Berlin Institute of Technology
FG Security in Telecommunications

Let Me Answer That For You: Exploiting Broadcast Information in Cellular Networks

USENIX Security '13

Nico Golde, Kévin Redon, Jean-Pierre Seifert
{nico, kredon, jpseifert}@sec.t-labs.tu-berlin.de

August 14th, 2013
Washington, D.C.

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Motivation - Yet Another Attack on GSM?

- Numerous security vulnerabilities already exist on GSM, but few of them involve active adversaries
- GSM is still one of the most relevant mobile telephony standards: it still account for an important part of the mobile traffic, every phone supports GSM, M2M and IoT will used it for long, ...
- GSM is still widely used and a model for mobile communication
- The same mechanism from GSM are used in UMTS and LTE, including the paging
- Freely modifiable GSM stack + baseband exist for verification

Contributions

- We present the paging response attack
  - Novel attack against mobile terminated services
- We show feasibility in practice
  - Implemented phone firmware which to steal SMS and perform denial of service attacks
  - Evaluate attack in major European GSM operator networks
- We access requirements and challenges to large-scale denial
  - Evaluate feasibility of attacks against large regions such as city districts (example: Berlin)

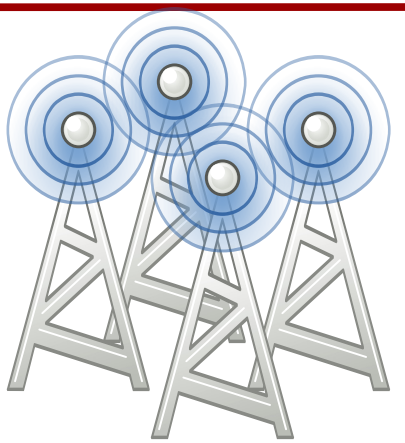
Introduction to paging

- Paging: mechanism used by the network to notify an incoming service
- Once a phone is registered to a cell, it listens to only the Paging Channel (PCH) broadcast downlink channel on the CCCH (this saves energy)
- Phone update their location only when they changes Location Area (LA), but can listen to any PCH from any BTS within this LA
- Paging message carries Mobile Identity (IMSI/TMSI)
- Each phone compares its identity and reacts
- Again, this information is **broadcast**!
  → every phone can see every paging request

Mobile Terminated service delivery cont.

All phones within a LA

Paging request on the PCH



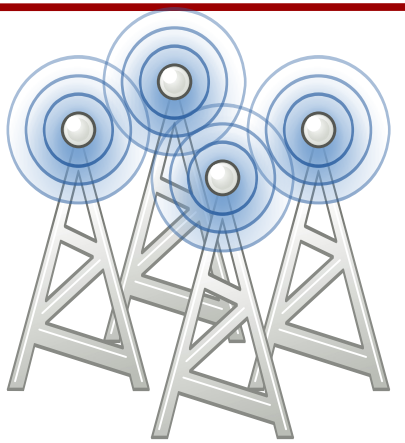
all BTSs within a LA

Mobile Terminated service delivery cont.

All phones within a LA

Paging request on the PCH

DEADBEEF == identity?



all BTSs within a LA

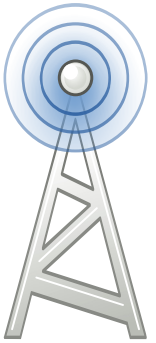
Mobile Terminated service delivery cont.

phone

Paging request on the PCH

DEADBEEF == identity?

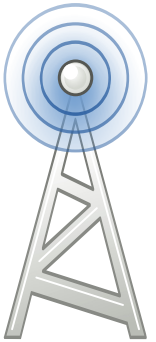
Initial channel request (RACH)



BTS

Mobile Terminated service delivery cont.

phone



BTS

Paging request on the PCH

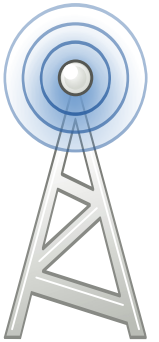
DEADBEEF == identity?

