GPRS Intercept: Wardriving your country

Karsten Nohl, nohl@srlabs.de
Luca Melette, luca@srlabs.de

SECURITY
RESEARCH
LABS

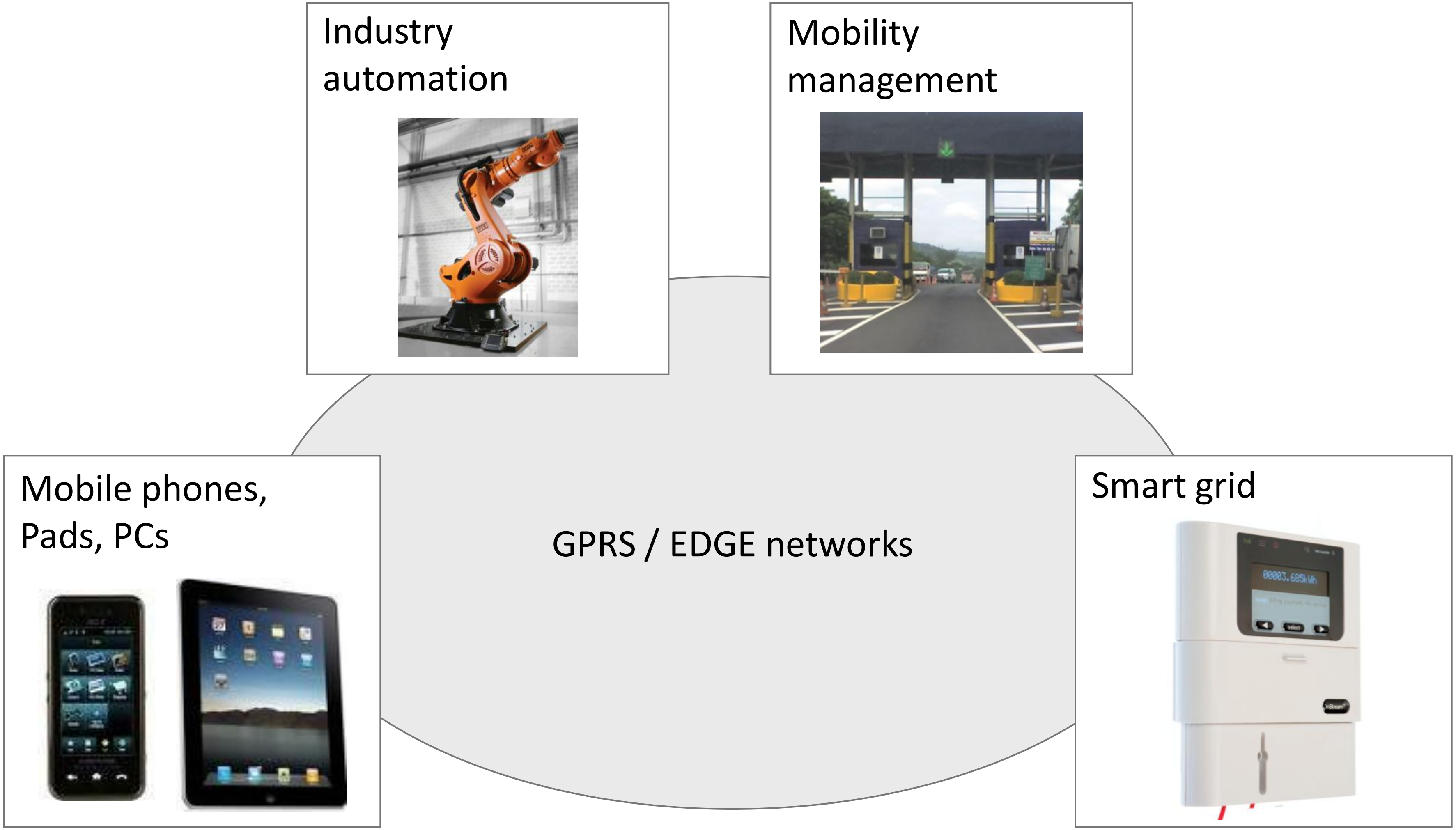
Executive summary – Do not send sensitive data over GPRS

- GPRS/EDGE networks provide the data backbone of smart phones and industry automation systems
- The cryptographic protection of GPRS/EDGE is out-dated and vulnerable to several attacks
  - Lack of mutual authentication allows for ‘fake base stations’ to harvest data
  - Lack of encryption (some countries) allows for passive intercept with EUR10 phone and software released during this talk
  - Weak encryption (remaining countries) enables cryptanalysis,
- Ever more applications are building up on mobile data networks, thereby amplifying the exposed risks instead of mitigating them

Agenda

- **GPRS basics**
- Practical GPRS attacks
- Mitigation measures

GPRS provides the communication backbone for mobile societies



Industry automation

Mobility management

GPRS / EDGE networks

Mobile phones, Pads, PCs

Smart grid

GPRS can encrypt data packets

GPRS/EDGE device

Base station

SGSN backend

Layer 3 – Data packets of typically 1,520 bytes are exchanged with backend. Encryption should prevent intercept over-the-air and on transport links.

