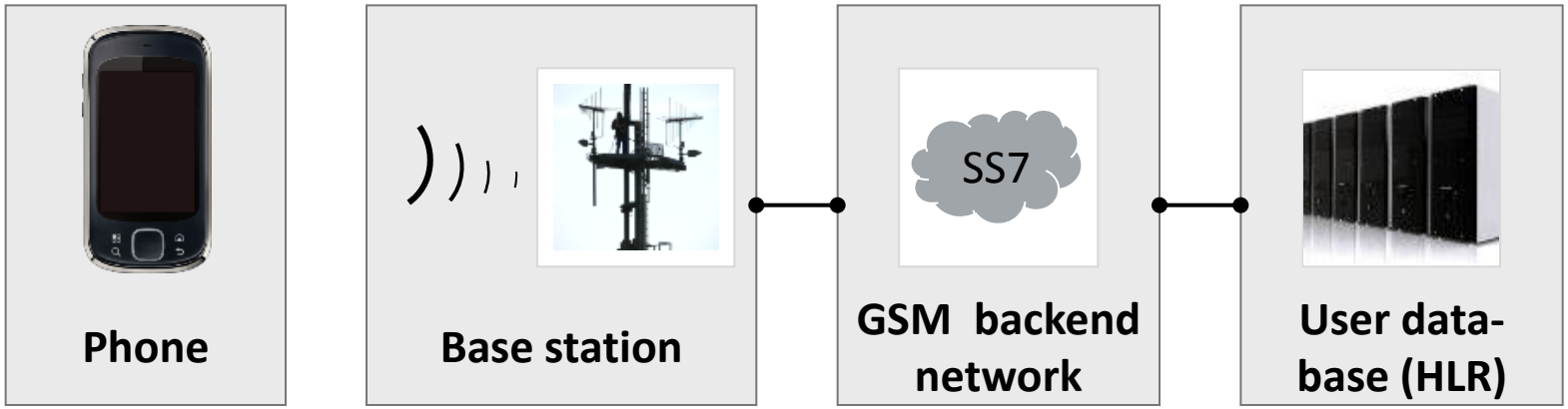
Defending mobile phones

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

SECURITY RESEARCH LABS

GSM networks provide the base for various attacks



Vulner-ability -> attack vector

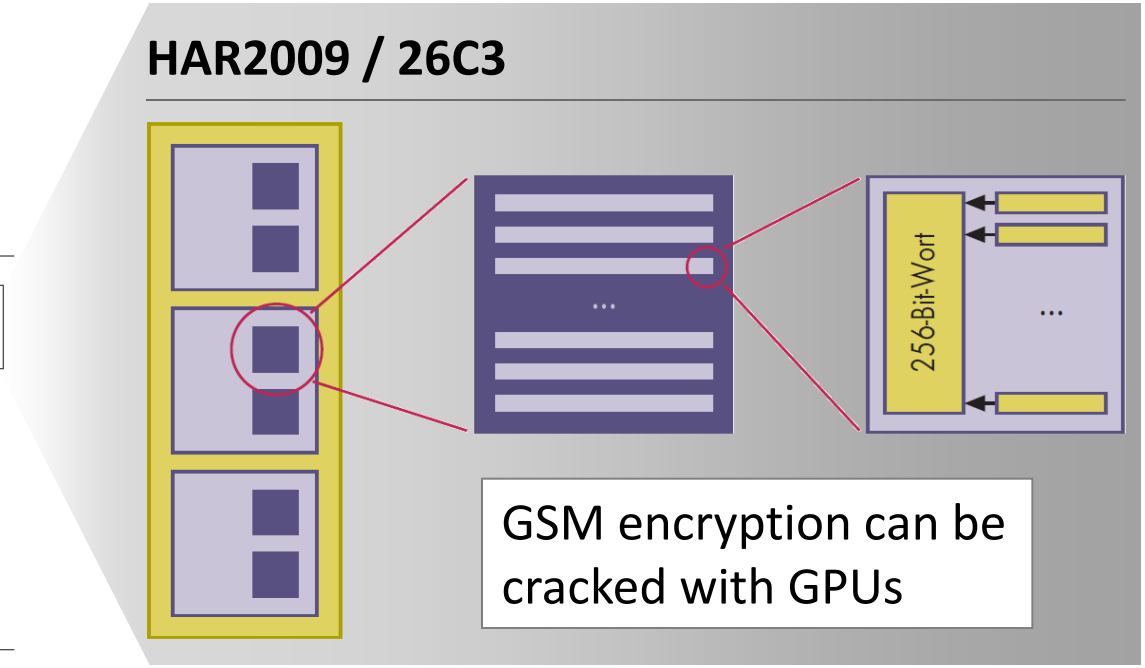
- User naiveté -> Phishing
- OS bugs -> Malware

