P1 Security
Priority One Security

Attacking GRX

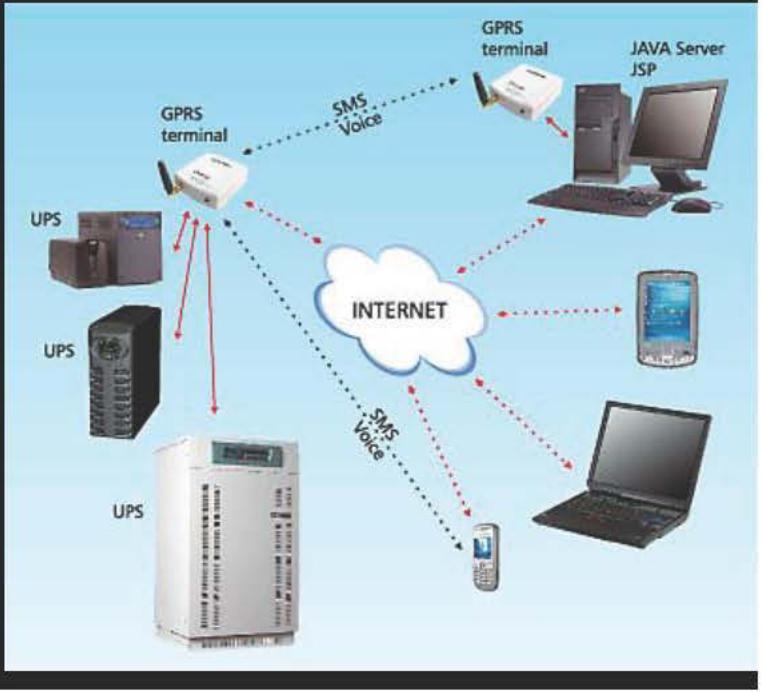
Attacking The GPRS Roaming eXchange (GRX)

Philippe.Langlois@p1sec.com

V1.5

Example: UPS management

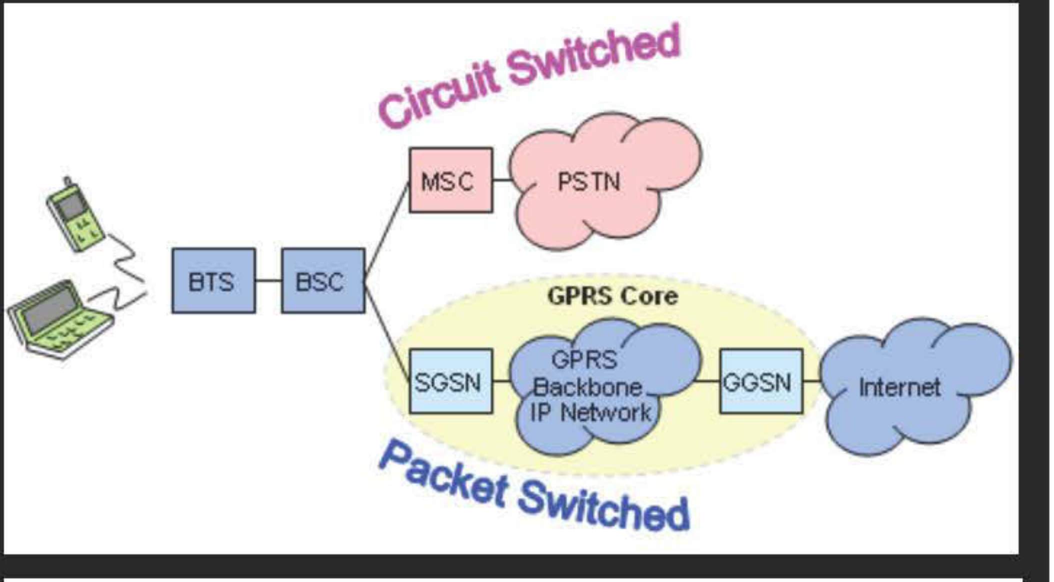
- Not only your Email or BBM
- M2M example
  - management of UPS
- Access the devices…
  - And the management console too
- Usually on corporate network
  - IP bastion or router

