



Northeastern University

Systems Security Lab



Probing Mobile Operator Networks

CSAW

Collin Mulliner, October 15th 2012, New York City, USA
crm[at]ccs.neu.edu

NEU SECLAB

\$ finger collin@mulliner.org

- 'postdoc' Security Researcher
 - \$HOME = Northeastern University, Boston, MA
 - cat .project
specialized in *mobile handset security*
- Past work
 - Some Bluetooth security work
 - A lot on SMS and MMS security
 - Mobile web usage and privacy
 - Some early work on NFC phone security
 - ... you get the picture ;-)

Overview

- History & Motivation
- How to probe & what to probe for
- Analysis Methods
- Results
- Results
- Conclusions

History

- I scanned public IPs of MNOs in 2009
 - No talk because of Ikee
- The Ikee.A/B worm + botnet
 - Targeted jailbroken iPhones
 - SSH installed
 - Default root password 'alpine'
 - Spread via scan of public IP ranges of MNOs
 - Active around November 2009
 - Hijacked devices to ask for ransom

see summary at: <http://mtc.sri.com/iPhone/>



My blog post on iPhone + SSH (end of 2008)

Friday, December 19 2008

The Danger of Jailbroken iPhones (not really news)

first, I known I'm not the first one to write/warn about this so don't flame me for it.

I recently jailbroken my iPhone so I could take a closer look at the iPhone and it's OS. As most people I just used the [PwnageTool](#) from the iPhone Dev-Team. It is easy, fast and just works. So what most people forget is that the jailbroken iPhone OS comes with an ssh server and that the *root* and *mobile* users have their password set to *alpine* (mobile password is *dottie*). This basically means that everybody can log into every jailbroken iPhone as user root. When I jailbroke my iPhone I didn't change my password right away since I was too busy playing with the new features and I strongly believe that many other people never changed the password of their jailbroken iPhone.

Again the danger lies in public Wifi hotspots or any other situation where you share Wifi with people you don't know. A good example is the upcoming [Chaos Communication Congress](#) which has one of the most hostile (wireless) networks I know.

So what can happen if you leave your iPhone's password unchanged? That is what I cooked up the last few nights.

The Basics:

- Anyone can log into your iPhone as user root and/or mobile
- Anyone can copy files to and from your iPhone using scp

In further detail this means all your private data is gone, just like this:

```
SSH_PARAMS="-q -o NumberOfPasswordPrompts=1 -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no"
scp $SSH_PARAMS root@$IP:/var/mobile/Library/AddressBook/* /tmp/yourdata/
scp $SSH_PARAMS root@$IP:/var/mobile/Library/SMS/* /tmp/yourdata/
scp $SSH_PARAMS root@$IP:/var/mobile/Library/Notes/* /tmp/yourdata/
scp $SSH_PARAMS root@$IP:/var/mobile/Library/Calendar/* /tmp/yourdata/
```

Motivation

- What kind of devices are on mobile networks today?
 - Number devices
- Security of those mobile connected devices
 - They probably are not seen as being on the Internet
- What devices are worth looking at?
 - Starting point for next project(s)
- Forecast on mobile network usage in the future
 - People have strange ideas...

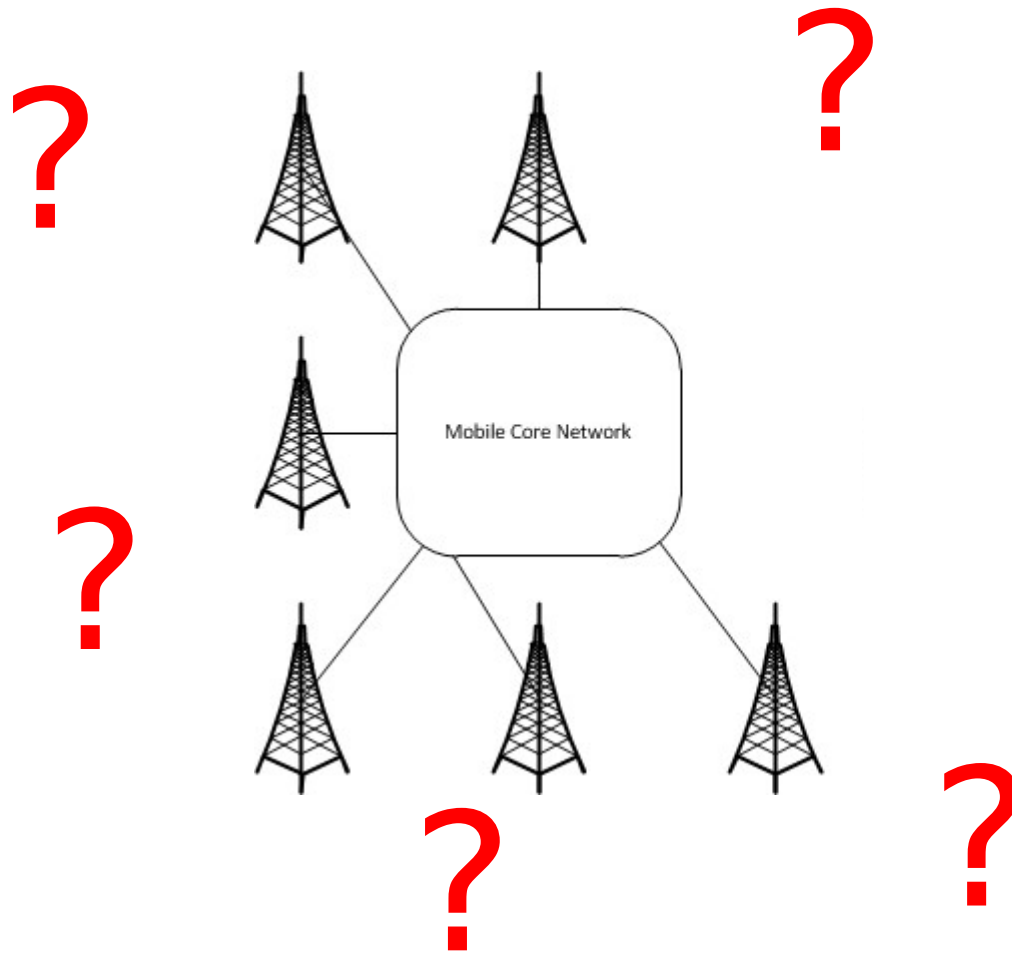
So...

- Mobile Network Operators (MNOs)
 - Do they know what devices are on their network?
 - Maybe they don't know – liability if they know?
- You, the audience: what do you expect?
 - Mobile phones?
- Hint hint ...
 - Findings are way more interesting than mobile phones!

Yes, this is a IP/port scanning talk!

- I've always wanted to do one :-)
- But I'm a “mobile” guy
- So I scanned the IPs of mobile operators
- No fancy super duper hot technique
 - But we get the data we want!

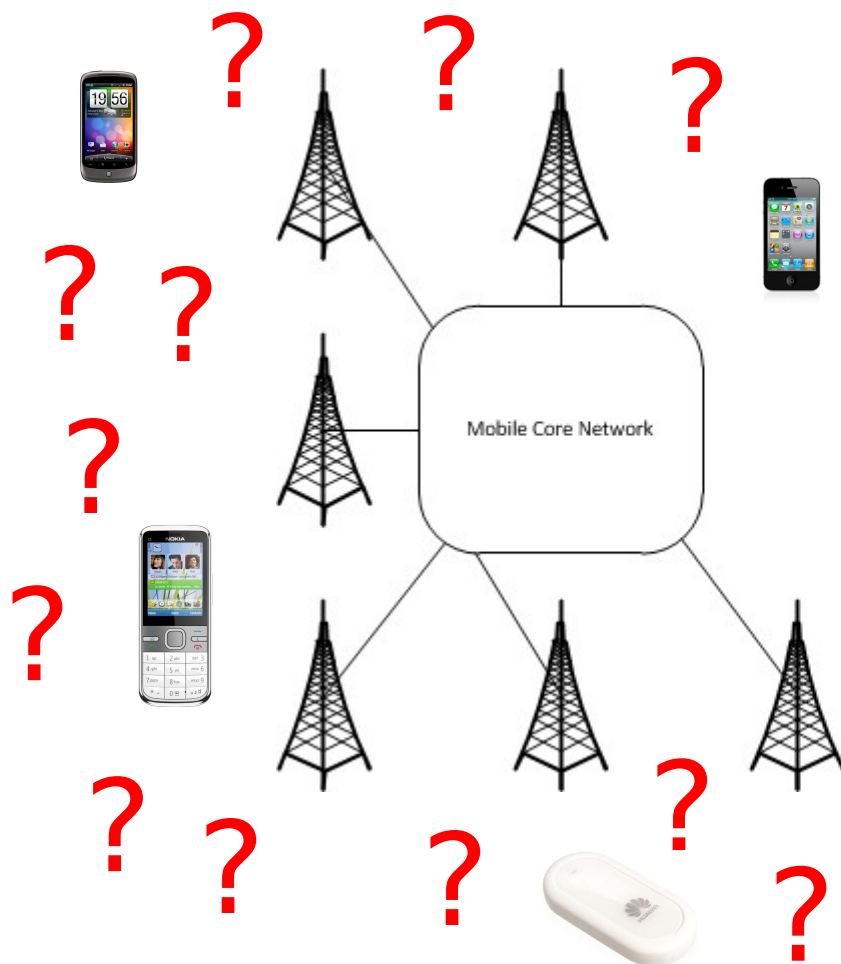
Devices on Mobile Networks: ?