Initial channel request (RACH)

Immediate Assignment (AGCH)

Mobile Terminated service delivery cont.

phone



BTS

Paging request on the PCH

DEADBEEF == identity?

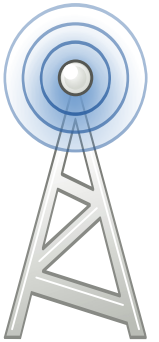
Initial channel request (RACH)

Immediate Assignment (AGCH)

Tune to allocated channel

Mobile Terminated service delivery cont.

phone



BTS

Paging request on the PCH

DEADBEEF == identity?

Initial channel request (RACH)

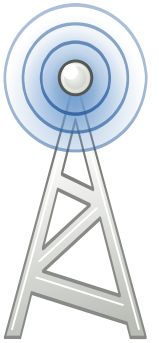
Immediate Assignment (AGCH)

Tune to allocated channel

Paging response message (SDCCH)

Mobile Terminated service delivery cont.

phone



BTS

Paging request on the PCH

DEADBEEF == identity?

Initial channel request (RACH)

Immediate Assignment (AGCH)

Tune to allocated channel

Paging response message (SDCCH)

Authentication, Ciphering, Service Delivery

Paging Attack

- We have a **race condition**!

- GSM protocols are driven by complex state machines

- Can we respond to other peoples paging messages?
- Can we do that faster?
- Will the network expect a 2nd paging response?

- We could do that from any BTS in the same area (preferably the one with the best radio link)!

Paging Attack – implementing a fast baseband

- Free Software/Open Source mobile baseband firmware: OsmocomBB
  - Runs on cheap hardware (e.g. cheap Motorola C123)
  - Mobile phone application exists (but runs on PC!)
    → not fast at all :/

- Completely implemented as Layer1 firmware
  - Ported Layer2/Layer3 to Layer1
  - Runs solely on the phone → very fast

- Listens to messages on the PCH
- Can react to IMSIs/TMSIs or TMSI ranges
- Sends paging response messages
- Performs invalid ciphering/auth

Paging Attack - Measuring paging response speed

- Relevant baseband stacks:

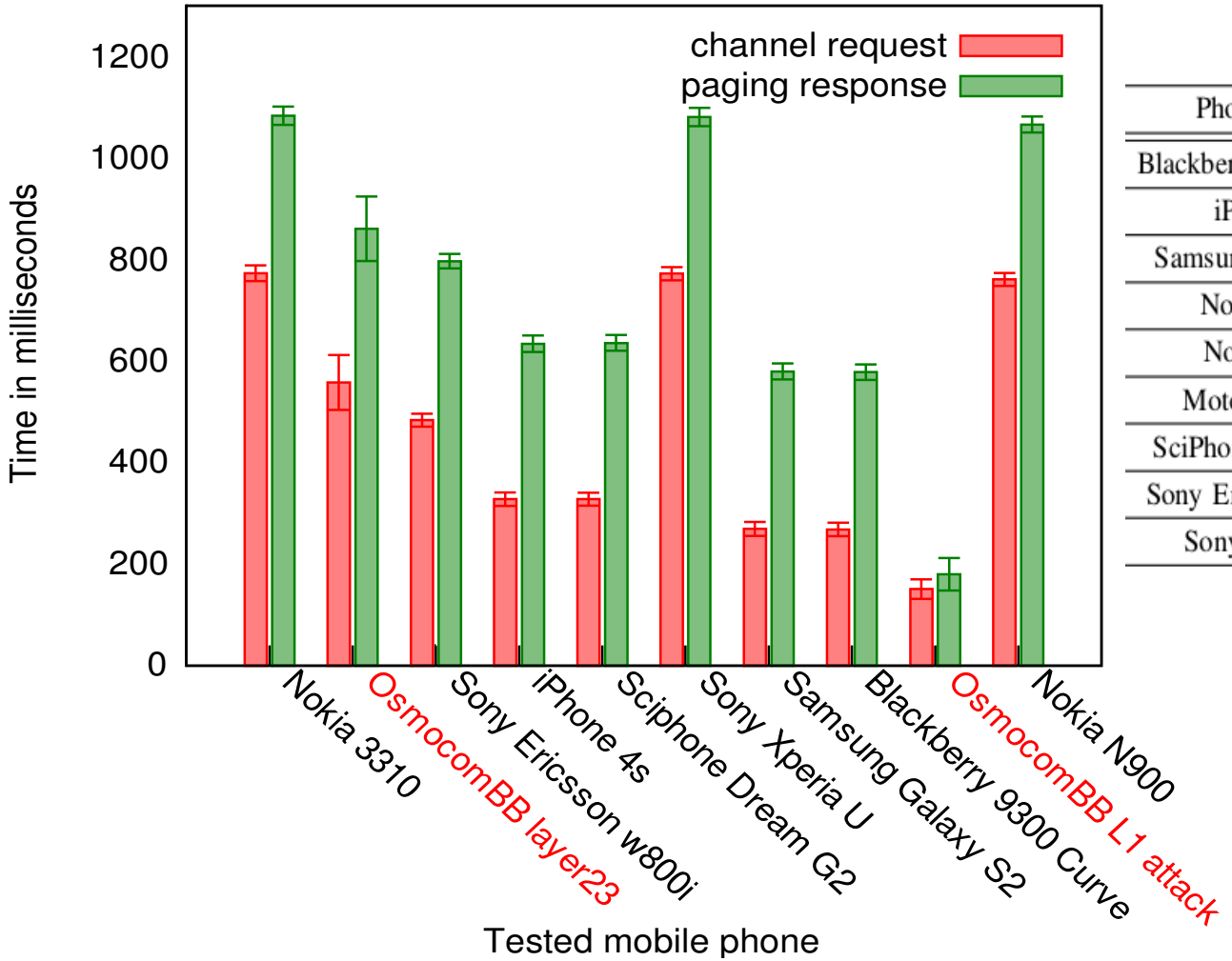
  Qualcomm, Intel (Infineon), Texas Instruments, ST-Ericsson, Renesas (Nokia), Marvell, Mediatek

- USRP + Modified OpenBTS version logs:
  - Time for Paging Request ↔ Channel request
  - Time for Paging Request ↔ Paging response

- Hookup phones to test BTS
- Send 250 SMS to each phone
- Measure time

Paging Attack - How fast is the “average” phone?

- Time measurements for each baseband



Phone model	BB chipset	BB vendor
Blackberry Curve 9300	Marvell PXA930	Marvell
iPhone 4s	MDM6610	Qualcomm
Samsung Galaxy S2	XMM 6260	Infineon
Nokia N900	Unknown TI (Rapuyama)	Nokia
Nokia 3310	TI MAD2WDI	Nokia
Motorola C123	TI Calypso	OsmocomBB
SciPhone Dream G2	MT6235	Mediatek
Sony Ericsson W800i	DB2010	Ericsson
Sony Xperia U	NovaThor U8500	ST-Ericsson