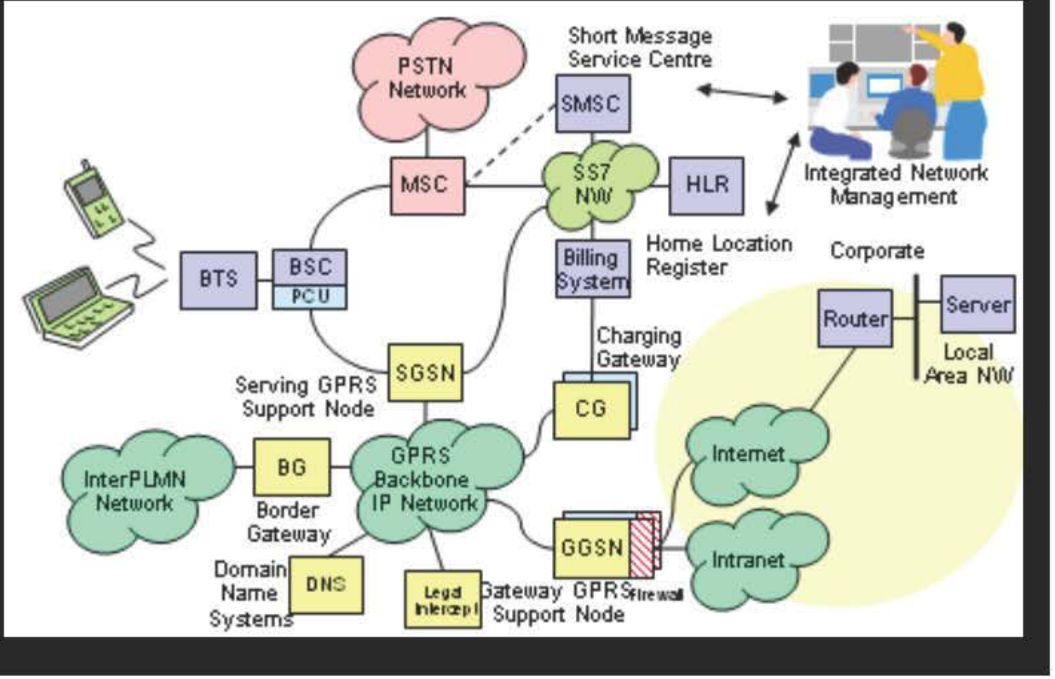


GPRS architecture

P1 Security
Priority One Security

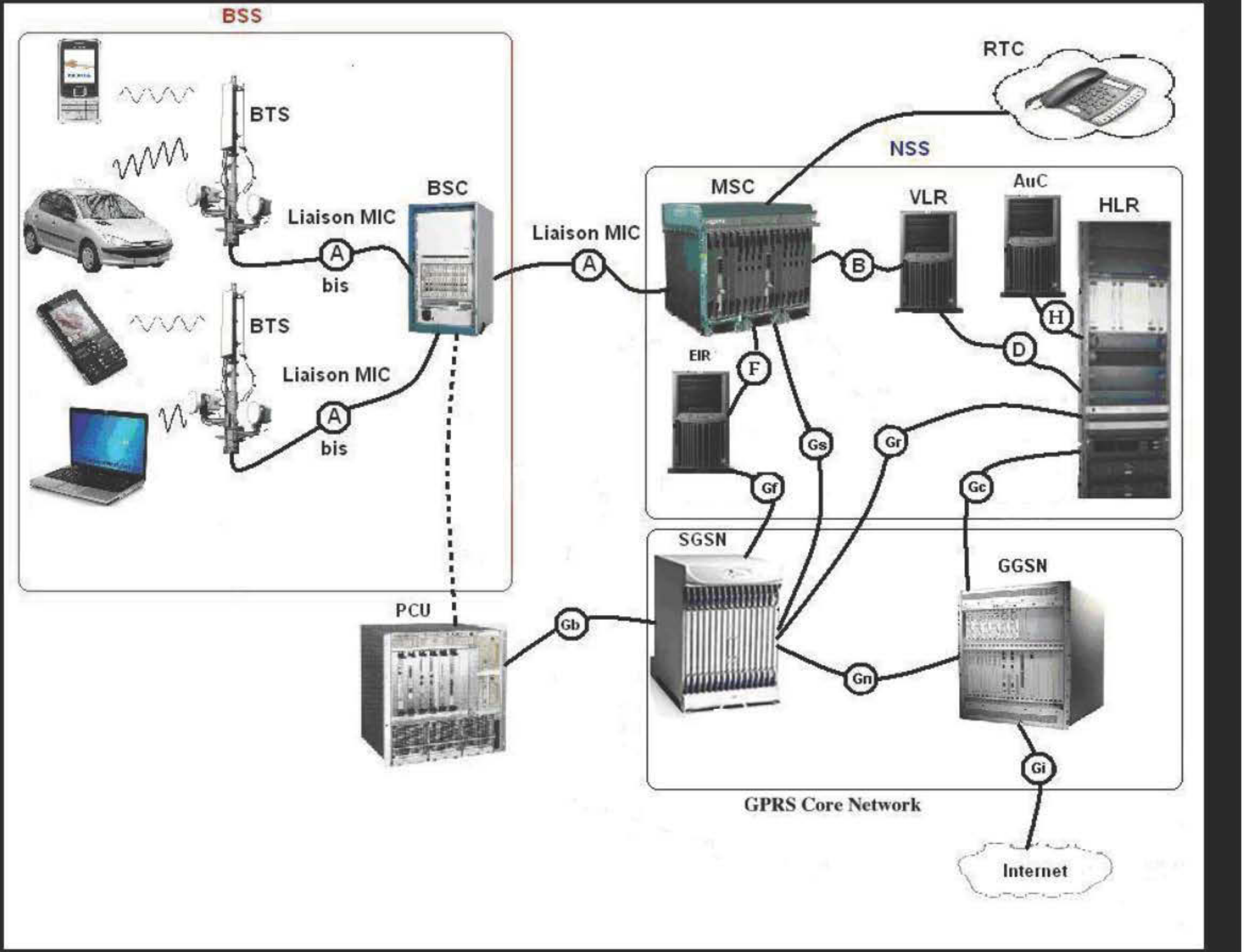
- “PS” Domain in context
- Successor to GSM 9600 baud modem (CSD or HSCSD)
- PDP context = GPRS session
- 2G/3G: SGSN, GGSN
- 4G: MGW, PDGW/PGW
- But also many more machines (LI, DNS, Billing…)
- GPRS backbone = GRX





2G

- IP was new in telco
- Billing is a big issue in GPRS
- Many GGSNs
- SGSN & GGSN to CGF not shown
- Proxies, security filters not shown
- Typical of telco



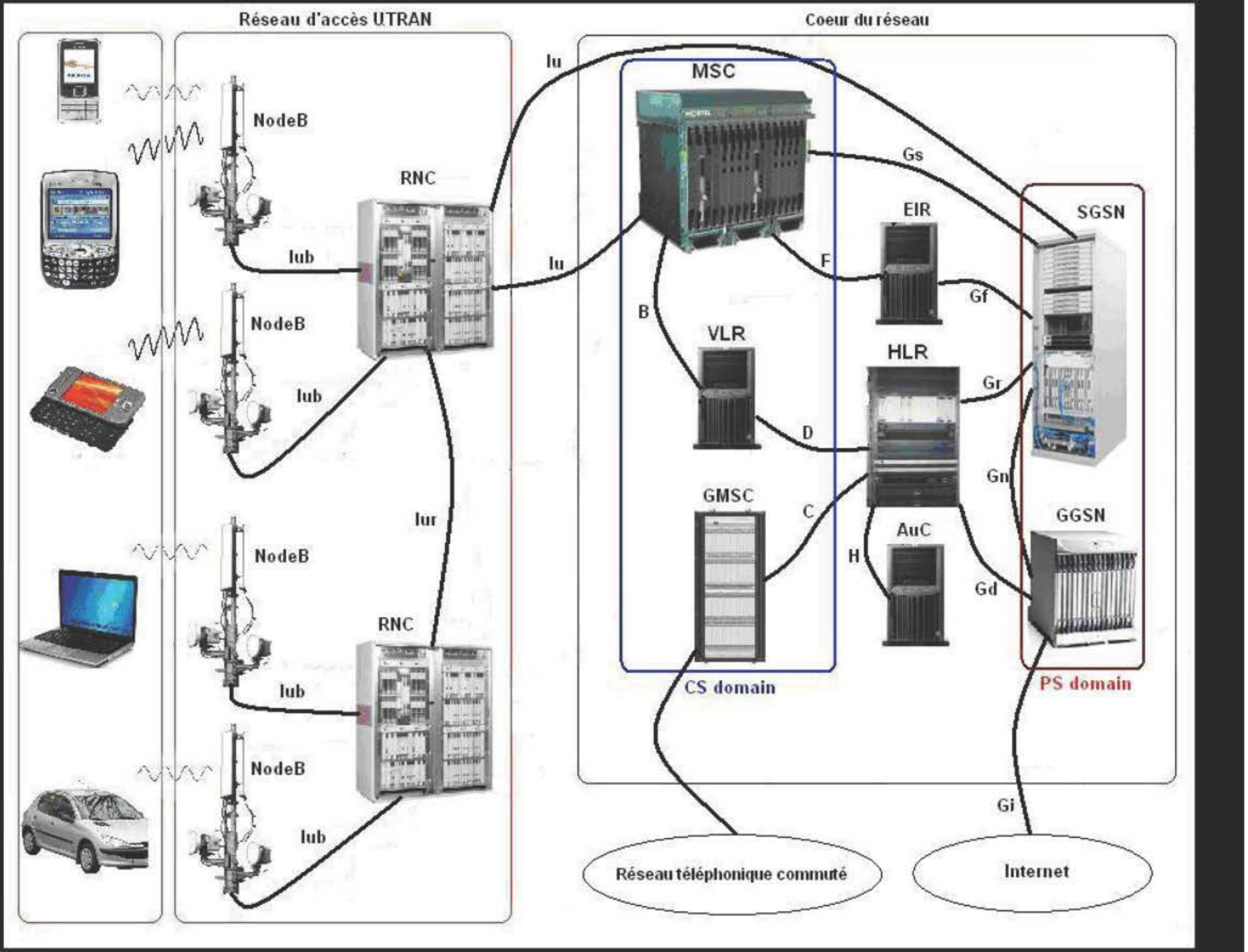
GPRS Radio security in 2G

P1 Security
Priority One Security

- Many GPRS implementations in clear text (Italy, Denmark) !
- OsmocomBB with 4 receptors (and HW mod) http://bb.osmocom.org
- Radio encryption algorithm GEA1 and GEA2 broken
  - By Karsten Nohl, Mate Soos, Sylvain Munaut
  - At CCC Camp 2011 (August)
- Big state (1500 byte MTU), many known point in the equation system
- Linearization, gaussian solving, not even SAT solving