Layer 1/2 – GPRS/EDGE share channels with GSM and only differ in the modulation and multiplexing.

GPRS support different encryption levels, but predominantly the weak ones are used

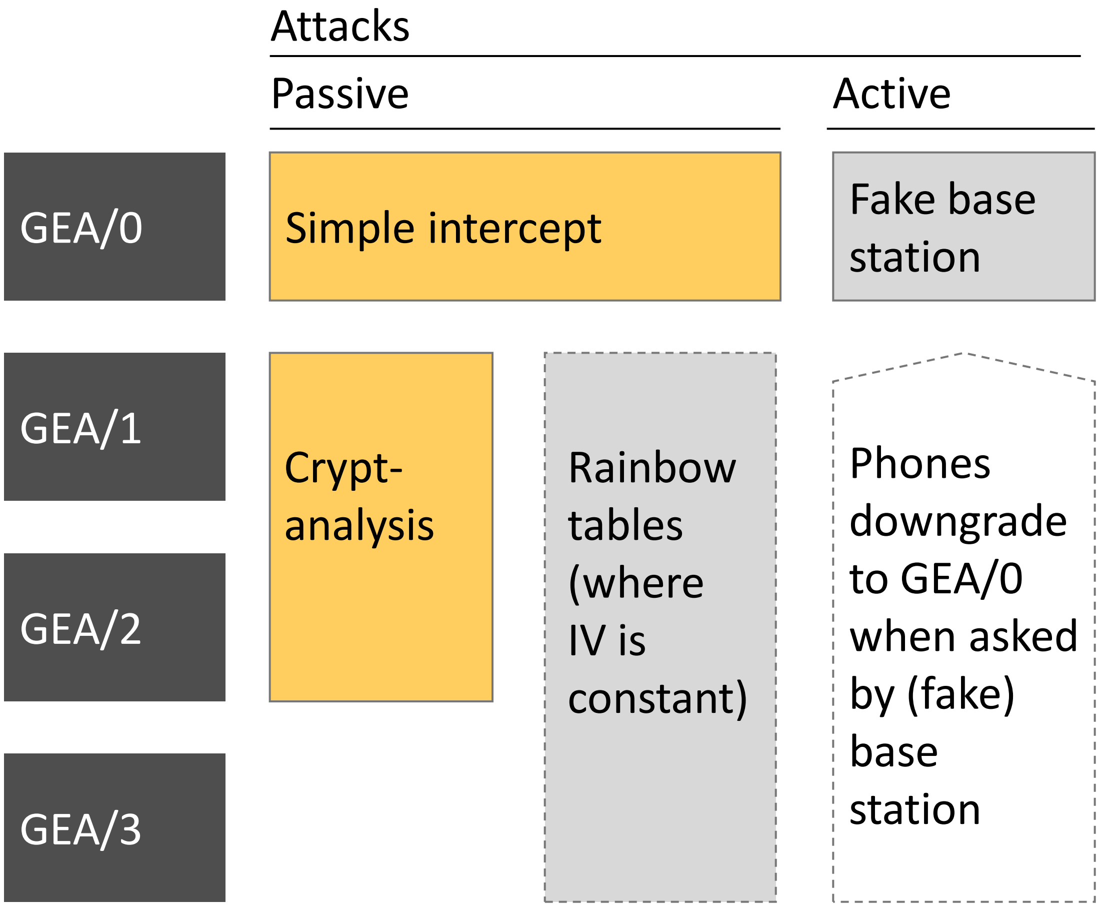
Protection function	Encryption	Key length	Used by
GEA/0	No encryption	N/A	Anybody?
GEA/1	Proprietary stream cipher (96 bit state)	64 bit	Most operators use both GEA/1 and GEA/2
GEA/2	Proprietary stream cipher (125 bit state)	64 bit	
GEA/3	Standard block cipher (128 bit state)	64 bit	Some, mostly newer networks
GEA/4		128 bit	**Nobody**

Agenda

- GPRS basics
- **Practical GPRS attacks**
- Mitigation measures

GPRS networks are valuable to multiple attacks

🟨 Covered in this talks ⬜ Covered in 27C3, 28C3 talks



Attacks

Passive

Active

GEA/0

Simple intercept

Fake base station

GEA/1

GEA/2

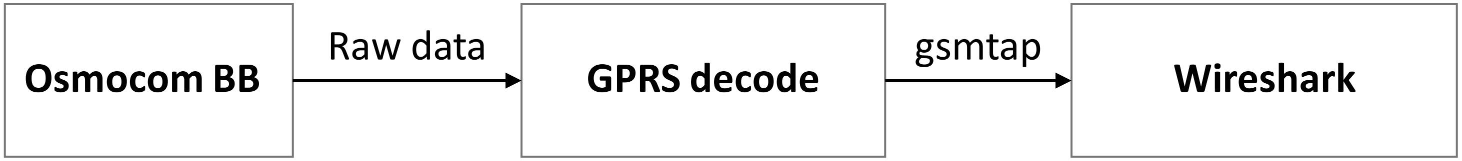
GEA/3

Cryptanalysis

Rainbow tables (where IV is constant)