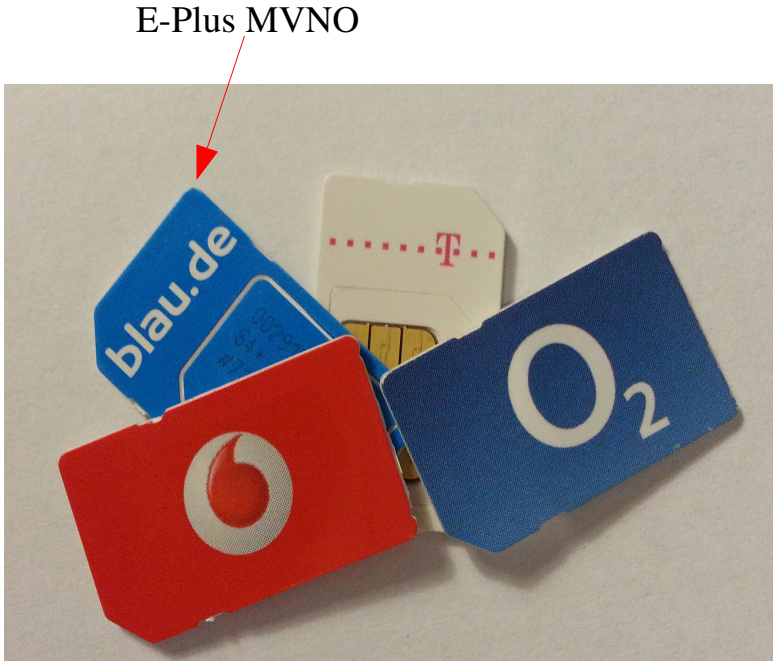
Paging Attack - Practice results

- Small layer1 only implementation can win the race!
  → DoS against Mobile Terminated services

- Tested all German operators:
  - Vodafone
  - O2 (Telefonica)
  - E-Plus
  - T-Mobile

  → all vulnerable to this attack

- Can be used for selective DoS



Hijacking Services

- To impersonate a victim we need:
  - victim's identity
  - credentials normally stored in the SIM to pass the authentication

- With this information we can hijack the MT service:
  - get the SMS
  - receive the call
  - ...

Getting victim mobile identities

- You don't necessarily have to (why not just react to every paging?)
- Network paging with IMSIs:
  - 3rd party HLR lookups provide number → IMSI mapping
- For TMSIs:
  - Monitor PCH with OsmocomBB phone
  - Call victim, drop call early (3.7 seconds on O2)
    → phone will not ring, but being paged!
  - Or use silent SMS
  - Rinse and repeat

  → Evaluate monitored data

"Location leaks over the GSM air interface", Kune et al., NDSS 2012

Hijacking delivery – Encryption

- GSM uses weak encryption, which enables us to pass the authentication and impersonate a victim

- We need Kc for encrypted communication!
- Some networks use A5/0 → No encryption
- Some networks use A5/2 → Broken (1999)
- Most use A5/1 → Broken (e.g. 26C3/27C3)
  - Kraken + OsmocomBB phones/airprobe can crack session key (Kc) in seconds

"Wideband GSM Sniffing", Munaut & Nohl, 2010

Paging Attack cont. – Authentication

- 50% of networks authenticate MT (SMS/call) 10% of the time
  (referring to Security Research Labs)

- Operators care about MO because of billing!
- However, MT indirectly affects billing

- Most MT service deliveries not authenticated

© Julien Tromeur

- Incomplete authentication allows MT hijacking
  → Our code can handle a known session key/encryption

Attacking large areas

- Paging requests are broadcasted on all BTSs within a location area
  → we don't need to camp on the same BTS