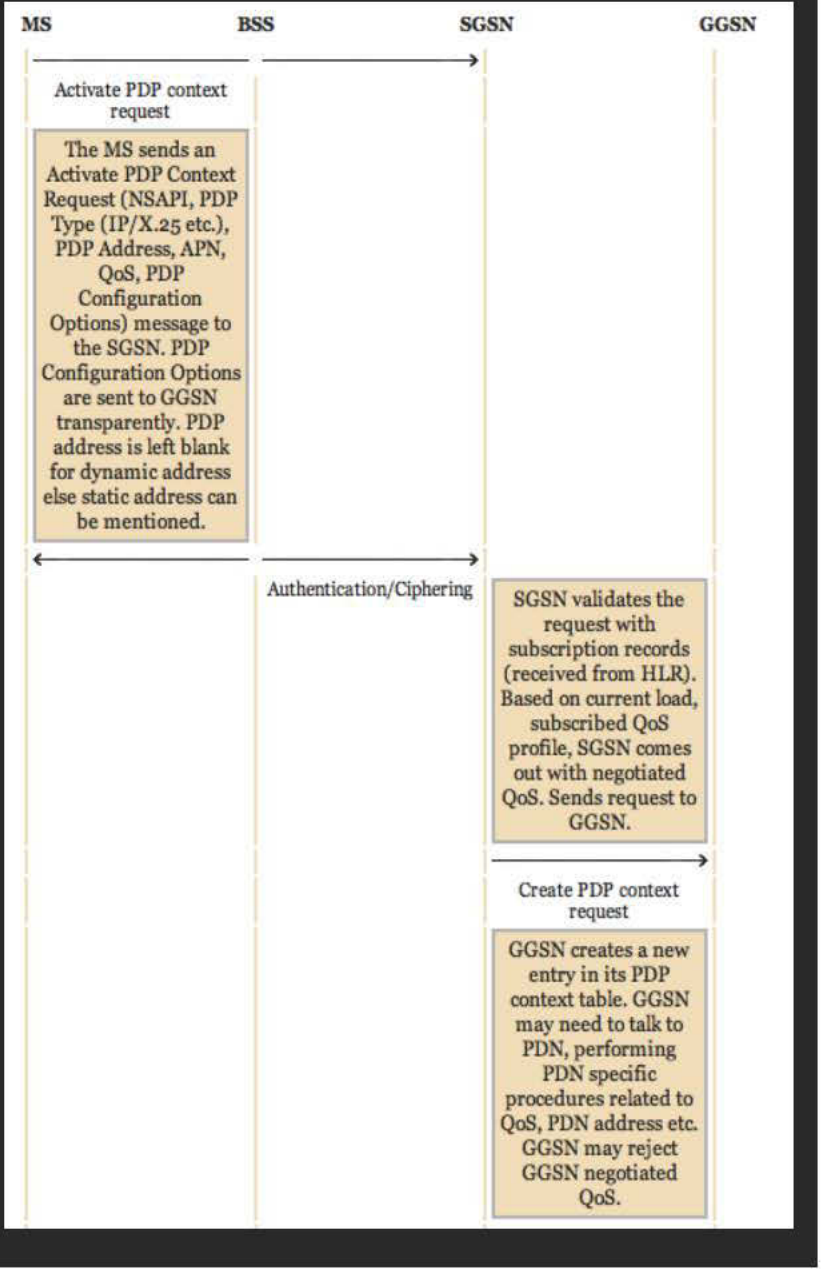
3G

- UMTS
- No open source hw receptor for 3G
- Only "client" access through USB dongles or 3G phones.
- GEA3 (Kasumi KLEN=64 bits) and GEA4 (Kasumi KLEN=128 bits)



GPRS uses cases

- APN
  - internet
  - mms
  - *.corp APNs (banks, gov, ...)
  - M2M APNs
  - special APNs (OAM, billing, ...)
  - Telco internal APNs !



The MS sends an Activate PDP Context Request (NSAPI, PDP Type (IP/X.25 etc.), PDP Address, APN, QoS, PDP Configuration Options) message to the SGSN. PDP Configuration Options are sent to GGSN transparently. PDP address is left blank for dynamic address else static address can be mentioned.

SGSN validates the request with subscription records (received from HLR). Based on current load, subscribed QoS profile, SGSN comes out with negotiated QoS. Sends request to GGSN.

GGSN creates a new entry in its PDP context table. GGSN may need to talk to PDN, performing PDN specific procedures related to QoS, PDN address etc. GGSN may reject GGSN negotiated QoS.

Getting access: The SIM card!

- Obtaining an anonymous SIM card for GPRS hacking
- Varying level of ID checking depending on the country
    - Malaysia checks a lot (mandatory passport or ID)
    - Thailand MNOs give them out for free at airport
    - France doesn't check well anymore (MVNOs arrival)
- MVNOs check less
- Prepaid SIMs with no credit
- SIM roaming gives interesting results (billing, routing errors)

Buy second-hand !

- Second hand hardware
- Guess what's still in it?
  - SIM card!
- Old BB, Cheap PCMCIA cards
- Sometime in laptops
- Company gets rid of previous “mobility” fleet
  - CUG access to network
- 1 out of 3 equipment !

Typical GPRS hacking methods

P1 Security
Priority One Security

- Now you’ve got your SIM then…
  - APN bruteforcing (modem perspective)
  - “In GPRS network” attack of peers / other client devices
  - X25 GPRS network hunting
- Covert channels / unaccounted IP use
- “In GPRS network” attack of server devices
  - GPS tracker M2M gives access to LEA management server !

In the beginning there was the APN

P1 Security
Priority One Security

- Know parameters
  - GPRS APN
  - username + password
  - Dial number
- More difficult parameters
  - MSISDN / IMSI (hard), IN profile
  - USSD setup (for example *136# on Maxis)
- These pipes are clean!

GPRS hacking from the air

- RFC1918 network, reach your peers
- Paris “Velib” M2M network
  - Win based
  - Worm !
  - Contaminated Velib stations over the air
- Enter GPRSdroid (automate!)
- It gets worse with MNOs…

Telco GPRS hacking

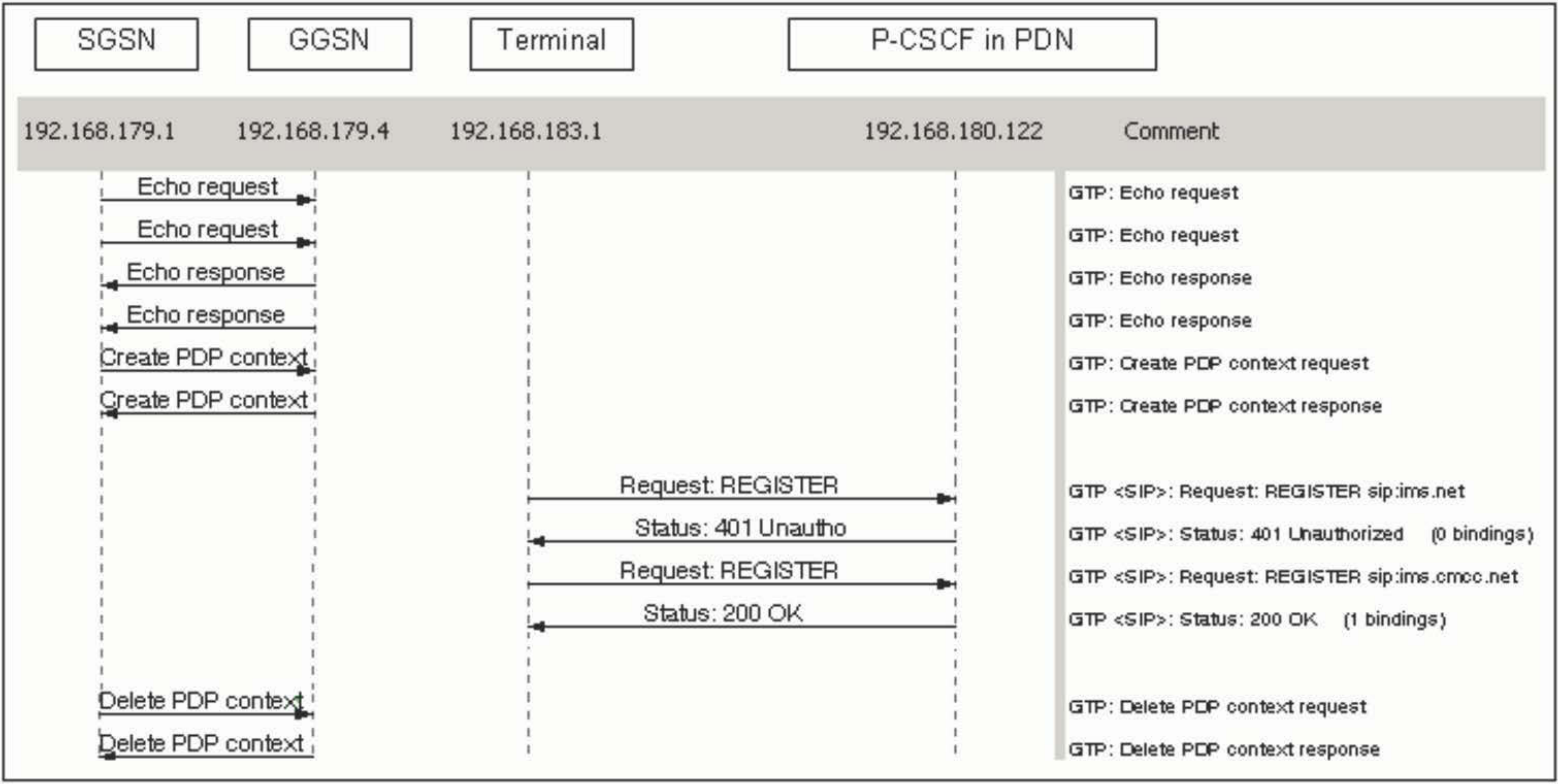
- A tale from Indonesia
  - GPRS normal connection
  - Lack of network segmentation from "Internet"
  - Seize control of NSS / OAM and Routers (MPLS CE and PE)
- APN "mms" or "wap"
  - Access to MMSC and other Core Network infrastructure
  - Ports not firewalled
  - Telecom Operators (MNO) lack proper automated tools to check network segmentation

But GPRS current (recognized) major issue is...