Phones downgrade to GEA/0 when asked by (fake) base station

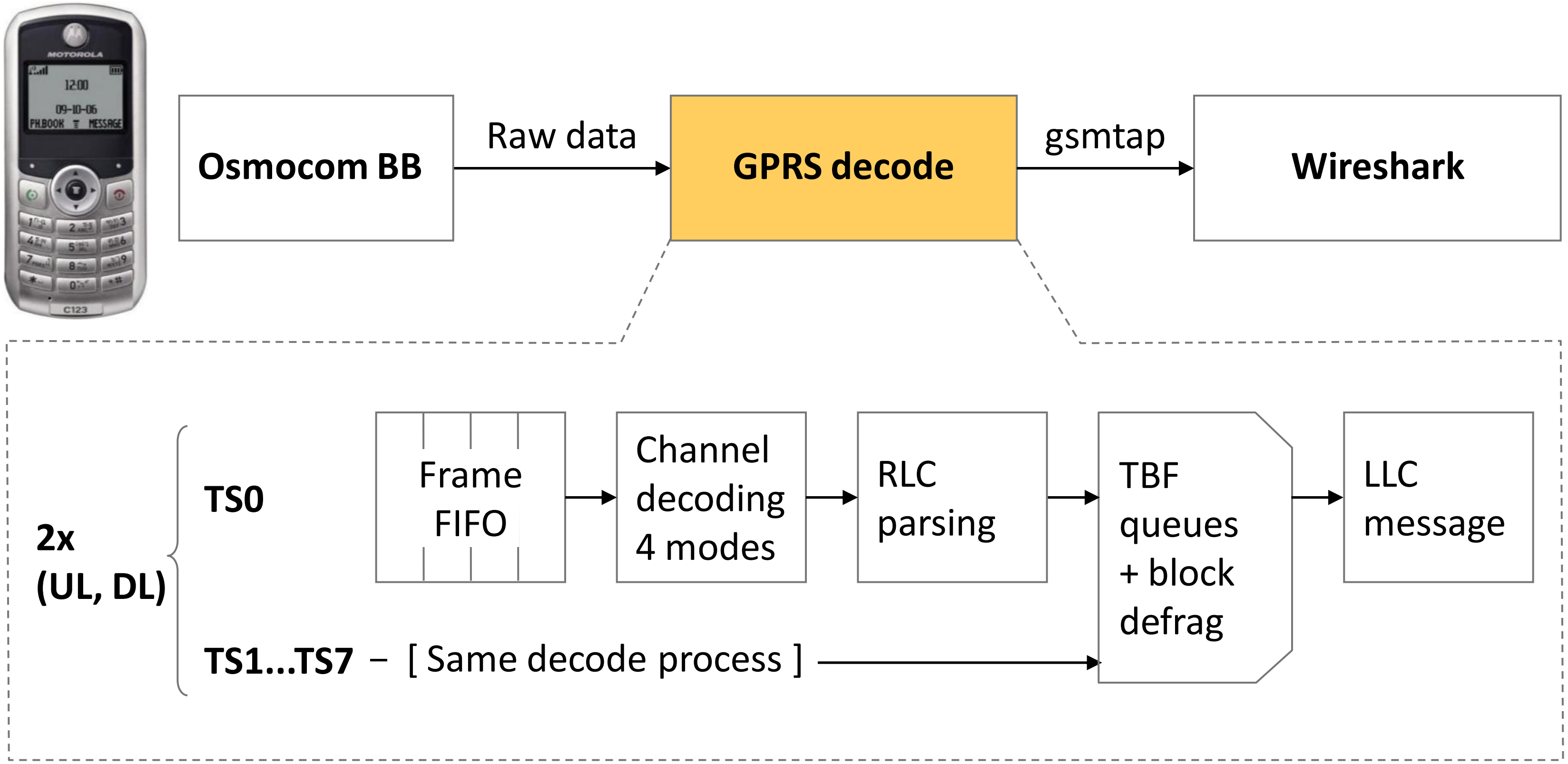
GPRS interception only requires open source tools