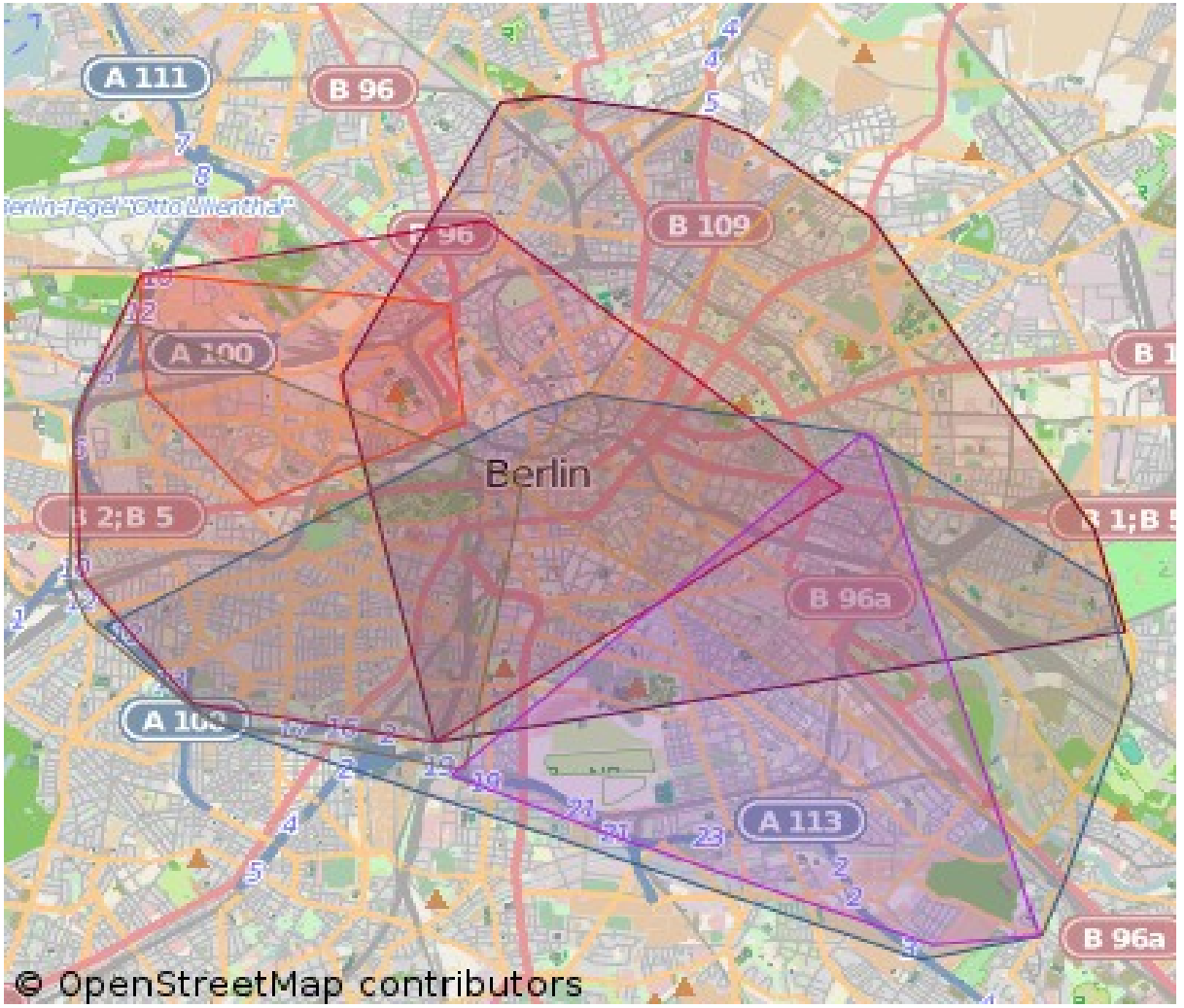
- We can respond to all paging requests faster
  → DoS to all subscribers in that area

- What is the size of a Location Area?
- How many users are affected?
- What is the amount of paging requests to answer to?

How large is a Location Area?

- Location Area Code broadcast on the BCCH
- 2 people + GPS loggers + OsmocomBB cell_log phones + car :)

Location Areas – Berlin/Vodafone



Attacking Location Areas cont.