- iodine !
- Bills (CDR) generated on proxy
- Traffic possibly not billed (SGSN or GGSN CDR?)
- Why Telecom operators (MNO) are lagging so bad?
  - Telecom Culture
  - If it does not create costs, it’s not detected by Fraud Management Systems
- Contrast with previous, more severe problems

P1 Security
Priority One Security

Toward IMS / 4G: Full IP



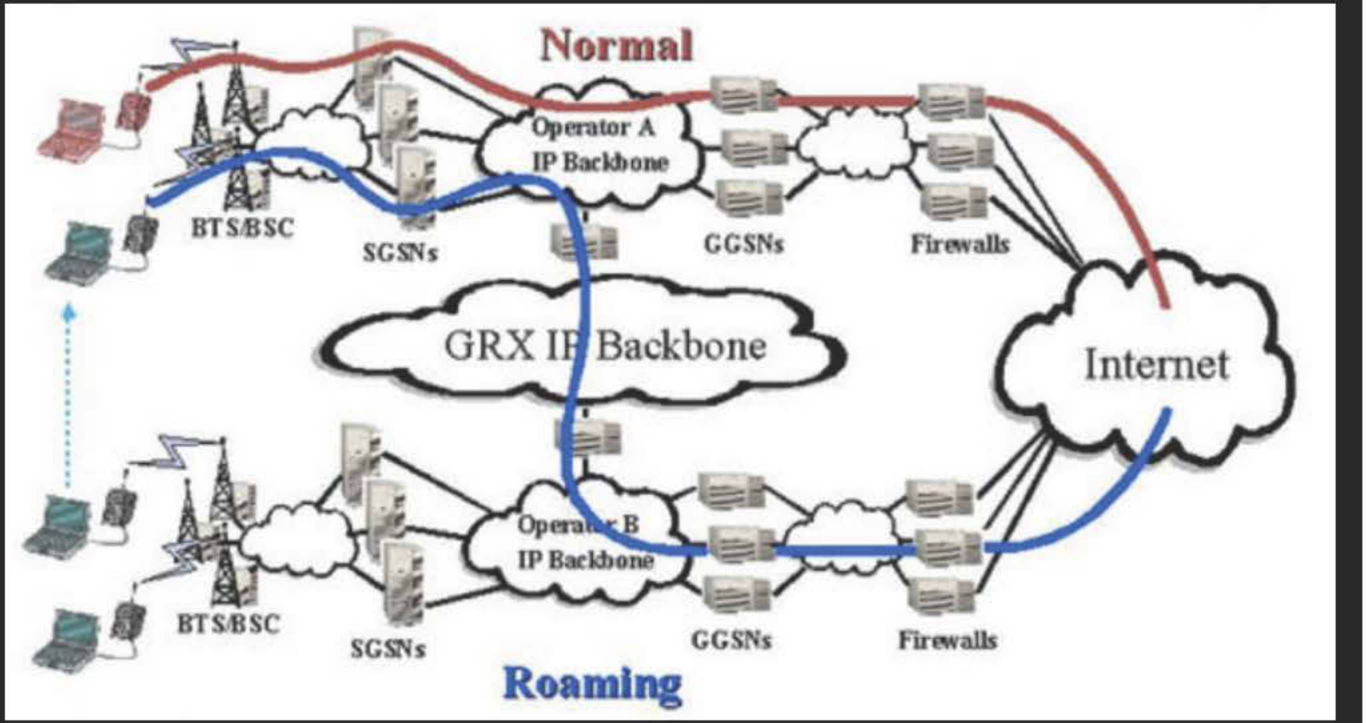
```
GTP: Echo request
GTP: Echo request
GTP: Echo response
GTP: Echo response
GTP: Create PDP context request
GTP: Create PDP context response

GTP <SIP>: Request: REGISTER sip:ims.net
GTP <SIP>: Status: 401 Unauthorized    (0 bindings)
GTP <SIP>: Request: REGISTER sip:ims.cmcc.net
GTP <SIP>: Status: 200 OK    (1 bindings)

GTP: Delete PDP context request
GTP: Delete PDP context response
```

Hint: a) SBC is not far away b) RTP is rarely inspected

P1 Security
Priority One Security

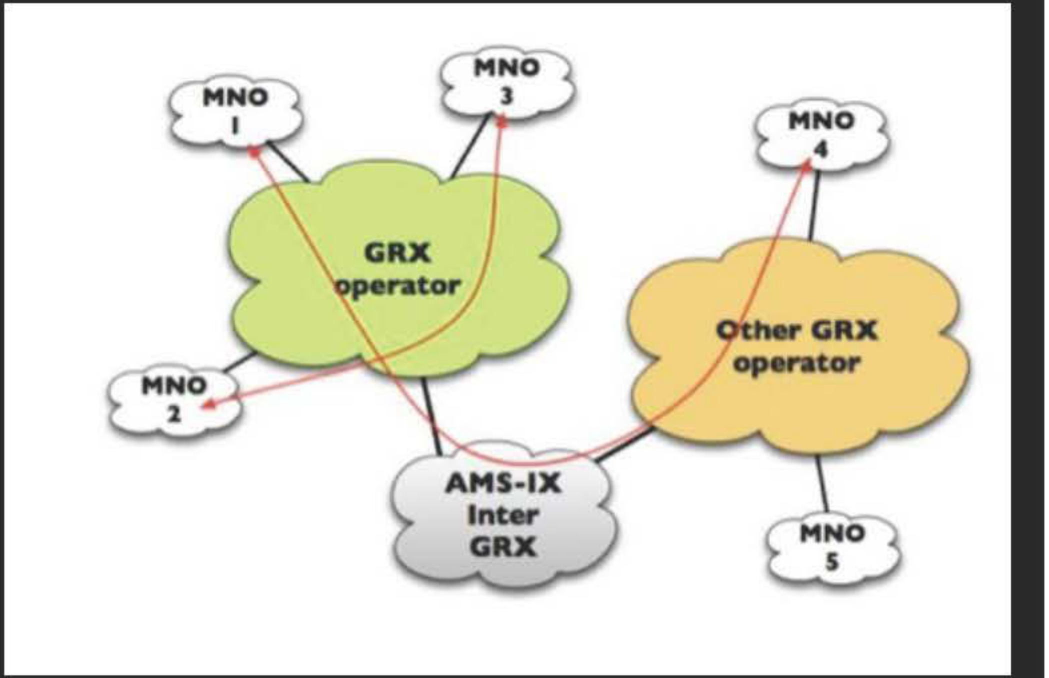
Here comes GRX

- Your national network, from abroad.
- GPRS roaming
- Tunnels (GTP)
- One to one vs. one to many
- From SGSNs to GGSNs



What do Amsterdam and Singapore share?

- NOPE! Not what you're thinking!
- Inter GRX exchanges
- AMS-IX & Singapore Equinix
- No need to go there to access GRX
- Many companies operating on GRX (Comfone, Aicent, Synniverse, …)