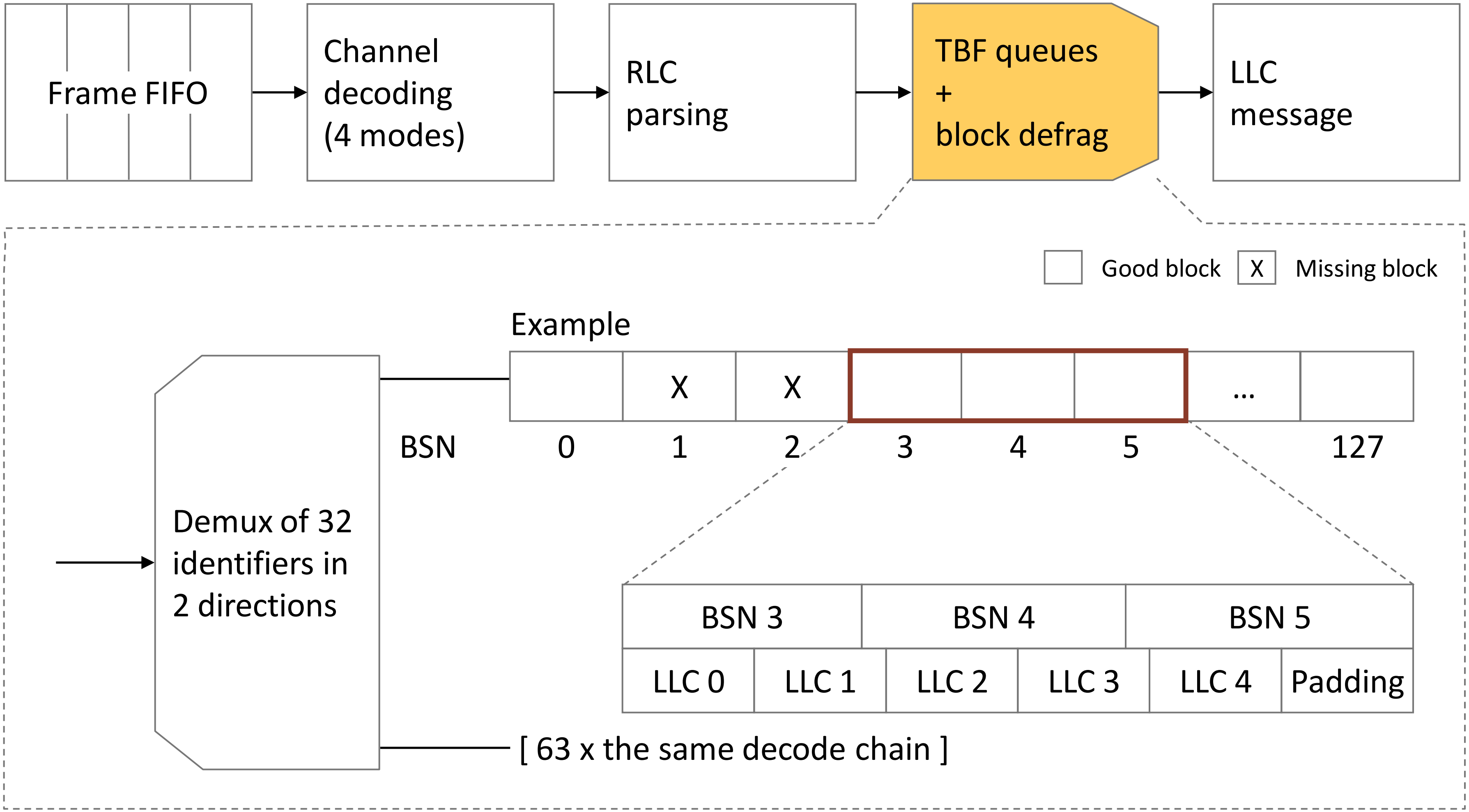
Osmocom BB → Raw data → GPRS decode → gsmtap → Wireshark

Function	**Capture bursts**	**Layer 2 parsing**	**Layer 3 parsing**
Imple-mented Adapta-tions	1. Start with Sylvain's burst_ind branch 2. Pimp the USB cable 3. Add multi-time-slot support	4. Multiplex data from multiple phones 5. Channel decoding 6. RLC parsing (block defrag)	7. LLC parsing (more block defrag) 8. Optional – Native RLC / LLC decoder

GPRS decode consists of 16 decoding chains



GPRS “overcapsulates”



Frame FIFO → Channel decoding (4 modes) → RLC parsing → TBF queues + block defrag → LLC message