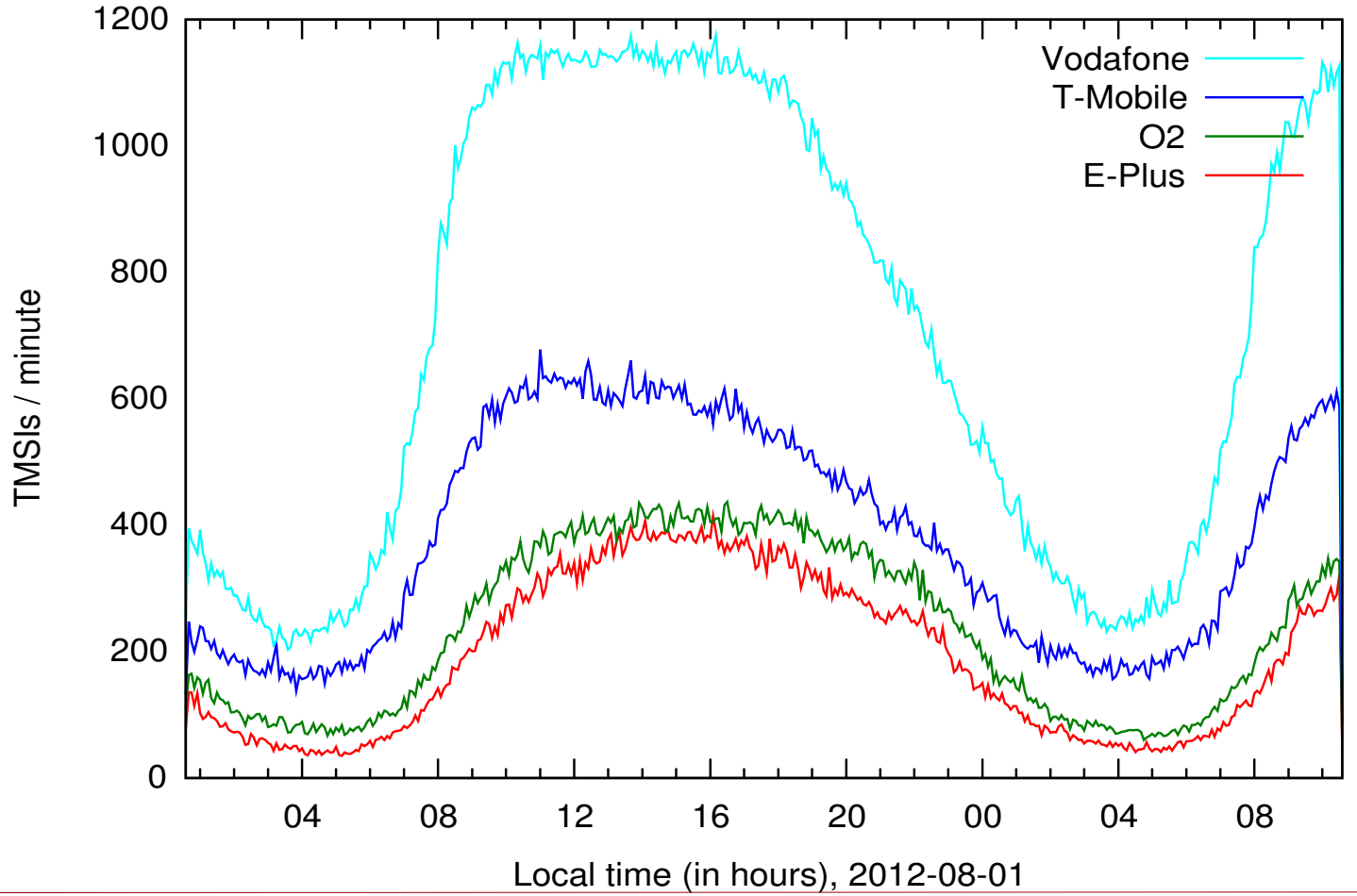
- Non-city LAs larger (and fewer) than for cities
  - Seen 1000 km²
- Location Areas are huge even in cities!
  - 100 – 500 km² in Berlin
  - Cover whole city districts

- For Mobile Terminated: Paging DoS way more effective than jamming (can be done from any location)

- Feasibility depends on paging activity

Attacking Location Areas - Activity

- We can camp on location areas and log paging
- Measured all 4 operators over 24 hours, same time and location



Attacking Location Areas cont.

- One phone can answer to ~1 paging request/sec (including sending paging response and retuning to BCCH)
- ~ 11 phones are needed to answer all paging requests within location area of a small operator (E-plus). This is supported by a single BTS.
- These phones are cheap (5-20 €)

DoS + Paging activity reduction

- Paging attack stops initial service delivery
- We don't want to answer every time in the future

- IMSI DETACH attack by Sylvain Munaut
- Phone detach signal to network
  → Mobile Terminated services not delivered until re-attach

- Detach message contains mobile identity
  → send paging response, send detach message
  → watch paging reducing over time

Conclusions

- Attacking single subscribers and Location Areas is practical!
- Impersonating victims is practical!
- DoSing all subscribers within a location area is practical!