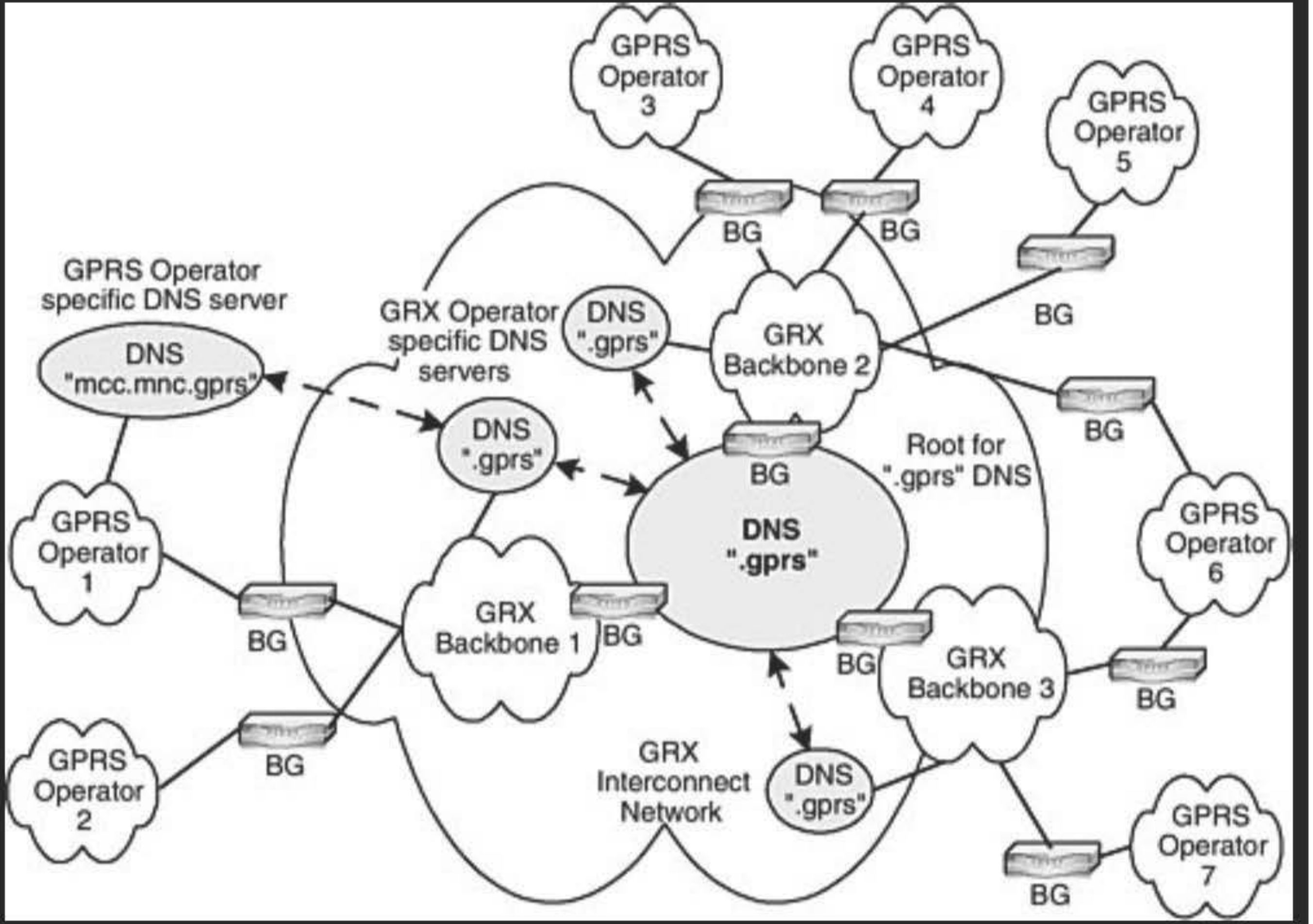


GRX technologies

- GTP
  - GPRS Tunnelling Protocol
- DNS
  - Private DNS
  - `<APN>.mncYYY.mccZZZ.gprs`
  - SFR in France : `internet.010.208.gprs`
  - “Segmented” from the internet… right.

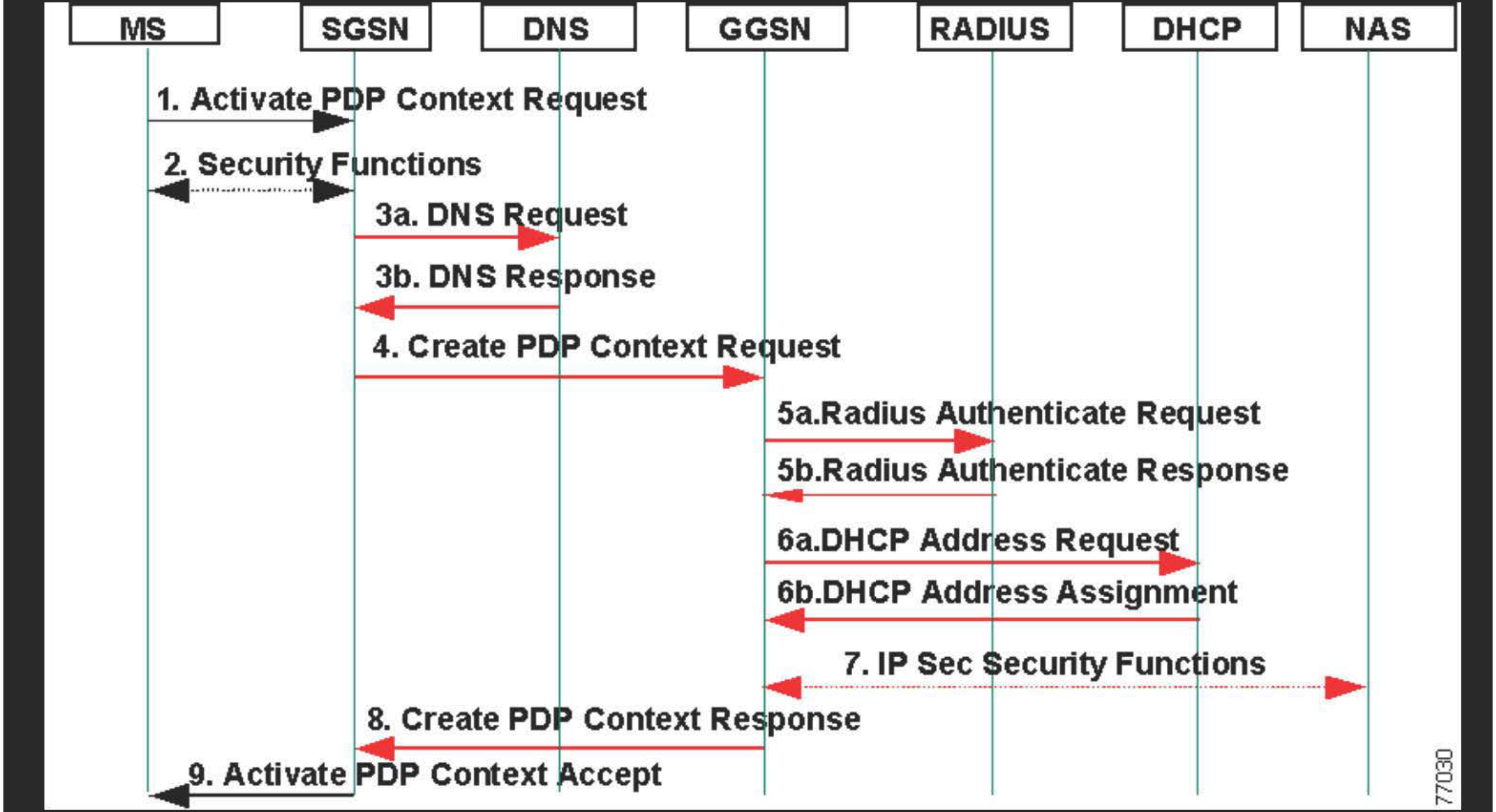
DNS - Do Not Share?

- Internet technology MADE FOR sharing
- Hard to split



GPRS Dialogue

P1 Security
Priority One Security


MS
SGSN
DNS
GGSN
RADIUS
DHCP
NAS
1. Activate PDP Context Request
2. Security Functions
3a. DNS Request
3b. DNS Response
4. Create PDP Context Request
5a.Radius Authenticate Request
5b.Radius Authenticate Response
6a.DHCP Address Request
6b.DHCP Address Assignment
7. IP Sec Security Functions
8. Create PDP Context Response
9. Activate PDP Context Accept
77030

A story of split DNS

- Of course it’s not a valid IANA TLD

```
$ host -t ANY gprs.
Host gprs. not found: 3(NXDOMAIN)
```

- “.gprs” is considered crown jewel, to be protected
    - Direct connectivity to all SGSN and GGSN
    - Big machines, one crash == thousands of disconnected
- Well… let’s try from inside a GPRS session?

And from inside?

- From a GPRS session, most of the time, same thing:

```
$ host -t ANY gprs.
Host gprs. not found: 3(NXDOMAIN)
```

- Some problem happens sometime (APN, IMSI, user/pw, ..)