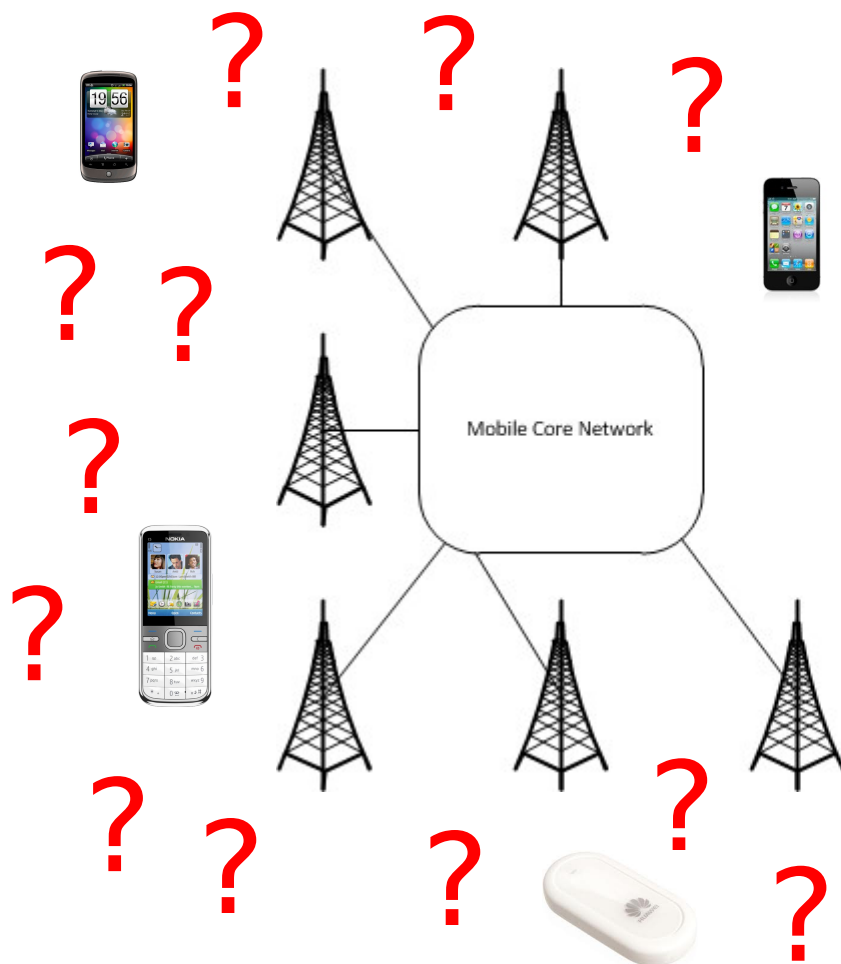
Devices on Mobile Networks: some knowledge



There should be more, right?



Probing Mobile Networks: scan from within net



Hook up laptop to cellular network and scan IP range of mobile operator.

Scanning from within the Mobile Network

- Depends on Access Point Name (APN) configuration
 - Inter-client connections allowed? ← **MOST IMPORTANT!**
- Need SIM card from each operator you want to scan
 - Costs + accessibility

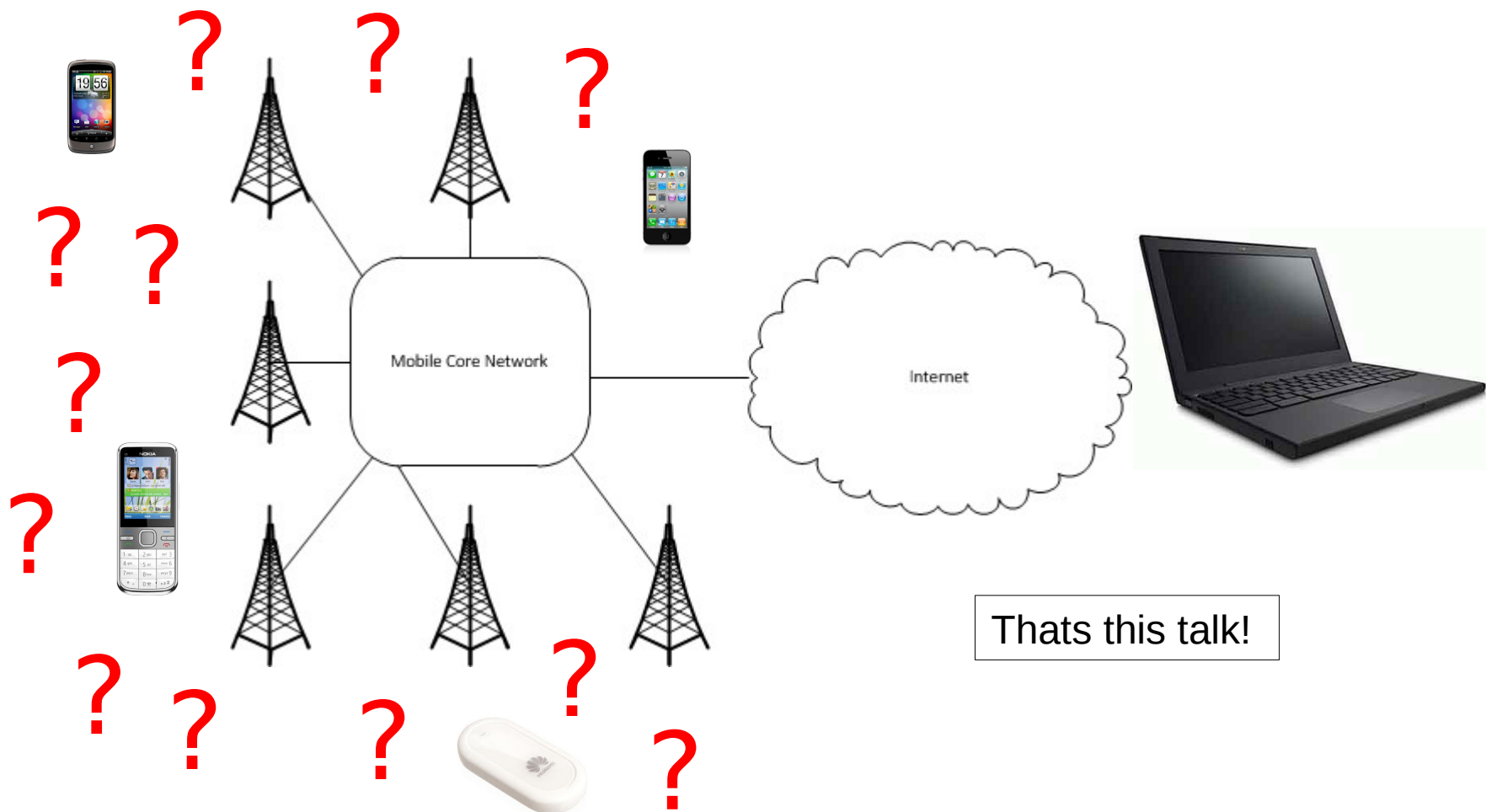


- Scanning will cost extensive amounts of money
 - Scanning foreign operators will cost even more
 - Roaming charges!

Special case APNs

- Special APNs for:
 - eBook readers (see my 2010 CanSec talk)
 - M2M (Machine-to-Machine) devices ← **TOP TARGETS**
 - Fancy toys
- Access to hardware
 - Extract SIM card
 - Get APN name
 - Obtain APN username and password (if required)
- Check if inter-client connections are possible
 - Scan...

Probing Mobile Networks: from the Internet

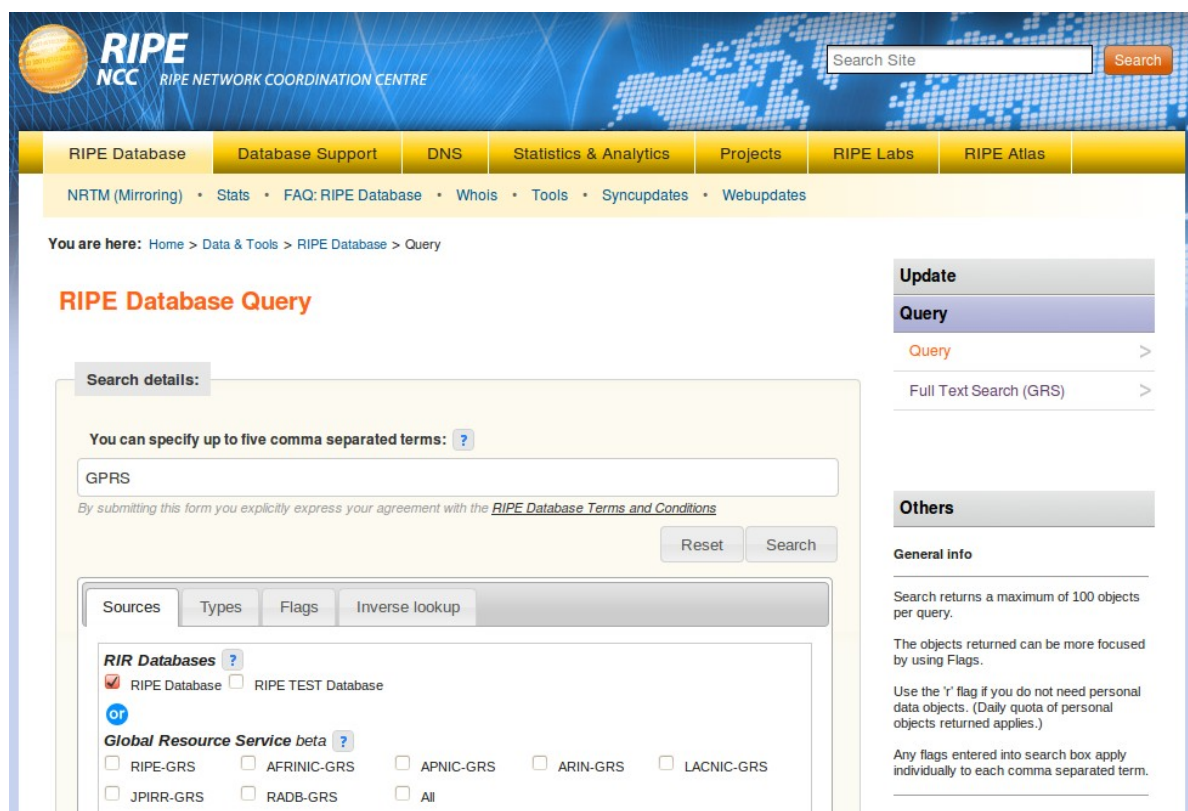


Acquiring IPs to scan...