- MT services need 100% authentication
- Active attackers (malicious phones) need to be considered by standardization bodies

Thank you for your attention!

- Also thanks to these people:
  - Dmitry Nedospasov
  - Benjamin Michéle
  - Alex Dent
  - Dieter Spaar
  - Harald Welte
  - Holger Freyther
  - Osmocom community!

Questions?

- Demonstration videos are available:
  https://www.youtube.com/watch?v=oep3zpY6cvE
  https://www.youtube.com/watch?v=4umb2P-93BQ
- (Uncleaned) source code available:
  http://tinyurl.com/fun-with-paging
  (Apply on osmocom changeset 4f0acac4c1fa538082f54cb14bef0841aa9c8abb)

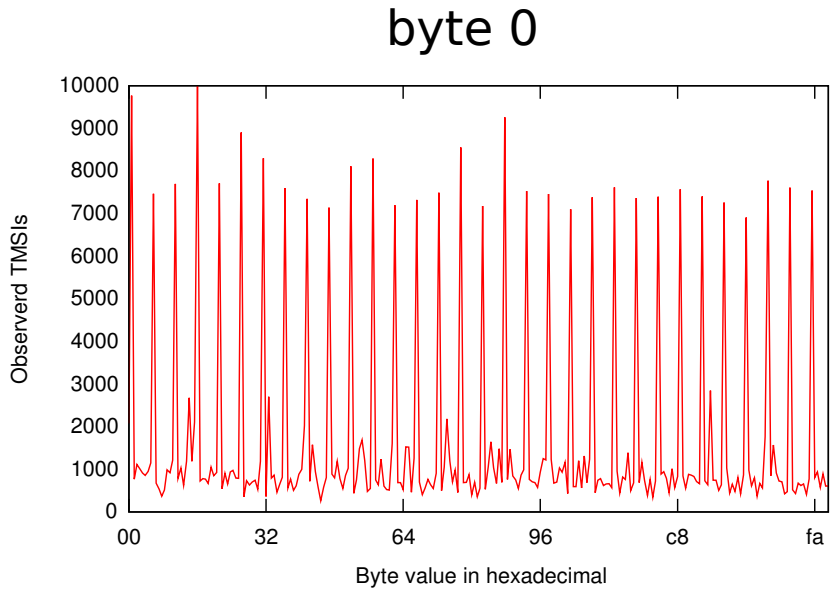
- Mail:
  nico@sec.t-labs.tu-berlin.de
  kredon@sec.t-labs.tu-berlin.de
- Twitter: @iamnion

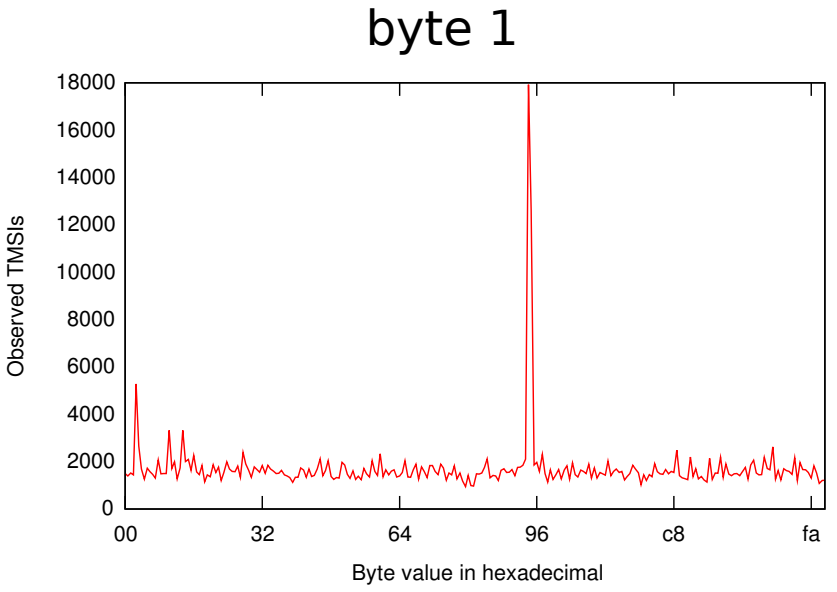
- Disclaimer: don't do this at home… or only with your own SIM cards!