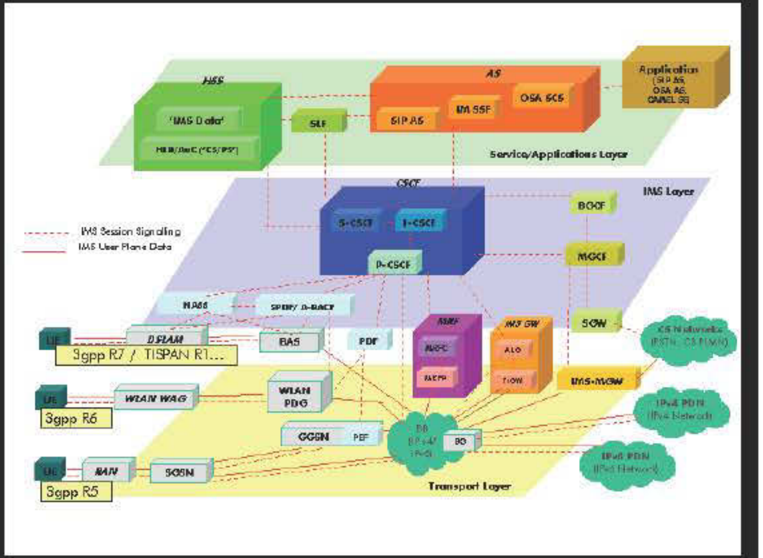
```
$ host -t ANY gprs.
gprs has SOA record dns1.GRXOPERATOR.com. info.GRXOPERATOR.com
gprs has address 10.XX.20.1
gprs name server dns5.GRXOPERATOR.com.
```

- W00t!
- Then the whole hierarchy is accessible
- Because you’re a SGSN!

Triple play, four way

P1 Security
Priority One Security

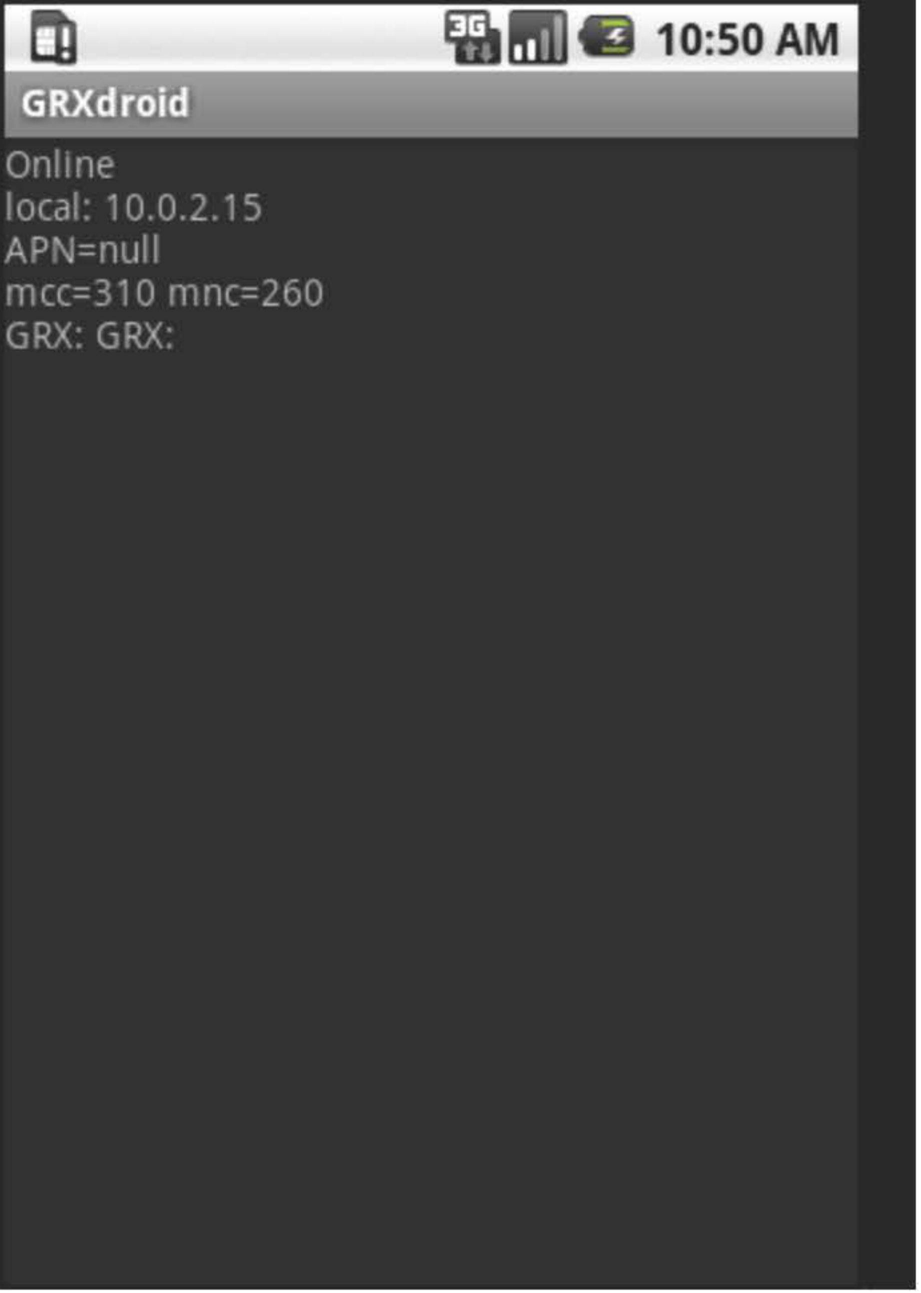
- Access Networks
  - GPRS APNs
  - VoIP network (VLAN and MPLS plane)
  - ADSL / FTTH network / IPTV
  - WLANs ! (recent case, GAN)



- Customer traffic
  - VLANs / MPLS planes everywhere, connecting to so many services
  - DNS resolution
- Everything for the application, Network is considered "necessary evil, make it just work"
  - Management cares only about new services roll out

Enter GRXdroid

- Bruteforce resolving of GPRS DNS (and more)
- Horrible UI for now (want to help? :-) But does the Job
- Soon on the Android market
- Send me an email, I'll send you the APK
- Future
  - APN automation?
  - USSD?



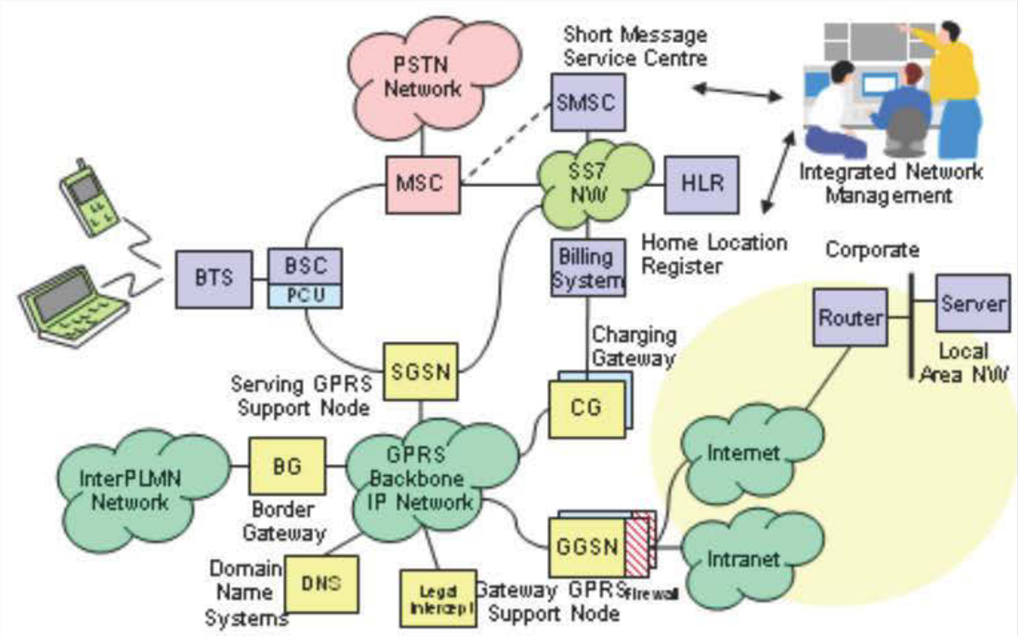
```
Online
local: 10.0.2.15
APN=null
mcc=310 mnc=260
GRX: GRX:
```

Sentinel: When, not if

- Wait, wait, wait, win!
- Here comes the sentinel, a tale of an old finger trick
  - Pentest from the 90s in Thailand
- DNSsentinel
  - Keep trying till it succeeds
- Organization hack – one day, the service will suck
  - And we'll be there

Inside the GRX

- From DNS leaks to route/packets leaks
- Firewalling issues
- You're a SGSN ! GTP to all GGSNs



- SGSN should contact GGSN… filter? Anyone?
- Way too many services exposed
  - From Solaris RPC down to SIGTRAN services (SS7! Wow!)
- MNO says: “Protect? Well, it’s restricted to operators right?”