- Regional Internet Registry databases
 - ARIN (American)
 - RIPE NCC (Europe)
 - ...
- Ikee.A/B's scan list
 - Europe + Australia
- Web server logs (my web server)
 - I have a lot of mobile visitors
- Search the “internetz”

RIPE NCC Database Search (my pick for now)

- Can also can search AFRINIC and others, sadly not ARIN
 - ARIN search sucks!



The screenshot shows the RIPE NCC Database Query interface. At the top, there's a search bar and a navigation menu with links like 'RIPE Database', 'Database Support', 'DNS', 'Statistics & Analytics', 'Projects', 'RIPE Labs', and 'RIPE Atlas'. Below the menu, there's a breadcrumb trail: 'You are here: Home > Data & Tools > RIPE Database > Query'. The main heading is 'RIPE Database Query'. Under 'Search details:', there's a text input field containing 'GPRS' and a 'Search' button. Below the input field, there's a link to 'RIPE Database Terms and Conditions'. To the right of the search input, there's a 'Reset' button. Below the search input, there's a section for 'Sources' with tabs for 'Types', 'Flags', and 'Inverse lookup'. Under 'Sources', there's a section for 'RIR Databases' with a checked box for 'RIPE Database' and an unchecked box for 'RIPE TEST Database'. Below this, there's a section for 'Global Resource Service beta' with a checked box for 'RIPE-GRS' and unchecked boxes for 'AFRINIC-GRS', 'APNIC-GRS', 'ARIN-GRS', 'LACNIC-GRS', 'JPIRR-GRS', 'RADB-GRS', and 'All'. On the right side of the page, there's a sidebar with sections for 'Update', 'Query', 'Others', and 'General info'. The 'Query' section has links for 'Query' and 'Full Text Search (GRS)'. The 'General info' section contains text about search results and flags.

Search terms, IPs, Problems

- RIPE Database searches
 - GPRS → 8.600.012 IPs
 - GGSN → 742.400 IPs
 - M2M → 27.904 IPs
- Unique total IPs: **9.306.060 IPs**
 - “Text” searches return overlapping ranges
- Problems
 - Netblocks are not “marked” honestly/correctly
 - Subnet might be used for DSL/cable/etc...
 - Netblock might NOT be marked as GPRS
 - Will likely miss a lot of IPs

More Problems...

- NAT (Network Address Translation)
 - Mobile phones often sit behind a NAT gateway (just check your own mobile phone)
 - NAT → devices unreachable from the Internet
 - Devices that don't sit behind NAT are interesting
 - Reason for being reachable?
- Most mobile phones don't run services
 - No open ports, nothing to connect to
 - iOS iPhone/iPad are exception (iphone-sync service)

... even more Problems

- GPRS is slow → scanning will take time
 - Bandwidth
 - Devices go into sleep mode when not active
 - 'wake up device when scanner connects'
- Devices move, get disconnected, etc... → new IP address
 - Problems
 - Device will be scanned multiple times
 - Device will never be scanned at all
- Scan blocked by operator because you light-up in his IDS

My Scanner

- Python TCP socks-client
 - For using TOR
- Connect to port
 - Send “string”, special “strings” for each port
 - Port 23: minimal telnet implementation
 - Port 80: “GET / HTTP/1.0\r\n”
 - ...
 - Save port status and responds → classic banner grab
- Randomized IP address list
 - Prevent to easily show up in operator's IDS

Scanning using TOR



- Anonymity
 - I kinda have a meaningful PTR record
 - AWS EC2 would be another way to solve this!
- **Scan from many different IPs**
 - Yay for NOT being blocked halfway through the project!
- But TOR is slow!
- Sorry for sucking up a lot of TOR capacity!
 - TOR capacity is limited, you should run a TOR node!

Ports / TCP only

- Side effect if you use TOR
 - No real issue for identifying devices

21	FTP
22	SSH
23	TELNET
80	HTTP
443	HTTPS
62078	iphone-sync
5060	SIP
8082	TR-069 on some devices
161/162	SNMP

SSH Probe

- If port 22 connects...
- Try password(s) 'alpine' and 'dottie' for iOS devices
- If we get shell, run:
 `uname -a; ps ax; ifconfig -a; dmesg`
 - This will generate a nice system fingerprint and a lot to look at
- This special probe of course has some ethical issues!
 - Hopefully no trouble for me!
- You'd be surprised that this is actually quite useful ;-)
 - Especially non iOS stuff!

Scanning...

- 1) Split up the IP address list
- 2) Run scanner on N machines
- 3) Check every few weeks
 - Do other research
 - From time-to-time: restart, fix, yell, look at data
 - Back to 2)
 - Decide to end project, goto 4)
- 4) Analyze data
 - Give talk & write paper ← still in progress

Responsible “Data” Disclosure

- So far I only talked to few people about this
 - Little to none pre notification
 - This talk should be kind of a wakeup call
- Some of the stuff is a little scary
 - I don't want people to get hurt
- I wont disclose some specific data
 - IP addresses and/or ranges for targets
 - Names of Mobile Network Operators
 - Specific stuff I found
 - Details of some targets (or where I omitted them)

Raw Data

- IP, time stamp, port, status, banner

```
85.26.x.x 1327277970 22 0 SSH-2.0-moxa_1.0\r\n
85.26.x.x 1327277970 21 111
85.26.x.x 1327277970 23 0
\xff\xfb\x01\xff\xfb\x03\xff\xfb\x00\xff\xfd\x00OnCell
G3150_V2\r\x00\nConsole terminal type (1: ansi/vt100
85.26.x.x 1327277970 80 0
85.26.x.x 1327277970 443 112
85.26.x.x 1327277970 62078 111
85.26.x.x 1327277970 5060 112
85.26.x.x 1327277970 8082 112
85.26.x.x 1327277970 161 112
85.26.x.x 1327277970 162 112
```

0 = open, 111 = closed, 112 = not scanned

Data Analysis & Verification

- By hand
 - Fun, needed to find some of the interesting devices
 - Not working for large scale analysis
 - grep for strings like: login, welcome, authenticate, ...
- Automated
 - Criteria?
- Verification
 - Web search for “product ID”
 - Connect to service (try default login/pass)
 - Very very few cases
 - We want to stay on the legal side!

Automated Data Analysis

- Find similar devices
 - **Fuzzy cluster similar banners for each port**
 - Stripping stuff like: versions, build, etc...
 - group/count devices
- Type of IP address/range: dynamic vs. static
 - Device on same address across multiple scans
 - Devices on static IPs are a real catch!
- Post Analysis : manual stuff again
 - Identify devices (lucky)
 - Identify software running on device (if unlucky)

Banner Clusters - Statistics

- Banner tells us what software is responding to our scan
 - Software tells us the kind of device
- Ports
 - SSH (22), FTP (21), Telnet (23), HTTP (80), ~~SIP (5060)~~

Disclaimer!

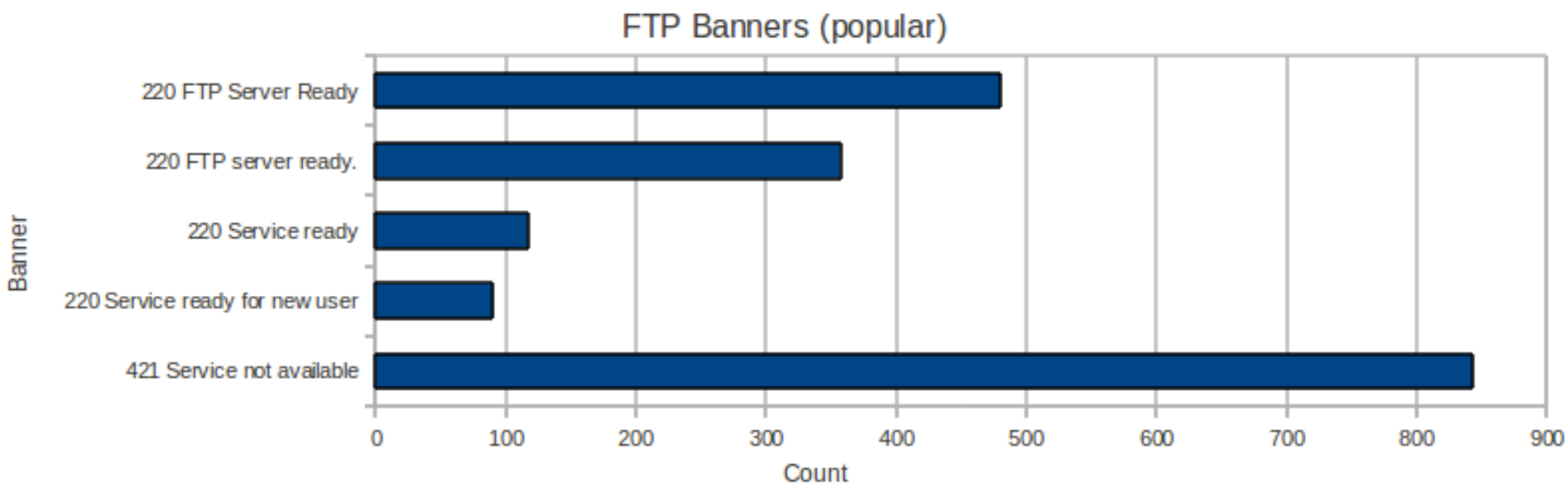
- These are all devices I found while scanning
- These are just examples
- This is not to blame or discredit manufacturers or operators!