- Lack of network authentication -> Fake base stations
- Weak encryption, predictable plaintext -> Intercept
- Irregular authentication -> Mobile impersonation
- HLR leaks -> User tracking

Covered in this lecture

Agenda

- **Mobile impersonation**
- GSM network defenses
- GSM self-defense



Premium number/SMS fraud is on the rising

sipgate

Trunking | Rufnummern | Vertrag & Standorte | Konto & Rechnung

Kontoauszug

Kontoauszug | Einzelverbindungsnachweis | Konto aufladen | Rechnungen

Automatische Aufladung

aktiviert

Weitere Informationen zur automatischen Aufladung finden Sie hier.

Ändern

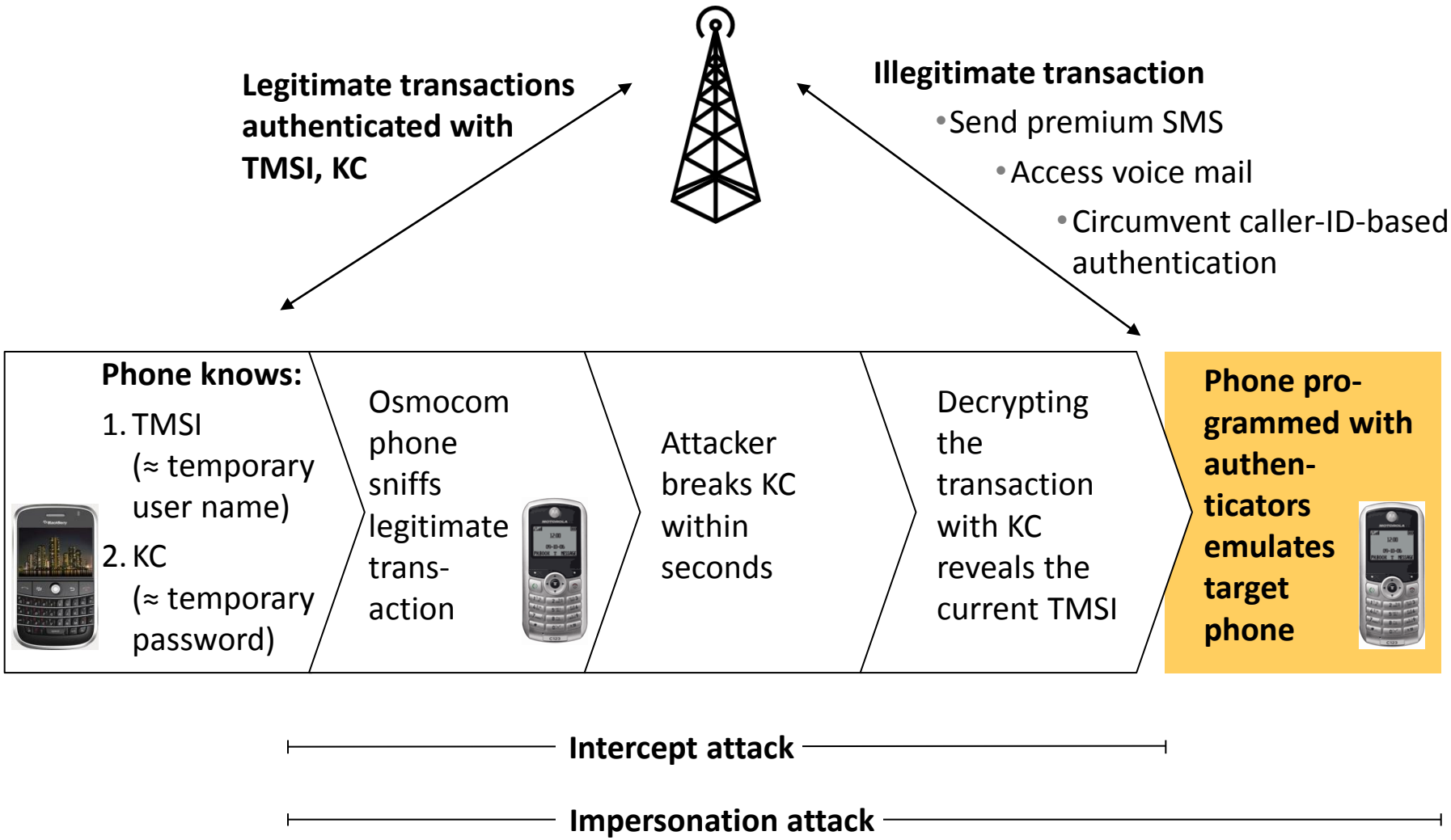
Benachrichtigung

Oktober 2011

01.10.2011 bis 31.10.2011 Anzeigen

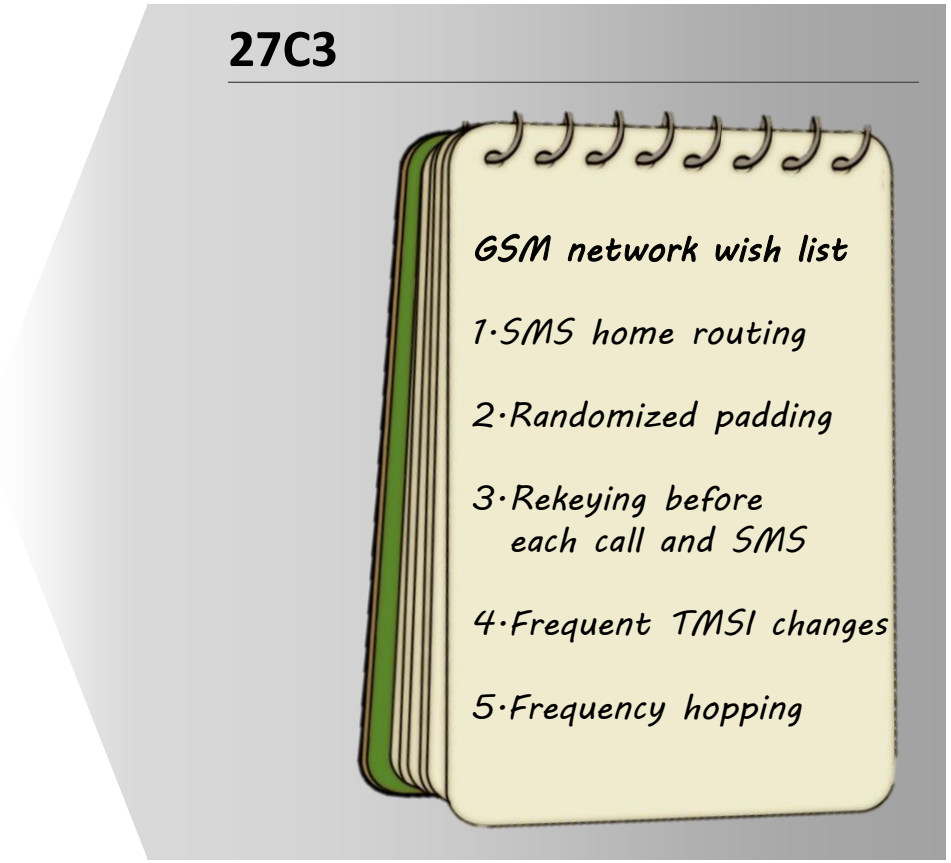
Kontostand vom 01.10.2011	**36,2460 €**
Kostenpflichtige Leistungen	**-1.185,0510 €**
1030 Verbindungen zu Anruf ausgehend SAO TOME AND PRINCIPE	-1.108,7780 €
19 Verbindungen zu Anruf ausgehend MACEDONIA, THE FORMER YU	-9,8670 €