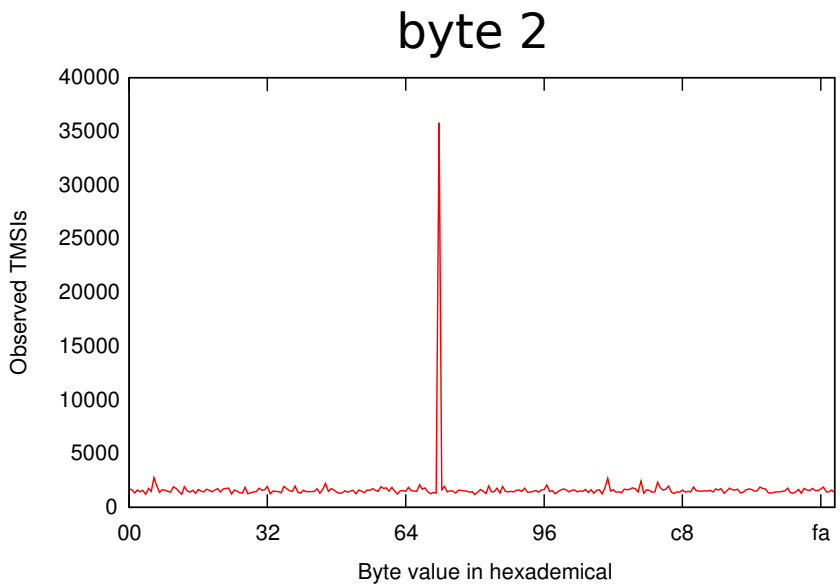
Countermeasures

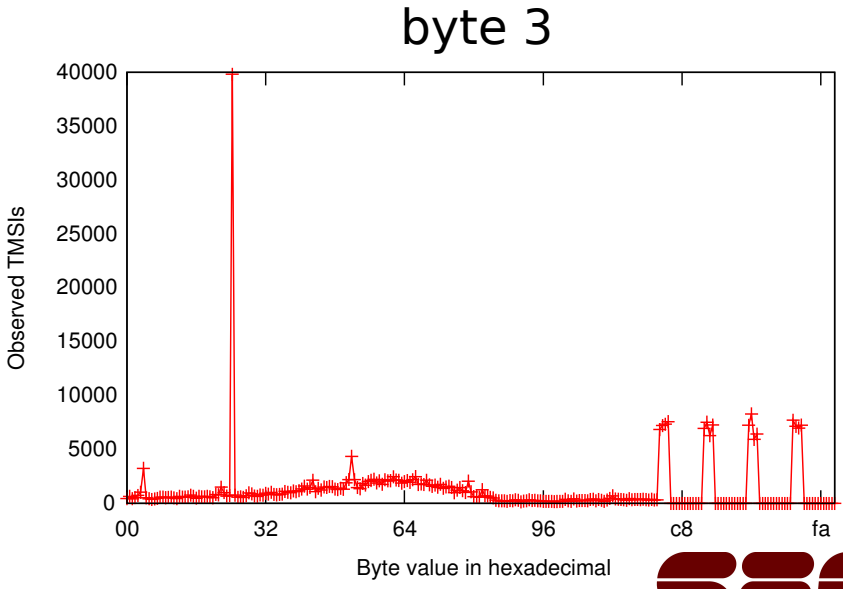
- 100% MT authentication: prevents hijacking
- Use A5/3: prevents hijacking
- Refresh TMSI: prevents targeted DoS
- Wait for authentication before assigning MT service: removes race condition
- Use authenticated paging: removes race condition

TMSI distribution









TMSI distribution (cont.)