SIP Banners Stats

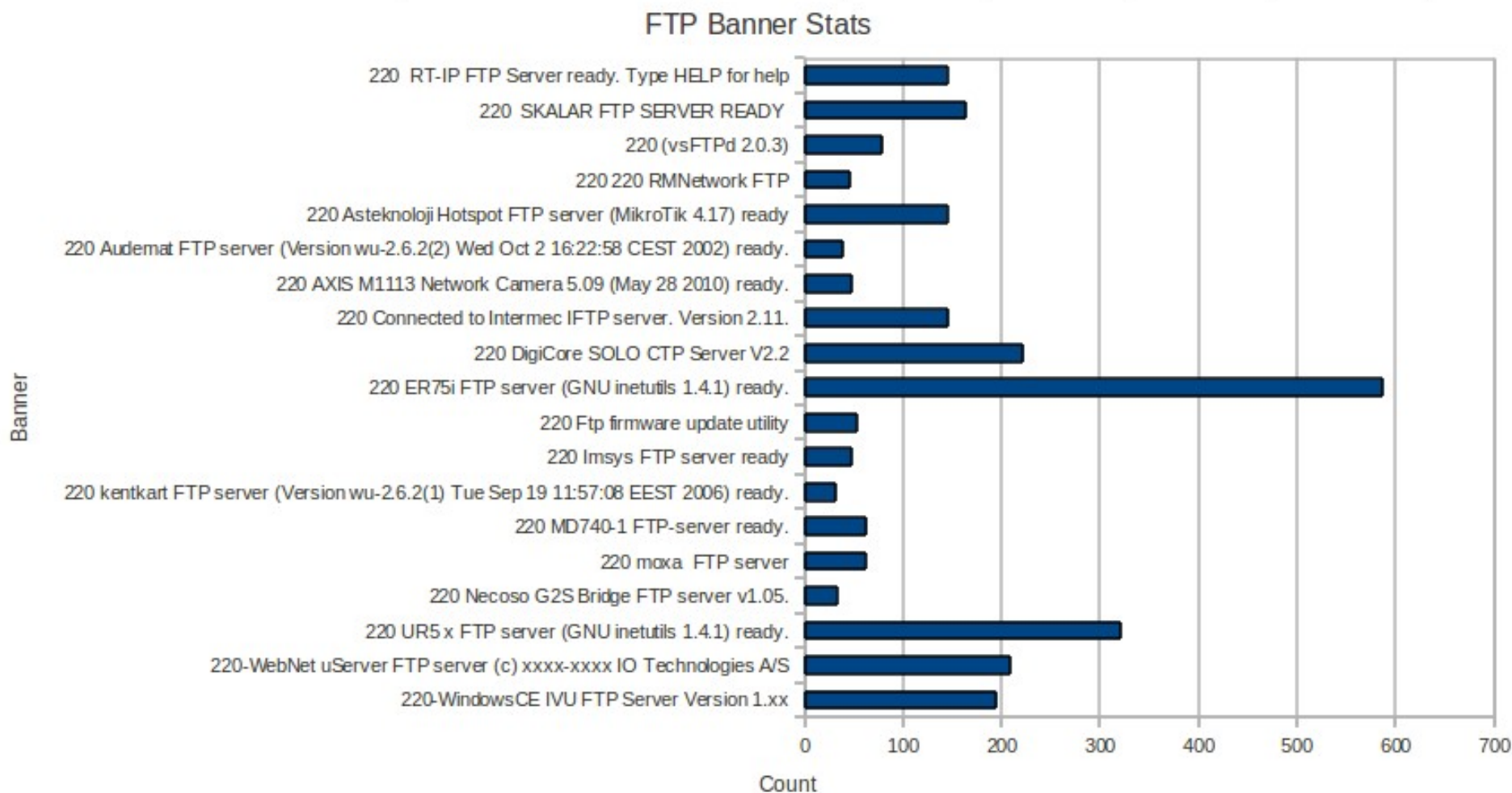
- Many devices with open ports
- Just one banner
 - SIP not further discussed in this talk!

```
SIP/2.0 200 OK\nVia: SIP/2.0/TCP  
127.0.0.1:5060;branch=1234567890\nFrom:  
sip:1234567890@127.0.0.1;tag=bad-012345\nTo:  
<sip:0987654321@127.0.0.1;user=phone>;tag=bad-012345\nCall-  
ID: 1348979872-797979222304855\nCseq: 15 INVITE\nContact:  
sip:0987654321@127.0.0.1\nContent-Length: 401\nContent-Type:  
application/sdp\n\nv=0\nAnonymous 1234567890 9876543210 IN  
IP4 127.0.0.1\ns=SIGMA is the best\ns=gotcha\nc=IN IP4  
127.0.0.1\nm=audio 36952 RTP/AVP 107 119 100 106 6 0  
97 105 98 8 18 3 5 101\na=rtpmap:107 BV32/160
```


FTP Banners (popular but useless)



FTP Banners Statistics



FTP Banner Statistics : Results

- 220 DigiCore SOLO CTP Server V2.2
 - Devices: >200
 - Networks: Germany, Finland, Belgium
 - Application: Vehicle Tracking

- Online search on “DigiCore”
 - GPS Tracking company
 - They build trackers for everything
 - Delivery truck
 - Rental cars
 - Individuals



DigiCore Sole Device

<http://www.digicore.com>

FTP Banner Statistics : Results

- 220 Connected to Intermec IFTP server.
 - Devices: ~150
 - Networks: Turkey, Hungary, Portugal, Germany, Czech
 - Application: Supply chain management devices
 - Barcode scanners, etc...
 - Details
 - Windows Mobile Devices



http://www.intermec.com/products/computers/handheld_computers/index.aspx

FTP Banner Statistics : Results

- 220 Welcome to Mobile File Service\r\n\r\n
 - Devices: >150
 - Application: Windows Mobile FTP
- 220-WindowsCE IVU FTP Server Version 1.xx
 - Devices: ~200
 - Application: Windows Mobile FTP
- Windows Mobile still seems popular
 - Also a lot of use in industrial applications

FTP Banner Statistics : Results

- 220 Imsys FTP server ready
 - Devices: ~50
 - Networks: Germany
 - Application: unknown (www.imsystech.com/)
- 220 RT-IP FTP Server ready.
 - Devices: ~150
 - Application: unknown (www.computer-solutions.co.uk)
- **Embedded SDKs**
 - Probably worth taking a look at

FTP Banner Statistics : Results

- 220 Welcome to the Leica Geosystems FTP server
 - Devices: ~20
 - Networks: France, Bulgaria, Portugal,
 - Application: Measurement Laser/GPS



http://www.leica-geosystems.com/en/Products_885.htm

FTP Banner Statistics : Results

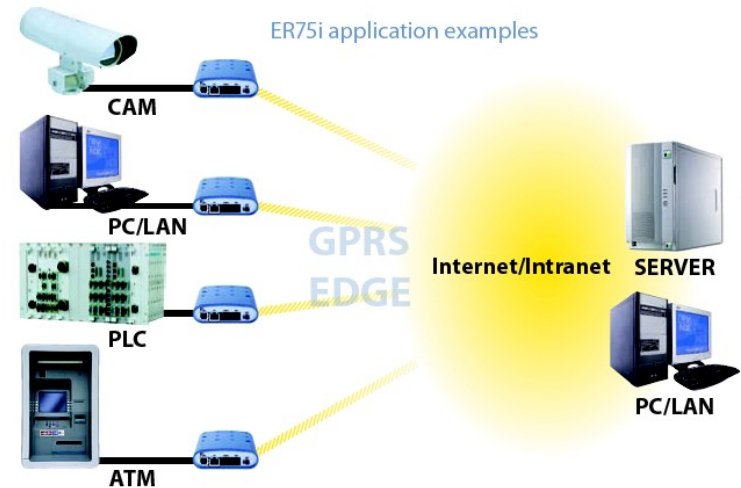
- 220 TAINY GMOD-V2 FTP-server ready.
 - Devices: 33
 - Networks: Germany
 - Application: M2M communication device
 - Manufacturer: Dr. Neuhaus



http://www.neuhaus.de/Produkte/M2M_Telemetrie/TAINY_GMOD-T1.php

FTP Banner Statistics : Results

- 220 ER75i FTP server (GNU inetutils 1.4.1) ready.
 - Devices: >500
 - Networks: Sweden, Belgium, Romania, Switzerland, Turkey, Germany, Russia, Czech,
 - Application: Industrial GSM/GPRS router
- Found several “ethernet” devices
 - Could be connected through on of these or similar