□ Good block X Missing block

Example

Demux of 32 identifiers in 2 directions

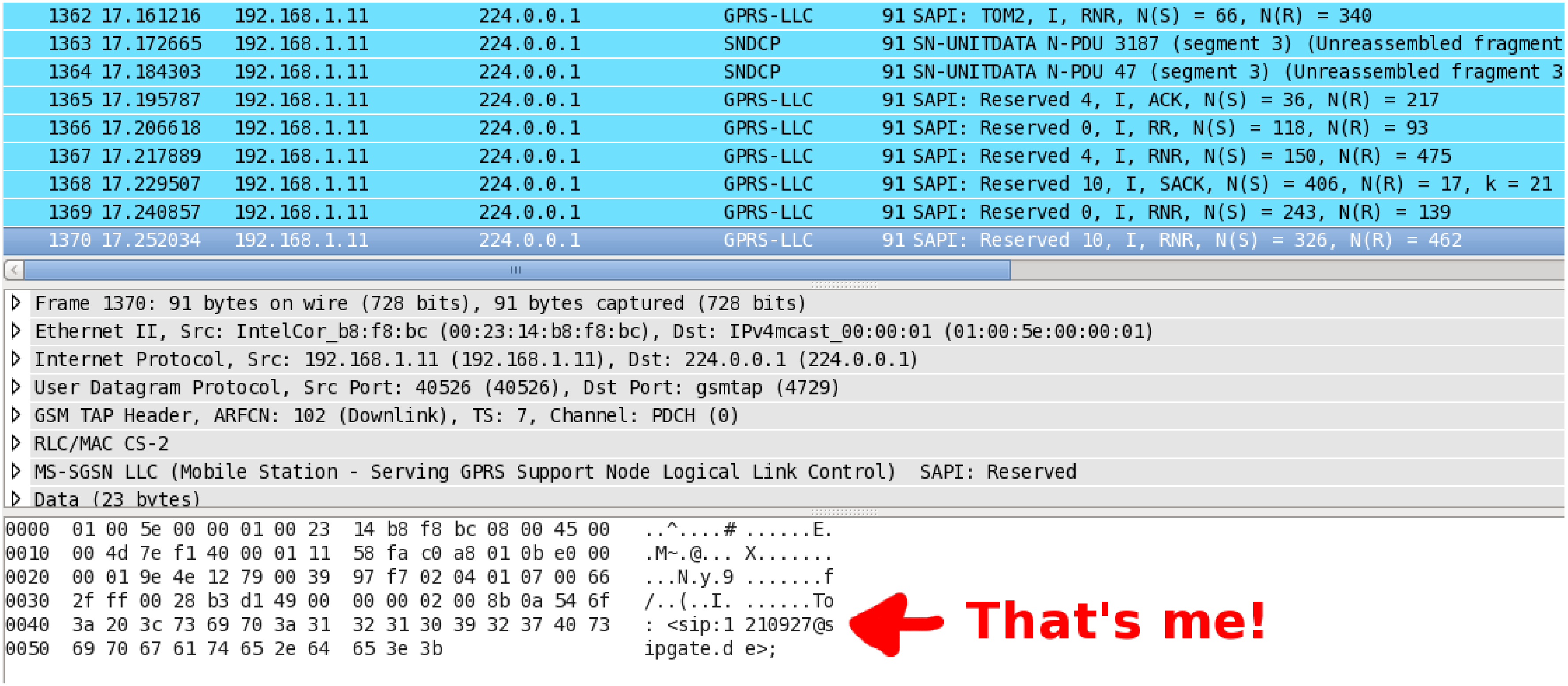
BSN	0	1	2	3	4	5	…	127
		X	X				…	

BSN 3		BSN 4		BSN 5	
LLC 0	LLC 1	LLC 2	LLC 3	LLC 4	Padding

[63 x the same decode chain]

Some GPRS networks do not use any encryption

Supposedly encryption hinders in-line data monitoring.
Hence some commercial networks use GEA/0—no encryption!



```
 1362 17.161216   192.168.1.11        224.0.0.1           GPRS-LLC     91 SAPI: TOM2, I, RNR, N(S) = 66, N(R) = 340
 1363 17.172665   192.168.1.11        224.0.0.1           SNDCP        91 SN-UNITDATA N-PDU 3187 (segment 3) (Unreassembled fragment
 1364 17.184303   192.168.1.11        224.0.0.1           SNDCP        91 SN-UNITDATA N-PDU 47 (segment 3) (Unreassembled fragment 3
 1365 17.195787   192.168.1.11        224.0.0.1           GPRS-LLC     91 SAPI: Reserved 4, I, ACK, N(S) = 36, N(R) = 217
 1366 17.206618   192.168.1.11        224.0.0.1           GPRS-LLC     91 SAPI: Reserved 0, I, RR, N(S) = 118, N(R) = 93
 1367 17.217889   192.168.1.11        224.0.0.1           GPRS-LLC     91 SAPI: Reserved 4, I, RNR, N(S) = 150, N(R) = 475
 1368 17.229507   192.168.1.11        224.0.0.1           GPRS-LLC     91 SAPI: Reserved 10, I, SACK, N(S) = 406, N(R) = 17, k = 21
 1369 17.240857   192.168.1.11        224.0.0.1           GPRS-LLC     91 SAPI: Reserved 0, I, RNR, N(S) = 243, N(R) = 139
 1370 17.252034   192.168.1.11        224.0.0.1           GPRS-LLC     91 SAPI: Reserved 10, I, RNR, N(S) = 326, N(R) = 462
```

```
▷ Frame 1370: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)
▷ Ethernet II, Src: IntelCor_b8:f8:bc (00:23:14:b8:f8:bc), Dst: IPv4mcast_00:00:01 (01:00:5e:00:00:01)
▷ Internet Protocol, Src: 192.168.1.11 (192.168.1.11), Dst: 224.0.0.1 (224.0.0.1)
▷ User Datagram Protocol, Src Port: 40526 (40526), Dst Port: gsmtap (4729)
▷ GSM TAP Header, ARFCN: 102 (Downlink), TS: 7, Channel: PDCH (0)
▷ RLC/MAC CS-2
▷ MS-SGSN LLC (Mobile Station - Serving GPRS Support Node Logical Link Control)  SAPI: Reserved
▷ Data (23 bytes)
```

```
0000  01 00 5e 00 00 01 00 23  14 b8 f8 bc 08 00 45 00   ..^....# ......E.
0010  00 4d 7e f1 40 00 01 11  58 fa c0 a8 01 0b e0 00   .M~.@... X.......
0020  00 01 9e 4e 12 79 00 39  97 f7 02 04 01 07 00 66   ...N.y.9 .......f
0030  2f ff 00 28 b3 d1 49 00  00 00 02 00 8b 0a 54 6f   /..(..I. ......To
0040  3a 20 3c 73 69 70 3a 31  32 31 30 39 32 37 40 73   : <sip:1 210927@s
0050  69 70 67 61 74 65 2e 64  65 3e 3b                 ipgate.d e>;
```