Evolution of GRX: 3gppnetwork.org

- A bit like ENUM (cf. e164.arpa zone) but for Core Network
- Many different subdomains

APN	<APN name>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.
IMS	ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org.
SGSN	sgsnXXXX.mnc<MNC>.mcc<MCC>.3gppnetwork.org.
LTE EPC	epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.
LTE MME	mmegiXXX.mme.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.

- Used for identities, many RAN / RAT

```
User-Name = "1210012000584533@wlan.mnc001.mcc210.3gppnetwork.org"
```

- Diameter enabled servers (scan for port 3868)

Getting the map

```
$ORIGIN epc.mnc111.mcc222.3gppnetwork.org.
$TTL    1800
@       IN      SOA     ns      root (
                                1       ; Serial
                                3600    ; Refresh
                                30      ; Retry
                                3600    ; Expire
                                600 )   ; Negative Cache TTL

@         IN      NS      ns
ns        IN      A       4.4.4.4
```

Zone transfer powahh

Per server, per protocol

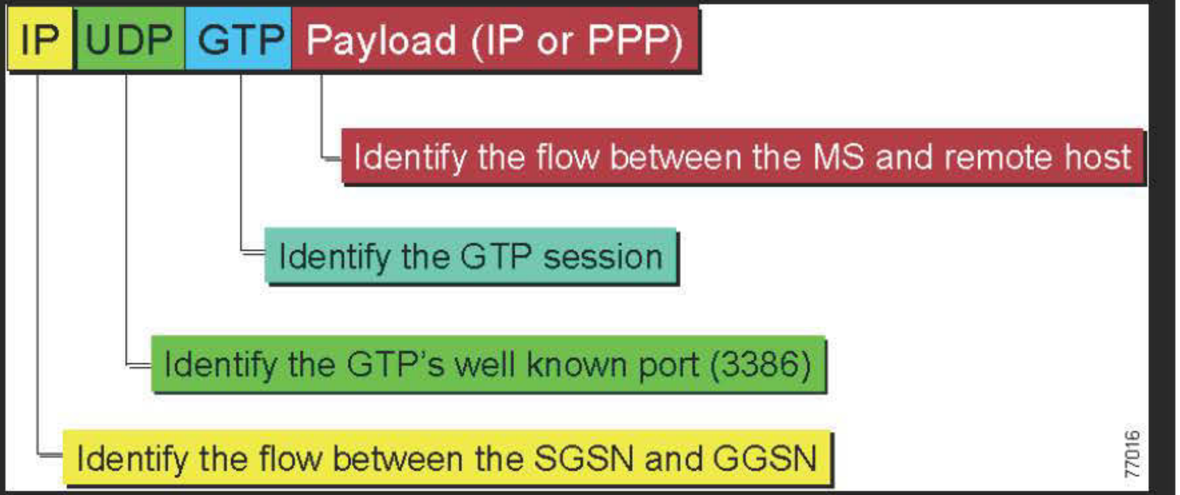
```
testapn1.apn  IN NAPTR 10  10  "a" "x-3gpp-pgw:x-s5-gtp" "" serv.s5.pgw.north
testapn2.apn  IN NAPTR 10  10  "a" "x-3gpp-pgw:x-s5-gtp" "" serv.s5.pgw.south
testapn3.apn  IN NAPTR 10  10  "a" "x-3gpp-pgw:x-s5-gtp" "" serv.s5.pgw.east
testapn4.apn  IN NAPTR 10  10  "a" "x-3gpp-pgw:x-s5-gtp" "" serv.s5.pgw.west
testapn.apn  IN NAPTR 10  10  "s" "x-3gpp-pgw:x-s5-gtp" "" _nodes._pgw
tac-lb01.tac-hb00.tac IN NAPTR 10  10  "s" "x-3gpp-sgw:x-s5-gtp" "" _sgw._north
tac-lb02.tac-hb00.tac IN NAPTR 10  10  "s" "x-3gpp-sgw:x-s5-gtp" "" _sgw._south
tac-lb03.tac-hb00.tac IN NAPTR 10  10  "s" "x-3gpp-sgw:x-s5-gtp" "" _sgw._east
tac-lb04.tac-hb00.tac IN NAPTR 10  10  "s" "x-3gpp-sgw:x-s5-gtp" "" _sgw._west
_nodes._pgw 1800 IN SRV 10 10 2123 serv.s5.pgw.north
[...]
_nodes._pgw 1800 IN SRV 10 10 2123 serv.s5.pgw.west
_sgw._north 1800 IN SRV 10 10 2123 serv.s5.sgw.north
[...]
_sgw._south 1800 IN SRV 20 10 2123 serv.s5.sgw.north
[...]
_sgw._south 1800 IN SRV 20 10 2123 serv.s5.sgw.west
_sgw._east 1800 IN SRV 20 10 2123 serv.s5.sgw.south
_sgw._west 1800 IN SRV 20 10 2123 serv.s5.sgw.north
[...]
_sgw._west 1800 IN SRV 10 10 2123 serv.s5.sgw.west
```

NOW WE HAVE THE MAP, WHAT CAN WE DO?

P1 Security
Priority One Security

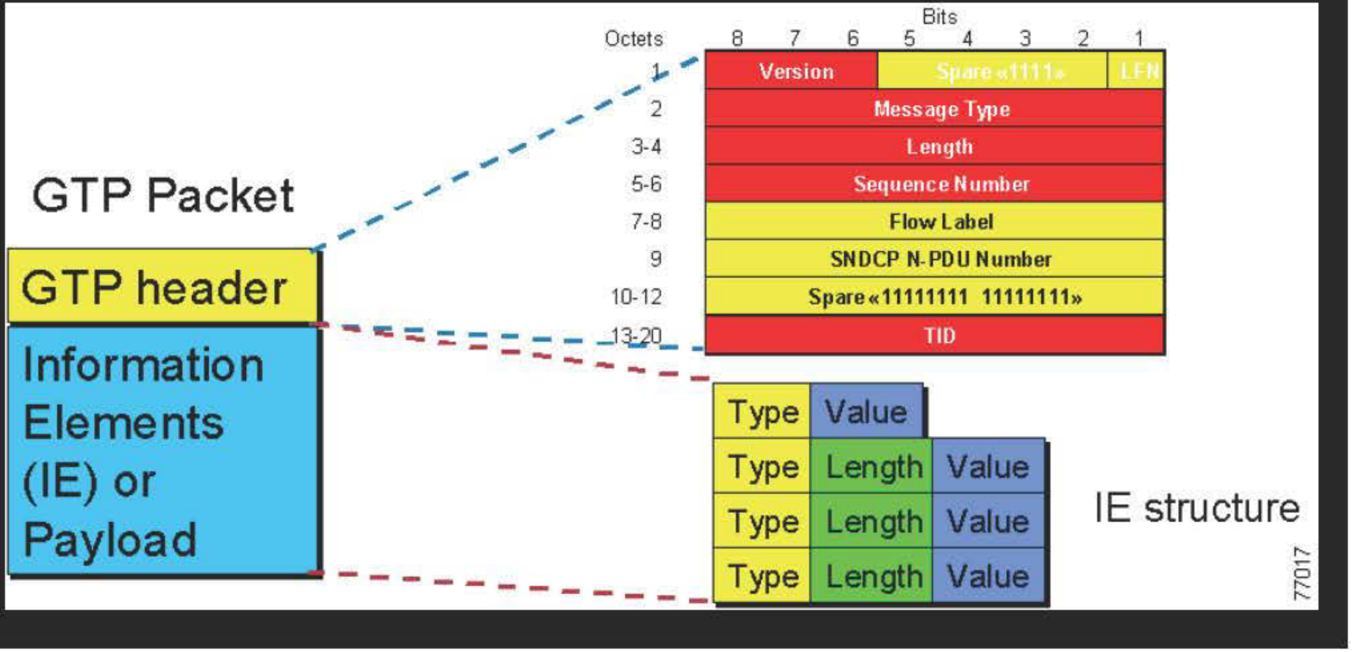
First, GTP basics

- From SGSN (client)
- To GGSN (server)
- Many “commands” possible in Message Type
- Extended a lot
    - GTP v0
    - GTP v1
    - GTP v2



IP | UDP | GTP | Payload (IP or PPP)

- Identify the flow between the MS and remote host
- Identify the GTP session
- Identify the GTP’s well known port (3386)
- Identify the flow between the SGSN and GGSN