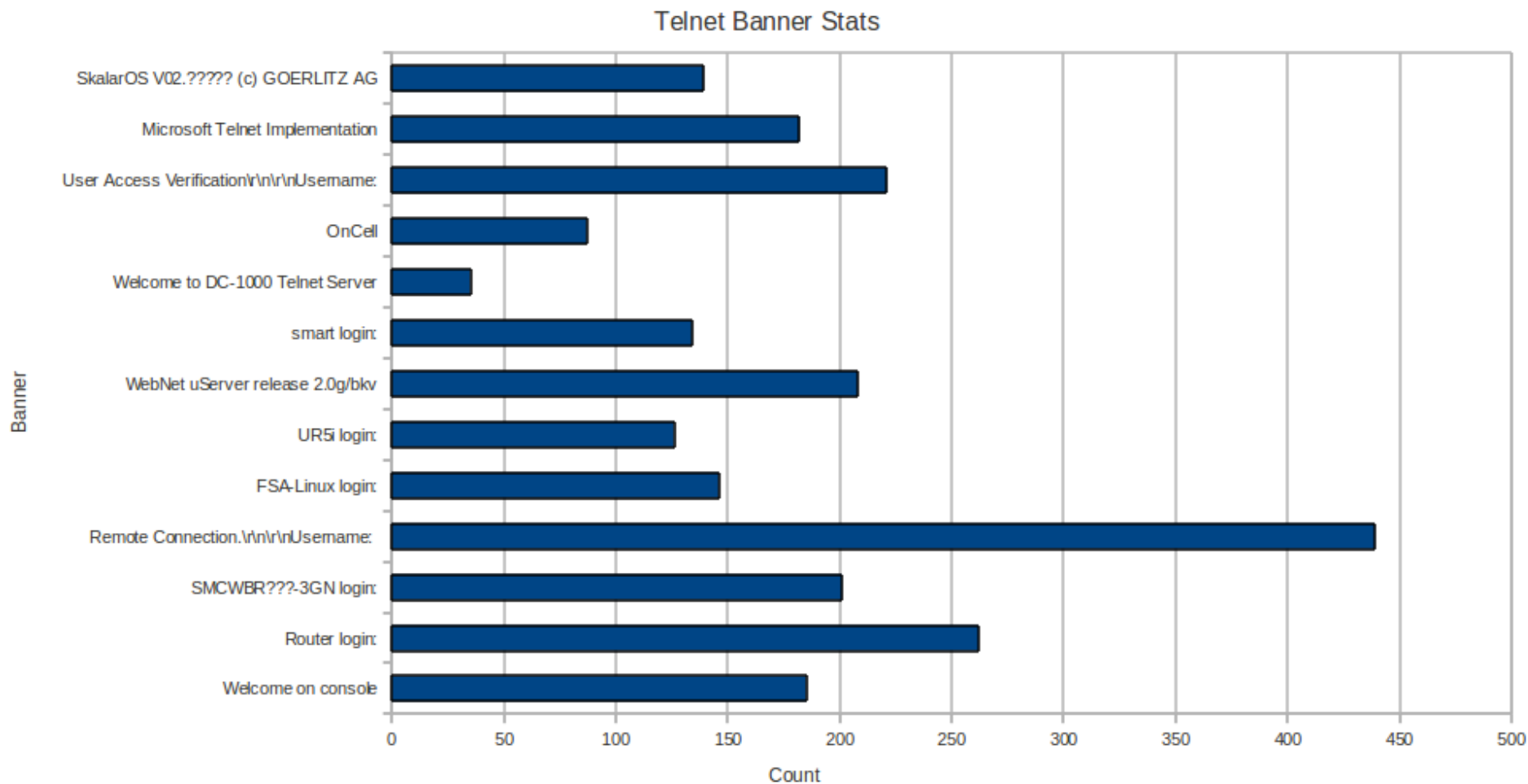
Source: product site

NEU SECLAB

FTP Banner Statistics: Results (and Telnet)

- `220-National Instruments FTP\r\n220 Service Ready`
 - FTP, few hits only
- `Remote Connection.\r\n\r\nUsername:`
 - Telnet, many hits
- Telnet + FTP → device Identification
 - Devices: +400
 - Networks: Portugal, Germany, France, Turkey
 - Application: Industrial measurement (expensive stuff)

Telnet Banner Statistics



Telnet Banner Statistics: Results

- SMCWBR11S-3GN login:
 - Networks: Portugal
 - Devices: >100
 - Application: 3G Home router



<http://www.smc-asia.com/products03.php?Fullkey=210>

Telnet Banner: Special Finds (NDL485)

- Telnet
 - NDL485-2545532156 login
- FTP
 - 220 NDL485-2545532156 FTP server (GNU inetutils 1.4.2) ready.
- Devices: ~50
- Networks: France, Germany
- IP ranges: Dynamic
- Application: environmental sensor



http://www.wilmers.com/html_en/html/dataloggers_en.html

Telnet Banner: Special Find (TDS 821)

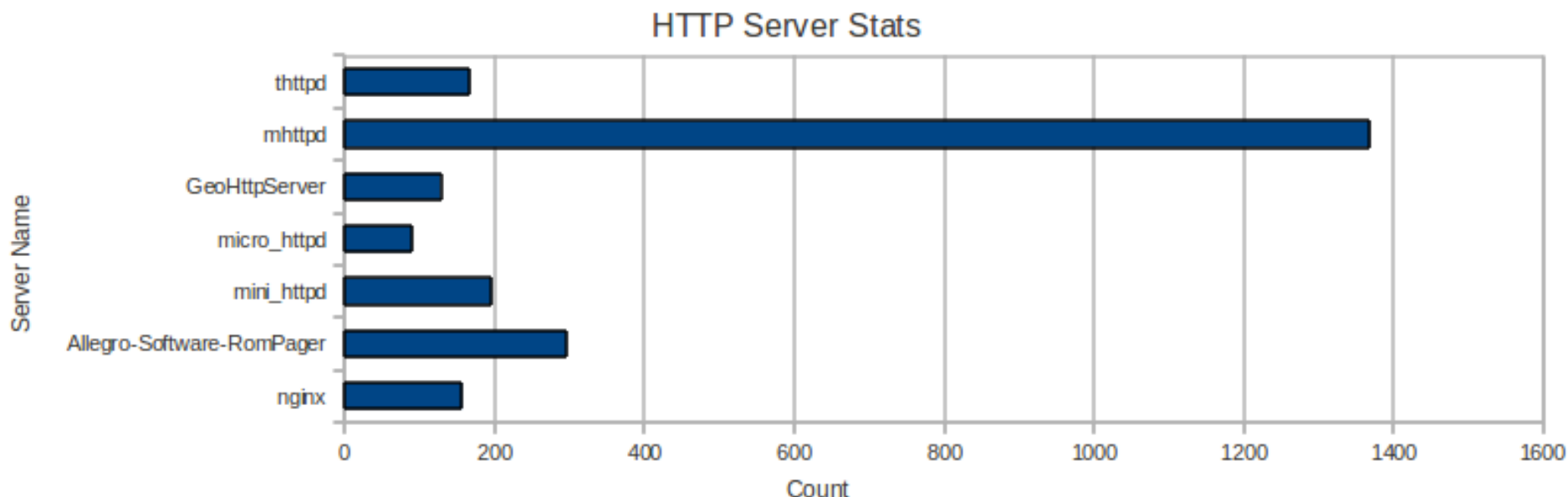
- 220-You are user number 1 of 5 allowed.\r\n220-Setting memory limit to 1024+1024kbytes\r\n220-Local time is now 15:28 and the load is 0.80.\r\n220 You will be disconnected after 1800 seconds of inactivity.\r\n
- TDS 821 tds821\r\n\r\ntds821 login:
- Networks: Germany
- Devices: ~20
- IP ranges: static IP (multiple scans)
 - Not online anymore



<http://www.traffic-data-systems.net/en/traffic-monitoring-systems/tds-821rvdk900.html>

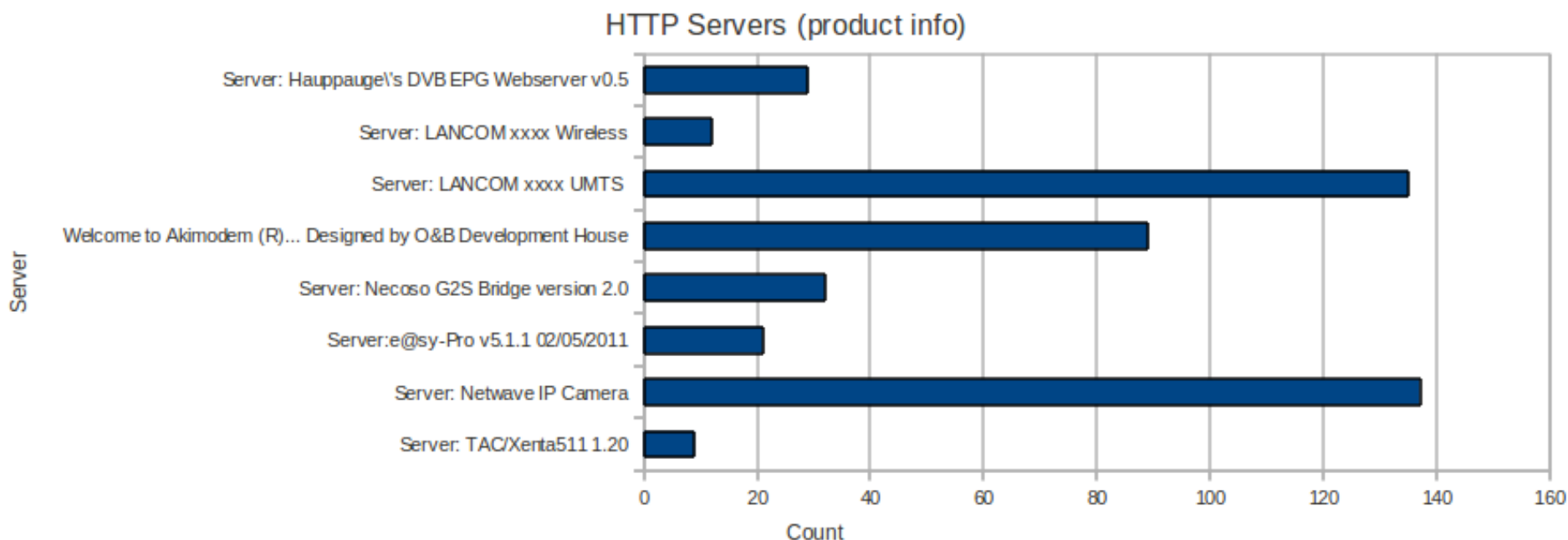
HTTP Banners “Servers”

- Generic “Server Strings”
 - small/minimal/generic HTTP servers (for embedded stuff)



HTTP Banners

- Detailed HTTP Banners
 - We can “determine” the product from the banner



HTTP Banner Statistics

- HTTP/1.0 200 OK\r\nServer: TAC/Xenta511 1.20
- Device: TAC Xenta511
- Application: building automation
- Networks: Russia,
- Devices: 8
- IP ranges: static and dynamic



http://www.tac.com/data/internal/data/05/00/1169146940063/xenta511_controllerviainternet.pdf

GPS Tracking Devices

- Track stuff
 - cars, delivery trucks, individuals, valuable items, ...
- Found many different systems...
 - Earlier, FTP Banner “DigiCore SOLO”
- Here is more ...

