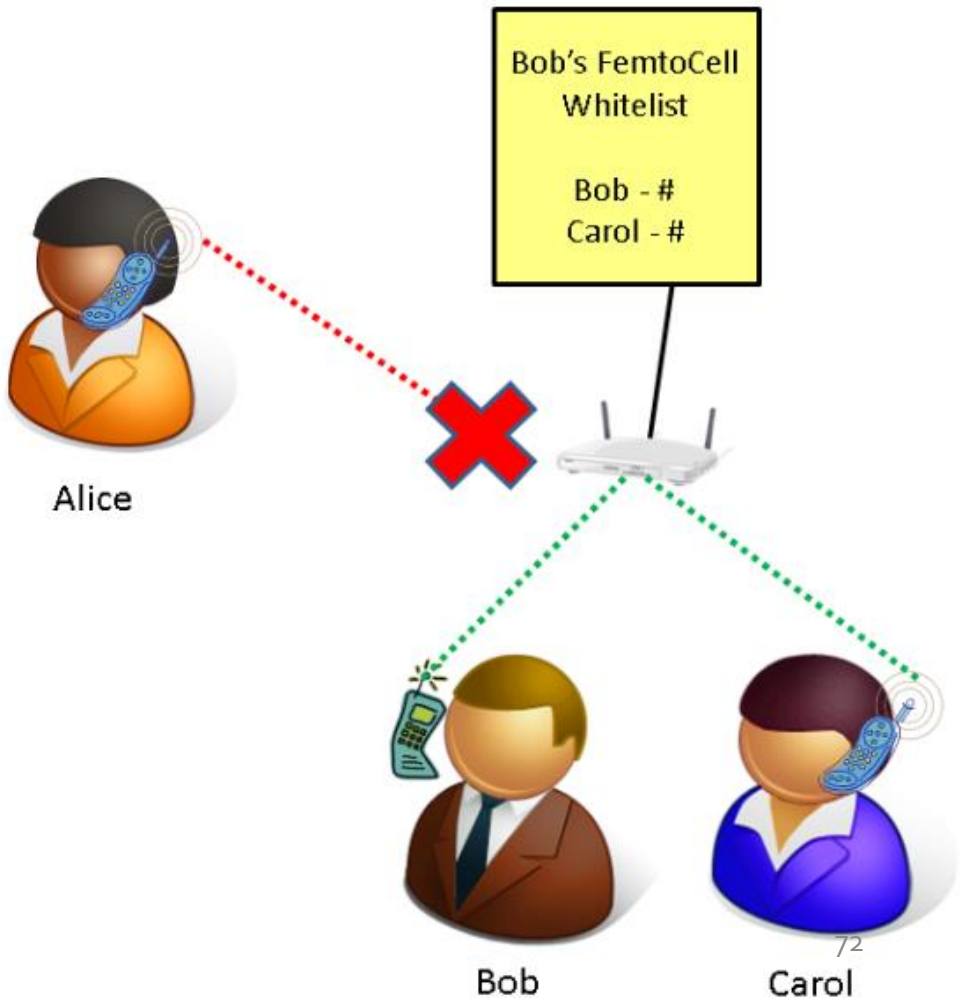
iSECpartners part of nccgroup

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



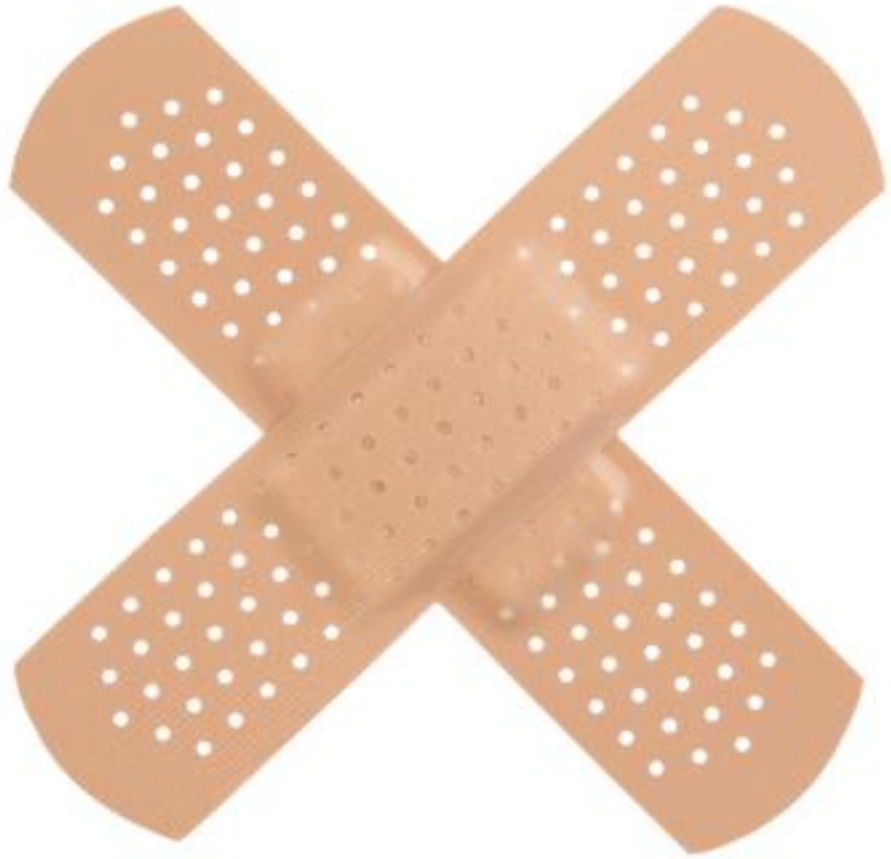
Long Term Mitigations

iSECpartners part of nccgroup