That's me!

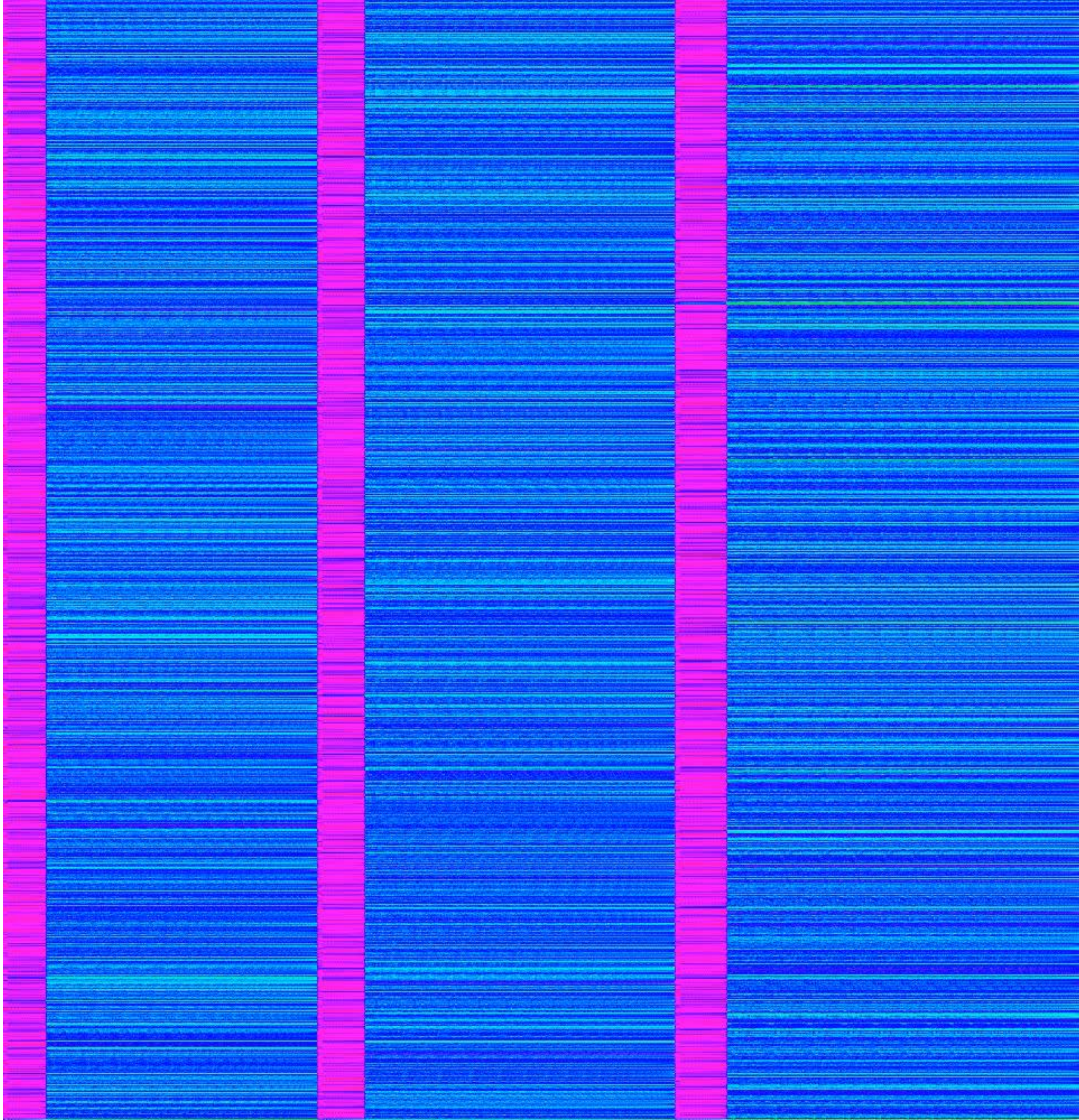
Now off to some actual cryptanalysis on all the other networks …