Unknown Tracking Device

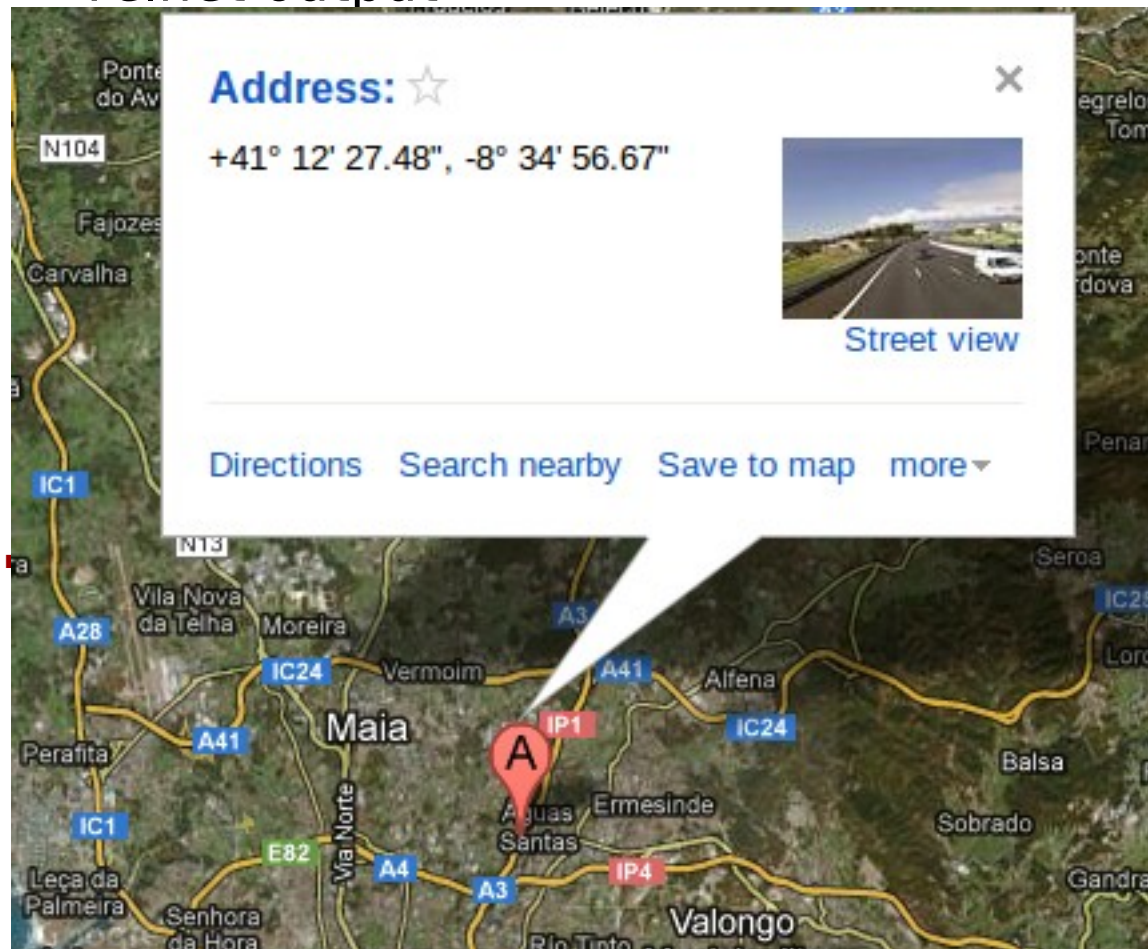
- Telnet output

```
RSI|353446030132219|2012-02-10:11:57:34|7000|009&N41.20213&|\r\n
RSI|358825031004961|2012-02-10:11:57:34|7000|009&N41.20213&|\r\n
RSI|353446030131690|2012-02-10:11:57:34|7000|009&N41.20213&|\r\n
RSI|358825031004912|2012-02-10:11:57:34|7000|009&N41.20213&|\r\n
RSI|000072798125797|2012-02-10:11:57:34|7000|010&W008.58452&|\r\n
RSI|00-10-F3-1B-3E-E5|2012-02-10:11:57:34|7000|010&W008.58452&|\r\n
RSI|353446030132219|2012-02-10:11:57:34|7000|010&W008.58452&|\r\n
RSI|358825031004961|2012-02-10:11:57:34|7000|010&W008.58452&|\r\n
RSI|353446030131690|2012-02-10:11:57:34|7000|010&W008.5845
```

- Only one hit ...

Unknown Tracking Device

- Telnet output



```
|009&N41.20213&|\r\n|009&N41.20213&|\r\n|009&N41.20213&|\r\n|009&N41.20213&|\r\n|010&W008.58452&|\r\n00|010&W008.58452&|\r\n|010&W008.58452&|\r\n|010&W008.58452&|\r\n|010&W008.5845
```

Coordinates match
country of operator

Unknown Tracking Device ... further investigation

- Lets search for “RSI” ... only one more hit...

```
2011/10/05 07:13:08.453 85|ThreadObject.cp{MTU  } 0x0714 Created
thread: 0x07d4 \r\n2011/10/05 07:13:08.453 85|hreadObject.cp{MTU
  } 0x0714 Created thread: 0x0a6c \r\n2011/10/05 07:13:08.453
146|ThreadObject.c{MTU  } 0x0a6c Set ThreadName
'CTcpTraceEndpoint S:xx.xx.xx.xx:xxxx'\r\n2011/10/05
07:13:08.453 146|ThreadObject.c{MTU  } 0x07d4 Set ThreadName
'Tcp Trace Listener thread'\r\nRSI|353446030136186|2011-10-
05:07:13:08|7000|013&0x130
```

- ...but **TcpTraceEndpoint** looks good
 - about 100 hits total
- All IPs seem dynamic
 - Turkey (90% of the hits), Portugal

Tracking Device: C4-D

- Telnet prompt
Welcome on console
- Networks: Portugal, Turkey
- Device: ~ 180
- IP ranges: dynamic
- Security: none!
 - No login/password required

Tracking Device: C4-D (Console)

```
scanner@bloodcough: ~/scan3
File Edit View Terminal Help
Trying [REDACTED]...
Connected to [REDACTED].
Escape character is '^]'.
Welcome on console

Help :
cmd [option1|option2]{string}(number)

Builtins :
cversion      Console version
help          Display help
screen [(X)]  Change to screen X. If no argument, display screens list
color [0|1]   Enable/Disable color output
lang [{str}]  Set the console language
reboot [(waitTime)] Reboot
completion    Activate advanced completion
exit          Quit

Basics :
lwire         Display lwire information
iostate       Display input/output state
modem         Display modem state
gpspos        Retrieve last GPS position
list [all|{module}][dl] List available modules.
               [all] List all available modules parameters.
               [module] List available module parameters.
               [dl] Download result.
g {module} {parameter} [(index)] Get module parameter value
s {module} {parameter} [(index)] {value} Set module parameter value
listdb        List available DB parameters
gdb {name}    Get a DB parameter
sdb {name} {value} Set a DB parameter
log [print|debug|warn|error|{str}] Display last logs
logdump [print|debug|warn|error|{str}] Display all logs
configure     Upload a new conf file

Basics[C4D]> 
```

Tracking Device C4-D

[Home](#)[Dreevo 3](#)[Morpheus](#)[H4](#)[C4-Evo](#)[C4-D](#)[CloudConnect](#)[Features](#)[Download](#)[FAQ](#)

C4-D

Introduction

Installation

[Install the C4-D](#)[Power consumption](#)

First use

[First use of the C4-D](#)

Advanced features

[Use the 1wire](#)[Use the I/O](#)[Use the CAN feature](#)[Flashing guide](#)

Download

[Packages](#)

Introduction



This page has been updated on the 11 April 2010.

Specifications

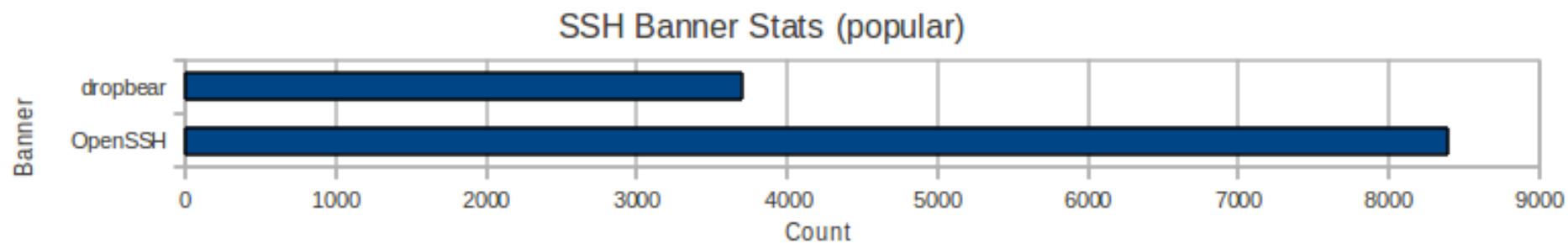
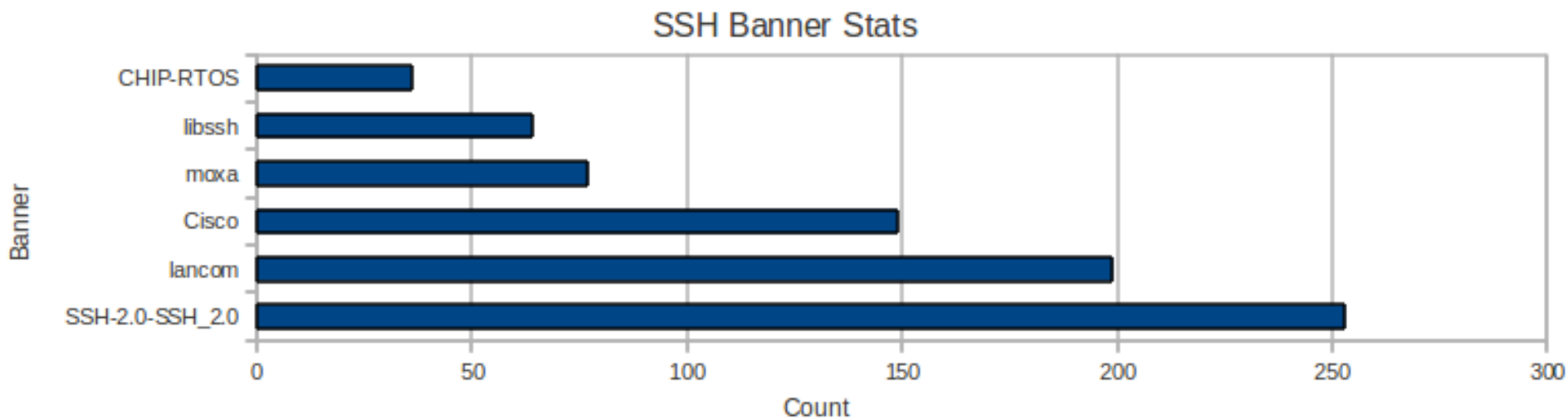
Performance	
Processor	ARM 9 – 210 MHz
Ram	32 MB