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

iSECpartners
part of nccgroup

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

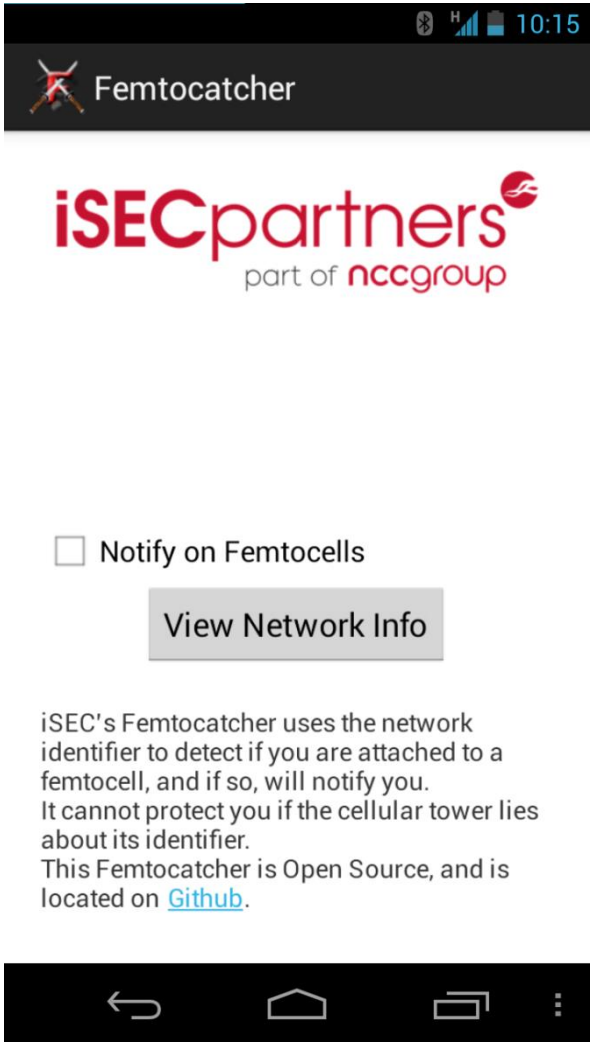
What Can / Do?