GEA/1 mostly mitigates A5/1's rainbow table attacks but opens new crypto holes

Bold = better

	A5/1	GEA/1	Relevant for
Key size	64bit	64bit	Brute force/(TMTO)
Internal state	64bit	**96bit**	TMTO
LFRSs	3	3	Algebraic attacks
Output nonlinearity	degree 1	**degree 4**	
Non-linear update	**Yes**	No	
Output	**114bit**	up to 1500 bytes	

GPRS lacks good non-linearity

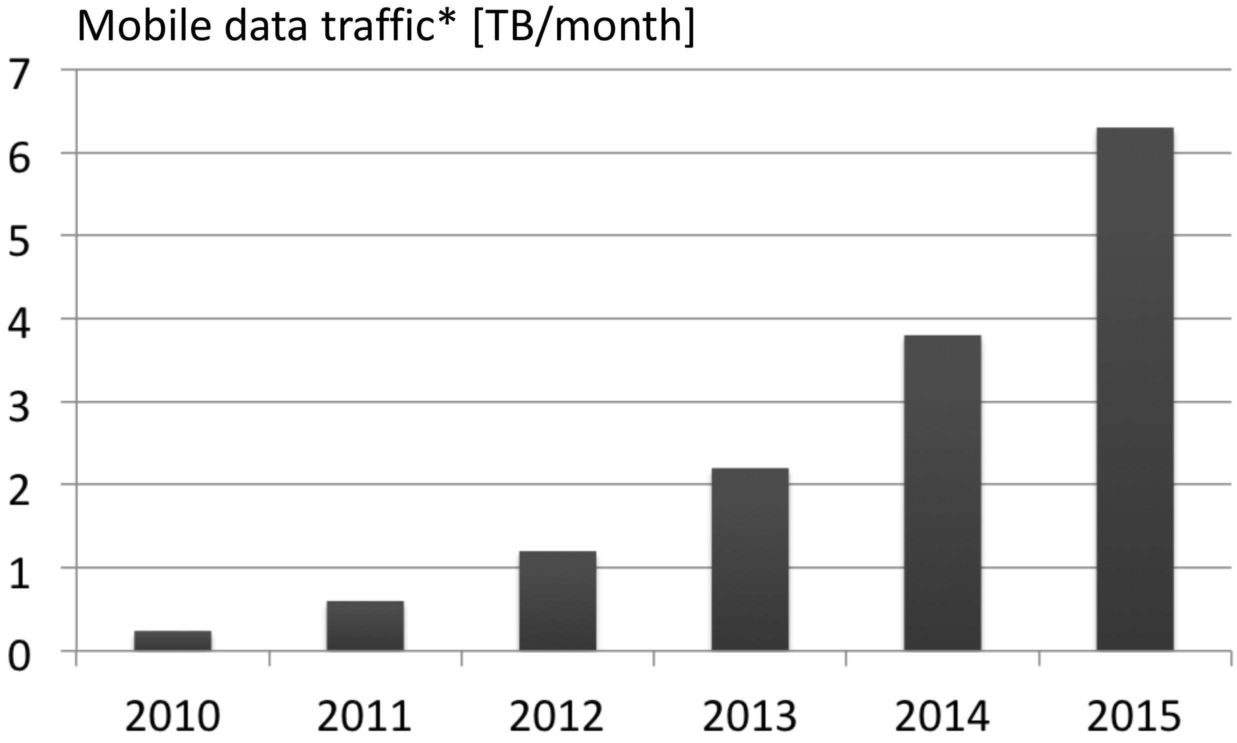


Agenda

- GPRS basics
- Practical GPRS attacks
- **Mitigation measures**

Not securing mobile data would be negligent

GPRS is here to stay



Securing GPRS requires actions from networks and application authors

A

Short term mitigation:

Application must protect themselves

+

B

Mid/long term need:

Networks must upgrade encryption

SECURITY RESEARCH LABS

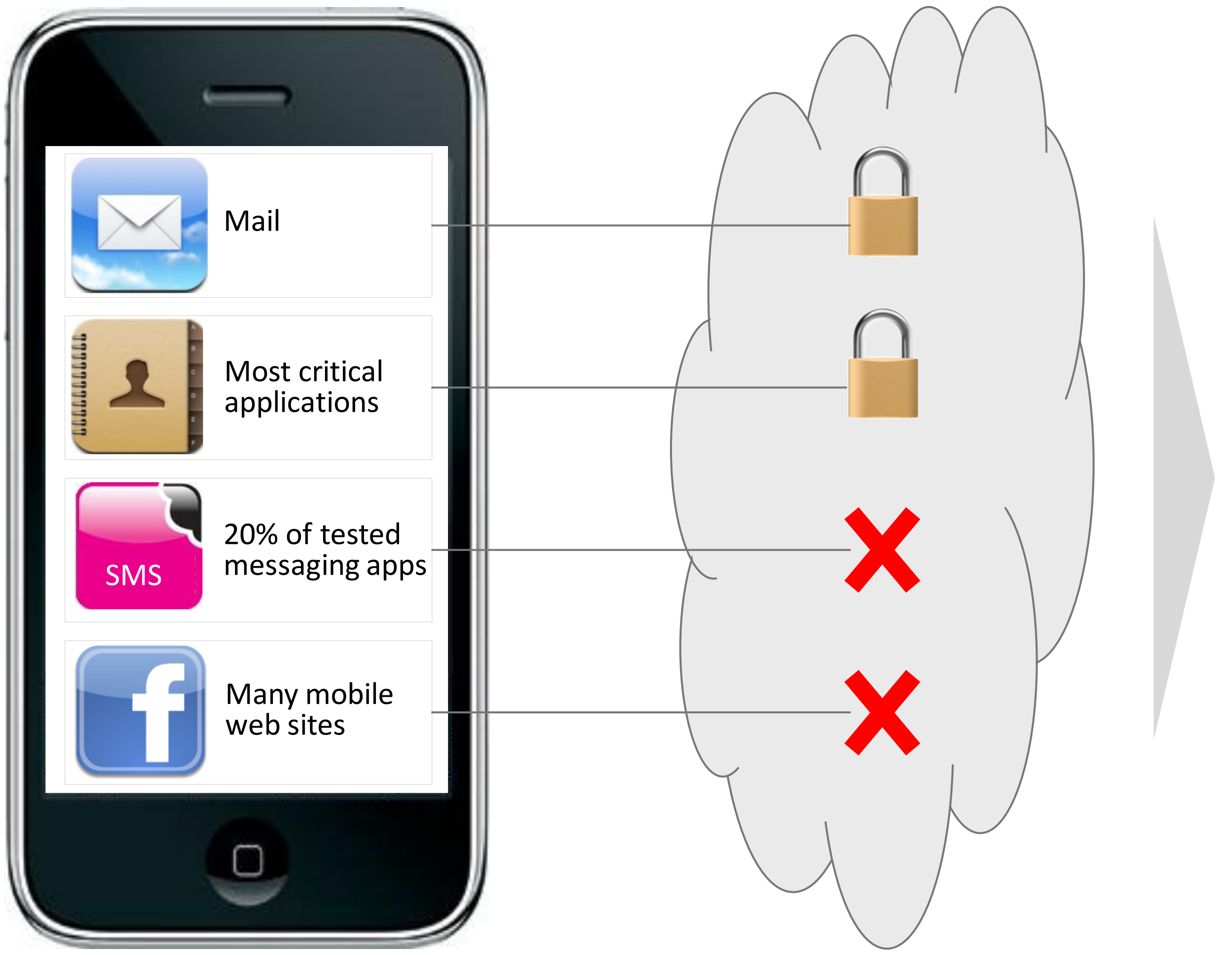
*Source: Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update (February 1, 2011)

A Mobile applications should start using internet-grade encryption

🔒 Well encrypted* ✗ Not encrypted

Example – iPhone applications

GPRS / Internet



- Some mobile application and most mobile web sites send data unencrypted over GPRS
- SSL, proudly used on the internet since 1994, could easily protect all this data

*Some iOS versions use vulnerable SSL implementations that can be abused in a fake base station attack

B GPRS network wish list – Continuous improvements

Immediately – Switch on encryption

Mid term – Add mutual authentication

Long term – Upgrade to USIM + 128bit GEA/4

Mobile data finally secure against todays threats

1. Deploy Java applet to SIM card

2. Execute mutual authentication from Java Applet before generating GPRS key

3. Use GEA/3 to secure connection

Network operator

GPRS currently is a risk to mobile societies

Lots of thanks to Mate Soos, Dieter Spaar, Harald Welte, Sylvain Munaut and Dexter

Risk: The level of protection widely differs among networks but is typically outdated.

Mitigation: Protect applications through SSL and start demanding better protection from your operator

Osmocom GPRS sniffing tutorial:
srlabs.de/gprs

Questions?
Karsten Nohl, nohl@srlabs.de
Luca Melette, luca@srlabs.de