In 1
Sp
De

GPS Tracking Devices: conclusions

- Really common application
 - No surprise to find these
- Security
 - Not really a thing here
 - Often no access restrictions
- Detailed study would be interesting
 - Find devices at “interesting” locations

SSH Banners



Moxa - OnCell

- Devices: ~70
- Networks: Turkey, Portugal, France, Hungary, Germany, Russia
- Application: power system automation
- Services
 - SSH, Telnet, FTP
- Security
 - sometimes root shell w/o login/password



Moxa - OnCell

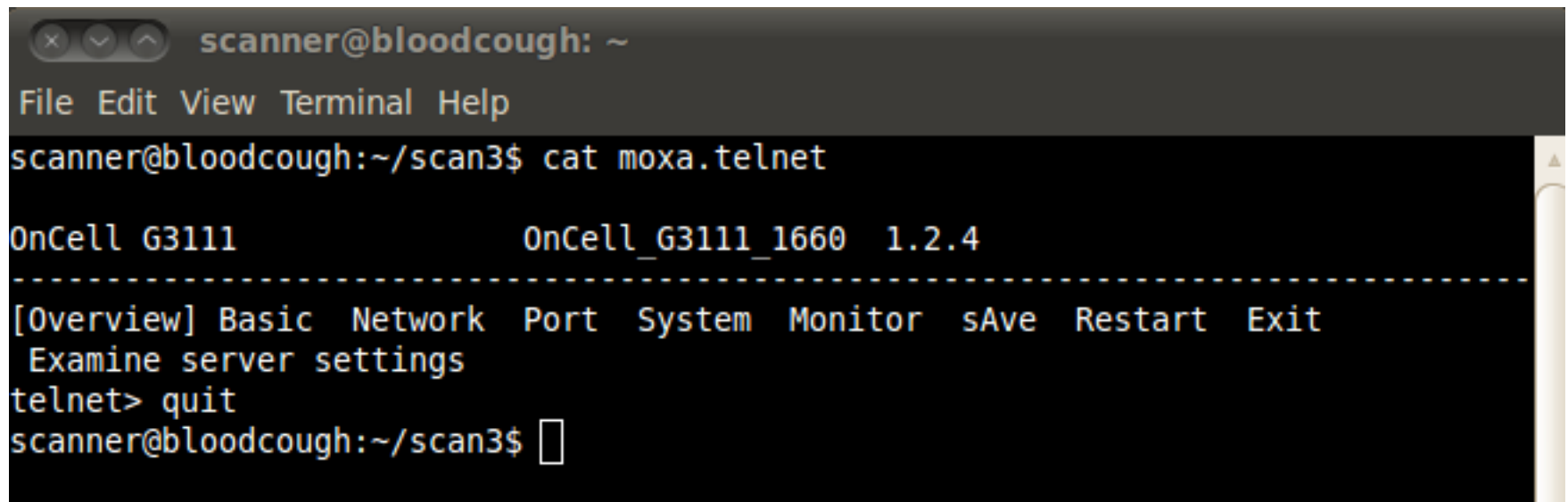
- Linux Moxa 2.6.9-uc0 #142 Fri Jun 19 15:13:00 CST
2009 armv4tl unknown

- Banners:

```
OnCell G3150-HSDPA\r\nConsole terminal type (1: ansi/vt100  
OnCell G3111\r\nConsole terminal type (1: ansi/vt100  
OnCell G3110_V2\r\nConsole terminal type (1: ansi/vt100  
OnCell G3151\r\nConsole terminal type (1: ansi/vt100
```

Moxa - OnCell

- Telnet



```
scanner@bloodcough: ~  
File Edit View Terminal Help  
scanner@bloodcough:~/scan3$ cat moxa.telnet  
  
OnCell G3111                OnCell_G3111_1660  1.2.4  
-----  
[Overview] Basic Network Port System Monitor sAve Restart Exit  
Examine server settings  
telnet> quit  
scanner@bloodcough:~/scan3$
```

Moxa - OnCell



MY MOXA | Partner Zone | International Sites | [Contact Moxa](#)

Search

About Moxa | Products | Applications | Knowledge Center | Support | News & Events | Where to Buy

Location: Home >> News & Events >> Press Releases

Hi! Please [sign in](#)

OnCell G3111/G3151 High Performance Cellular IP Modem for Power System Automation

 E-Mail this Page

 Print this Page

Taipei, Taiwan, Oct. 16, 2009—Moxa is proud to introduce the 1-port RS-232 OnCell G3111 and the RS-232/422/485 OnCell G3151, which are intelligent GSM/GPRS industrial cellular IP modems. These new products empower system integrators with a versatile, cost-effective, and robust cellular solution for power system automation applications, such as Automatic Meter Reading (AMR). The features of the OnCell G3111/G3151 have been designed to deliver high reliability, flexibility, and value while helping system integrators keep operational costs low.

Both the OnCell G3111 and G3151 come with a full TCP/IP architecture, enabling simple transparent cellular connections to legacy devices over TCP/IP networks. The OnCell G3111/G3151 not only provides multiple operation modes, including TCP server, TCP client, and UDP, but also offers the flexibility of three types of GSM/GPRS connection modes: Always ON, Inactivity Timeout, and Remote Host Recovered.

Many cellular ISPs only provide private IPs for their customers, and this IP address can change frequently. This is a substantial system management hurdle as the connection between the host and your device is broken unless the IP address is reconfigured in the cellular IP modem. The OnCell Central Manager software included with the G3111 and G3151 greatly simplifies system management by solving this private IP issue. As long as the control center is connected to the Internet, it can connect to remote metering devices; remote devices configured with a private IP address such as AMR meters can access resources on the Internet, and can be managed or accessed directly on a private network or over the Web.



News & Events

[Press Releases](#)

[Events](#)

[Newsletters](#)

[RSS](#)

Arctic Viola

- `uClinux ViolaArctic 2.4.19-uc1 #356 Mon Nov 13 14:59:46 EET 2006 m68knommu unknown`
- Security
 - root w/o password
- Networks: Germany
- Devices: 3
- Application: M2M router/gateway



<http://www.violasystems.com>

3G “Professional” Routers

- LANCOM

- Models: 3550, 1780, 3850, 1751
- Networks: Germany, Belgium, Spain
- Devices: ~200

- Telnet

- LANCOM 3850 UMTS\r\n| Ver. 7.70.0100Rel /
18.08.2009\r\n| SN. 171731800xxx



Smart meters

Smart meter

From Wikipedia, the free encyclopedia

A **smart meter** is usually an [electrical meter](#) that records consumption of [electric energy](#) in intervals of an hour or less and [communicates that information](#) at least daily back to the [utility](#) for monitoring and billing purposes.^[7] Smart meters enable two-way communication between the meter and the central system. Unlike home energy monitors, smart meters can gather data for remote reporting. Such an advanced metering infrastructure (AMI) differs from traditional [automatic meter reading](#) (AMR) in that it enables two-way communications with the meter.

- Found just a few devices on networks in
 - Germany
 - 6 devices, dynamic IPs
 - Turkey
 - 3 devices, static IPs


Smart Meter (Dr. Neuhaus)

- Devices: DNT8166 and DNT8172
- Run Linux
- Telnet prompts
DNT8166 login:
DNT8172 login:
- Security
 - SSH root w/o login/password



http://www.neuhaus.de/Produkte/Smart_Metering/ZDUE-GPRS-MUC.php

Smart Meter (ENDA)

- Actually is an Ethernet device
 - Guess: hooked up to some GPRS M2M gateway
 - Telnet prompt
 - Welcome to ENDA Administration Terminal
 - Security
 - Admin password is: 1234
- 
- A small white Ethernet device, possibly a switch or a small router, with a green Ethernet port and a green terminal block. The device is labeled "Ethernet" and "RJ45". It has a small green LED indicator. The device is connected to a green Ethernet cable.