GTP Packet

GTP header

Information Elements (IE) or Payload

Bits

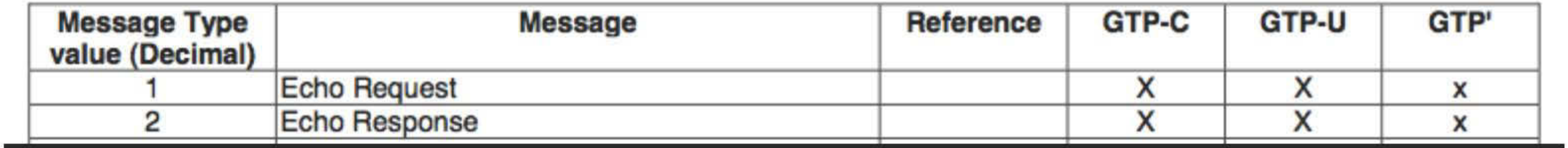
Octets	8	7	6	5	4	3	2	1
1	Version			Spare «1111»				LFN
2	Message Type							
3-4	Length							
5-6	Sequence Number							
7-8	Flow Label							
9	SNDCP N-PDU Number							
10-12	Spare «11111111 11111111»							
13-20	TID							

IE structure

Type	Value	
Type	Length	Value
Type	Length	Value
Type	Length	Value

GTP scanning in GRX

Table 6.1-1: Messages in GTP-U



Message Type value (Decimal)	Message	Reference	GTP-C	GTP-U	GTP'
1	Echo Request		X	X	x
2	Echo Response		X	X	x

- Daniel Mende did it on the Internet, here is
- Way too many open GTP service on the Internet
- Higher ratio on GRX of course
- Easily scanned with GTP Echo Request
- UDP ports 2123, 2152, 3386, Super fast positive scanning

GRX	MNO
✓	✓

GTP in GTP attack

GRX	MNO
✓	✓

- Free Internet surfing
- Access directly the GGSN from another GGSN
- Not supposed to happen… but happens!
- Just use sgsnemu / OpenGGSN to create new interface and route your traffic through it
- Sometime, GTP in GTP is not supported by GGSN… at all
  - Crash and unavailability
- Super fast scanning on GRX: covers the whole planet!

GPRS CUG accesses attacks

GRX	MNO
✓	✓

- CUG = Closed User Group
- At GTP level, you’re either a SGSN or GGSN
- Since you are a SGSN (client), you control
  - APN you’re going to use for the tunnel and
  - MSISDN / IMSI you are impersonating.
- CUG are based on these parameters
- Bank networks, Operator networks, Administration, etc…
- Straight from the Net or from an existing PDP with unfiltered GGSN GTP ports.

GTP Tunnel disconnection DoS attack

GRX	MNO
✓	✓

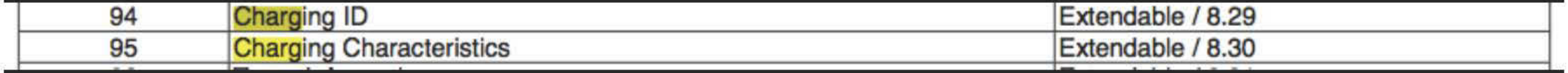
- TEID bruteforce

- Disconnect Message Type (Delete Session Request. Delete PDP, …) + spoof SGSN (really?)

- 2^32 would be a problem… if TEID were not sequential :-)

```
[...]
00 00 17 04    Delete PDP Context: Request Accepted
00 00 17 44    Delete PDP Context: Request Accepted
00 00 17 A1    Delete PDP Context: Request Accepted
00 00 17 BF    Delete PDP Context: Request Accepted
00 00 17 D8    Delete PDP Context: Request Accepted
00 00 17 E8    Delete PDP Context: Request Accepted
[...]
```

Fake charging attacks



94	Charging ID	Extendable / 8.29
95	Charging Characteristics	Extendable / 8.30

GRX	MNO
✓	✓

- Normal GTP 2 traffic
- But with Charging ID and Charging GW (CGF) address specified
- Creates fake CDRs (Call Detail Records or Charging Data Records) for any customer
- Not necessary to get free connection anyway :-)

GRX Subscriber Information Leak

GRX	MNO
✓	✓

- SGSN and GGSN need to communicate with many Network Elements in 3G and 4G networks
- GTP v2 enables many requests to these equipment directly over GTP.
- Think “HLR Request” over UDP
  - No authentication
  - Much more available than an SS7 interconnection :-)
- And you’re GLOBAL ! Thanks GRX. That is, any operator in the world that is connected to any GRX.

Relocation Cancel attack

- Basically tell one SGSN that the user it is serving should come back to you
- User is effectively disconnected (or hangs), no more packets.
- Target user by IMSI
  - But you already got that by the Info leak of previous attack

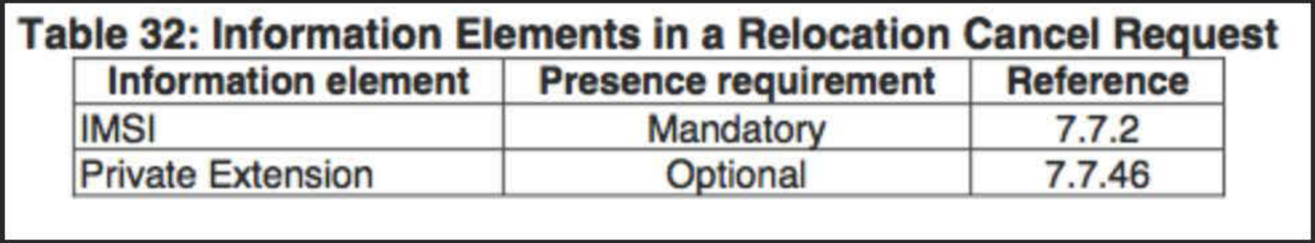


Table 32: Information Elements in a Relocation Cancel Request

Information element	Presence requirement	Reference
IMSI	Mandatory	7.7.2
Private Extension	Optional	7.7.46

GRX	MNO
✓	✓

  - Shoule be Intra-operator, but does work over GRX!

GGSN DoS attack

GRX	MNO
✓	✓

- Another magic packet
- “Oh, I’m a bit congested and about to crash, it would be good for you to relocate to another GGSN to continue your service”
- Result: GGSN deserted, users don’t get any other GGSN, users loose service.
- Per APN impact (i.e. “internet” or “*.corp”)
- Exercise to the ****er

SGSN DoS attack - Ouch

GRX	MNO
✓	✓

- More rare because by their nature (client), SGSN are rarely reachable through IP
- Same attack as previous (Hey, you should really switch to another node, this one is going down)
- Much more impact:
  - Targets a region rather than a network,
  - Repeat on GRX == Disconnect many countries
- Both these are caused by “evolved GTP” i.e. GTP on LTE Advanced networks.

A tube in a tube in a tube

GRX	MNO
✓	✓

- Air -> GTP -> SIGTRAN M3UA SCTP -> SS7
- Oh My Goat, SS7 from the GPRS network
- Script:

  1) Connect to APN

  2) Scan for SCTP M3UA (port 2905)

  3) Establish M3UA connection to say 10.27.1.30

  4) Send SS7 over GPRS ;-) for example, SSP (SubSystem Prohibited) or MSC Reset !!! (disconnect all users from MSC)
- It’s Core Network access from GRX !

As an operator: Protecting your GRX connection

- Filter smartly your GGSN
- Beware of spaghetti tunnel (i.e. tunnel in a tunnel, tunnel chainings, ...)
- Hard, even impossible to predict routing and filtering results (GTP + GRE + MPLS + VLAN + Filtering + Routing + Load Balancing + HA + Multihoming)
  - You need to TEST !
- You are responsible of all entries on GRX through your GRX interconnection!

Go massive

- “A tube in a tube in a tube”
- With many access network technologies
- Very difficult to get right
    - To test
    - To protect
- Automation is key!
- 10 000 hosts to scan, reliably, without causing crash
    - LTE fuzzing story and size/breadth of network

GRX: In the end, the customer

- Banks, Transportation, Smart grid, smart meters
  - Worm on the CUG?
  - Bills of the other side of the planet
- Nice little global network
  - Globally accessible with the right APN and GTP tunneling
- Consequences
  - Operators security maturity, security is not for Internet only
  - India DoT leading the way in telecom regulation: $11M fine, license kill

Questions?

Or join us for the workshop

Send email for the APKs

Conference announcement:

Hackito Ergo Sum, Paris, 12-14 April 2012.

SVC approved!

P1 Security
Priority One Security

THANK YOU!

Philippe.Langlois@p1sec.com

http://www.p1sec.com