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



What Else Can I Do?

iSECpartners part of nccgroup

- End-To-End Encryption
- Voice
  - RedPhone
  - OSTel
- SMS / Chat
  - TextSecure
  - Gibberbot
  - Silent Circle
  - Wickr
- Browsing
  - VPN
  - Tor (Android: Orbot+Orweb iOS:Onion Browser)

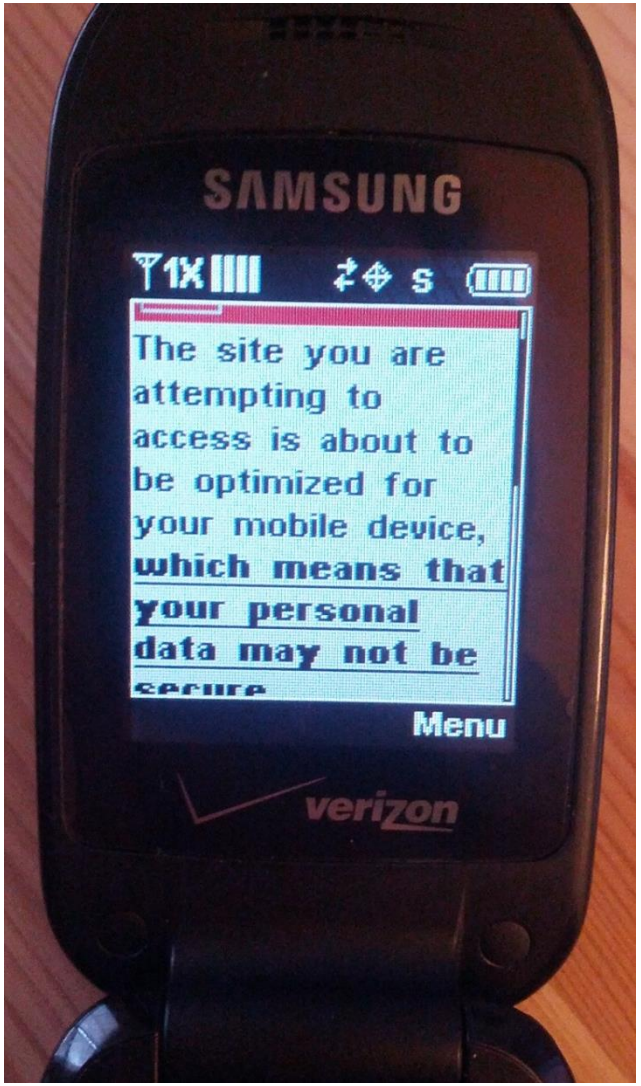
iSECpartners
part of nccgroup

Future Work

WAP (Wireless Application Protocol)

iSECpartners part of nccgroup

- Custom Protocols
- Heavily Proxied
  - Forced gzip
  - Chunked Encoding
- SSL Middling
  - Advertised…
  - …or not (Nokia)



WAP

Nokia 105 and 301 candybar phones announced at MWC, offer simplicity on the cheap

By **Brad Molen** posted Feb 25th, 2013 at 2:41 AM 13

Additionally, the 301 lets you take advantage of Mail for exchange, Nokia Xpress internet (which compresses data down by about 90 percent) and HSPA connectivity with video sharing.

iSECpartners
part of nccgroup

Fuzzaaaaaaaaaaaaaaaaaaing

- What happens when you fuzz the baseband?

iSECpartners
part of nccgroup

Internal Femtocell Network

- Femtocell -> Femtocell (rsaxvc/BH2011)
- Femtocell -> Internal Carrier Network (BH2011)

Thank You & Questions?

iSECpartners part of nccgroup

- Doug DePerry
  - Senior Security Engineer at iSEC Partners
  - @dugdep
  - doug@isecpartners.com
- Tom Ritter
  - Principal Security Engineer at iSEC Partners
  - @TomRittervg
  - tritter@isecpartners.com
- Thanks to
  - RSAXVC & Doug Kelly
  - Andrew Rahimi, Davis Gallinghouse, Tim Newsham
    - These guys did much of the hard work
  - Mira, Michael, Pratik, Peter Oehlert, Joel Wallenstrom, and really all of iSEC