<http://www.enda.com.tr/ENG/Products/Default.aspx?UrunGrupID=39>

NEU SECLAB

Smart Meter (ENDA)

```
scanner@bloodcough: ~/scan3
File Edit View Terminal Help
telnet> quit
Connection closed.
scanner@bloodcough:~/scan3$ tsocks telnet [REDACTED]
Trying [REDACTED]...
Connected to [REDACTED]
Escape character is '^]'.
Welcome to ENDA Administration Terminal
Password: 1234
Password accepted
> help
Available commands: read, write, and, or, run, stop, help, info, program, passwd, netstat, uptime, reboot, readplc, wr
iteplc, readplcm, upload, time, mac, settime, plcmemrst, calib, ifconfig, top, label, model, test
Type 'help commandname' for further information.
> info
Compiled with gcc
Revision: 270
System clock: 50000000 hertz
Systick period : 50000
Systick counter: 14827
Config base : 0x0001f800
Program0 base: 0x0000e800
Program1 base: 0x0000e800
Program size: 58 kb
Program bank to boot: 0x0000e800
VCC: 857
> ifconfig
IP: 0x6401a8c0 Netmask: 0x00ffffff Gateway: 0x0101a8c0 DNS: 0x08080808
> shell
Unknown command.
Type 'help' for a list of commands.
> 
```



Smart Meters: conclusions

- Most likely test installations
 - Lets really hope this are not production units
 - Small number of units
- Full Linux OS system makes these interesting
 - Smart meter botnet?
- Smart meters are just being deployed
 - We will see a lot more of these in the near future!

WIRMA

- `Linux wirma000245 2.6.13.2-1.13 #501 Mon Apr 28 09:08:00 CEST 2008 armv4tl unknown`
- Application
 - General purpose M2M platform
 - GPS tracking, telemetry,
- Security
 - root w/o password on 41 devices
- Networks: France



<http://www.kerlink.com/rubrique.php5?SiteID=1&LangueID=2&RubriqueID=141>

iOS Devices (iPhone + iPad)

- Identify by open port 62078 (iphone-sync)
- “Jailbreak” identification → open ports
 - 62078 (iphone-sync) and 22 (SSH)
(need ssh installed of course!)
- Devices: ~500k
 - Jailbroken: 2000

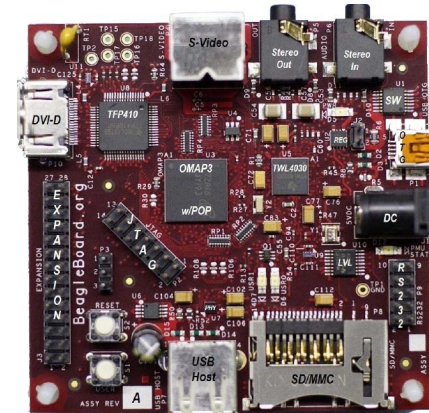


Jailbroken iOS Devices

- Not that many devices in my target search netblocks
 - Netblocks from my RIPE search
- Many more iOS devices in other netblock I scanned
 - Quite a lot with default root password 'alpine'
 - Probably NOT enough for a 2nd worm, but I wouldn't bet!
- Hazard waiting to happen
 - Easy SMS and call fraud
 - Private data: photos, SMS, ...
- If I ever needed a way to send SMS anonymously
 - TOR + jailbroken iPhones!

Strange Finds

- Beagleboards
 - Devices: +20
 - SSH: root w/o password
 - Application: development?
 - Networks: Turkey
- Cameras...



Camera Network (AXIS)

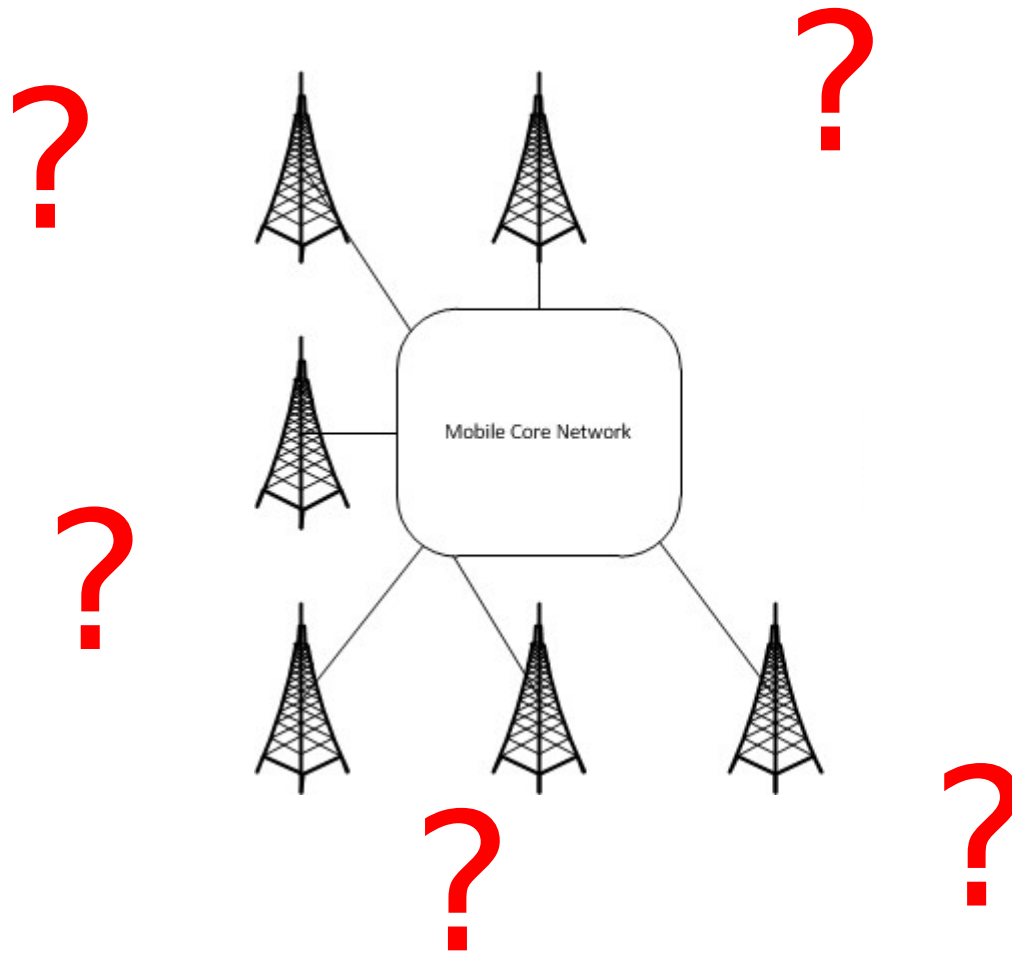
- Overall found plenty of AXIS cameras
- Subnet filled with AXIS stuff is a find :)
 - 38 cams and 1 cam server
 - Network: Turkey



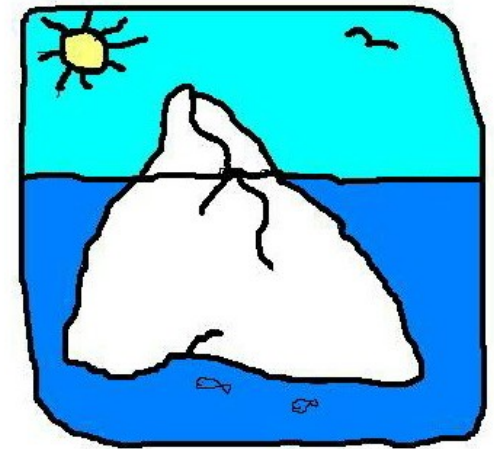
AXIS 213 PTZ

```
x.x.192.29 1328757036 21 0 220 AXIS 214 PTZ Network Camera 4.40
x.x.192.41 1328712454 21 0 220 AXIS 213 PTZ Network Camera 4.35
x.x.192.4 1328893766 21 0 220 AXIS 214 PTZ Network Camera 4.40
x.x.192.44 1328216505 21 0 220 AXIS 213 PTZ Network Camera 4.35
x.x.192.57 1328483890 21 0 220 AXIS 213 PTZ Network Camera 4.35
x.x.192.61 1328931661 21 0 220 AXIS 214 PTZ Network Camera 4.40
x.x.192.63 1328000826 21 0 220 AXIS 213 PTZ Network Camera 4.35
x.x.192.66 1328768193 21 0 220 AXIS 214 PTZ Network Camera 4.40
x.x.192.68 1328736105 21 0 220 AXIS 213 PTZ Network Camera 4.35
x.x.192.69 1328596002 21 0 220 AXIS 241Q Video Server 4.47.2
x.x.192.8 1328387937 21 0 220 AXIS 214 PTZ Network Camera 4.40
```

Devices on Mobile Networks: ?



Devices on Mobile Networks: result!



Device Summary

- Professional
 - GPS Tracking
 - Smart meters
 - Traffic monitoring (as in streets and cars)
 - 3G routers
 - Industrial control stuff
 - Supply chain management stuff (barcode scanner)
 - M2M devices, routers, ...

- Personal
 - iPhones and iPads
 - 3G routers

Why we don't see stuff

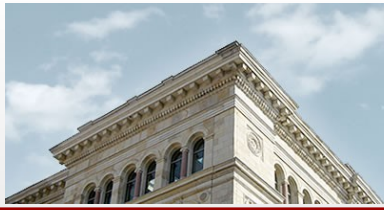
- Operator didn't tag their netblock as “GPRS”
 - Big drawback for this kind of research
- Operator uses IP address not handled by RIPE
- Netblock is used for NAT only
 - Large portions of our scans terminated in HTTP proxies
- Devices don't have open ports
 - Most mobile phones don't run network services
- I made a mistake!

What we Learned

- “Embedded software” that is used in the field
 - Stacks
 - Platforms
 - “single” application
- Check them out for...
 - Features and behavior
 - Default credentials
 - Vulnerabilities
- Probably a lot of really easy targets
 - Pick the hard ones for next research project!

Conclusions

- Mobile networks are full with interesting devices
 - A lot of industrial/enterprise devices
- Public IPs mostly for M2M devices
 - Static address assignment seems rare
- Many different M2M devices
 - Security doesn't seem to be a strong aspect here
 - Root shells on everything!
- Mobile networks and GPRS hardware is a real commodity
 - All devices go mobile → connected to the Internet
 - Big problem if you have to fix Ownd stuff in the field!



Northeastern University

Systems Security Labs

EOF

Thank you! Any Questions ?

twitter: @collinrm
crm[at]ccs.neu.edu
<http://mulliner.org/security/pmon/>