Fraud can happen through mobile impersonation



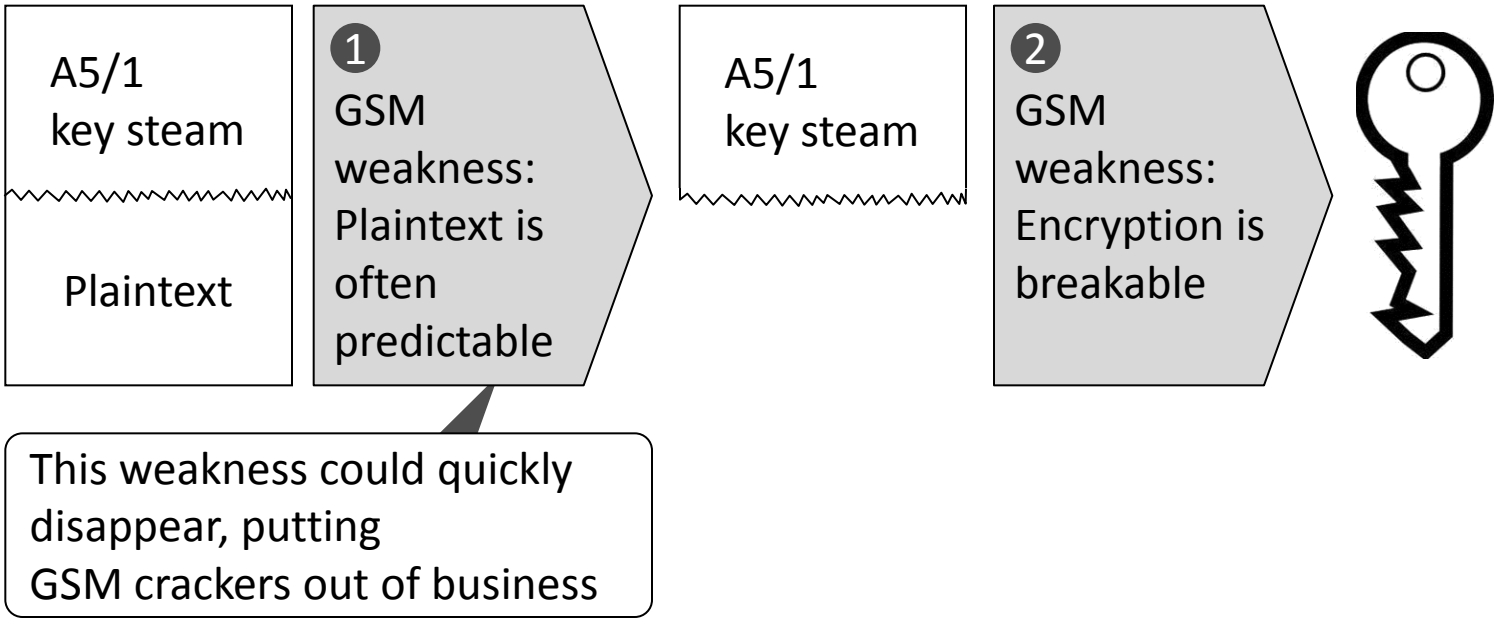
Agenda

- Mobile impersonation
- **GSM network defenses**
- GSM self-defense



Cracking GSM requires both a weak cipher and predictable transactions

A5/1 cracking



Some network defenses can be deployed within weeks

GSM crackers rely on 2 GSM weaknesses

GSM weakness	Mitigations: Measures	Mitigations: Cost	Mitigations: Deployment time
1 Predictable plaintext	▪ Padding randomization ▪ SI randomization	Software update (free to a few millions $)	Weeks
2 Stream cipher with small state 3 Statistical weaknesses	▪ A5/3 ▪ A5/4	New base station con-trollers (tens to hundreds of millions $)	1-2 years

GSM transaction are often highly predictable

SDCCH trace

238530	03 20 0d 06 35 11 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
238581	03 42 45 13 05 1e 02 ea 81 5c 08 11 80 94 03 98 93 92 69 81 2b 2b 2b
238613	00 00 03 03 49 06 1d 9f 6d 18 10 80 00 00 00 00 00 00 00 00 00 00 00
238632	01 61 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
238683	01 81 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
238715	00 00 03 03 49 06 06 70 00 00 00 00 00 04 15 50 10 00 00 00 00 0a a8
238734	03 84 21 06 2e 0d 02 d5 00 63 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
238785	03 03 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b

Mitigations

Padding randomization was standardized in 2008 (TS44.006)

SI5/SI6 randomization standardized in 2011 (TS 44.018)

"Do not encrypt predictable control messages" being standardized, however not backward-compatible with existing phones (GP-111234 and GP-111333)

Randomizing control messages can win the arms race against A5/1 crackers

GSM security upgrades	1. Basic network randomization	2. Full network randomization	3a. A5/3 encryption OR 3b. Uplink randomiz.
Effect	▪ Current A5/1 black boxes drop to < 30% success rate	▪ Current black boxes drop to < 5% for long-range (passive) sniffing	▪ Current black boxes are defeated, even in short-range and active operations
Popularity	▪ Patches available ▪ Roll-outs in some networks	▪ Standardization finalized ▪ Select operators test proprietary ideas	▪ Select networks plan A5/3 upgrades ▪ A5/3 available on new phones (but buggy on at least one!) ▪ Randomization available on latest chips, seen on 1 phone

Network operators greatly differ in protection, none implements all available security

Select European networks ordered by their protection against impersonation*

		Authenticated calls, %	Randomization		
			Padding	SI	HLR blocking**
Example best-in-class networks		38	✓	×	×
		99	×	×	×
		100	×	×	×
		100	×	×	×
	. . .				
Example weak networks		2	×	×	×
		0	×	×	✓
		0	×	×	×
		1	×	×	×

No network currently implements all available protection measures

SECURITY RESEARCH LABS

* Based on the SRLabs GSM security metric v0.6, ** Parameter not relevant for mobile impersonation

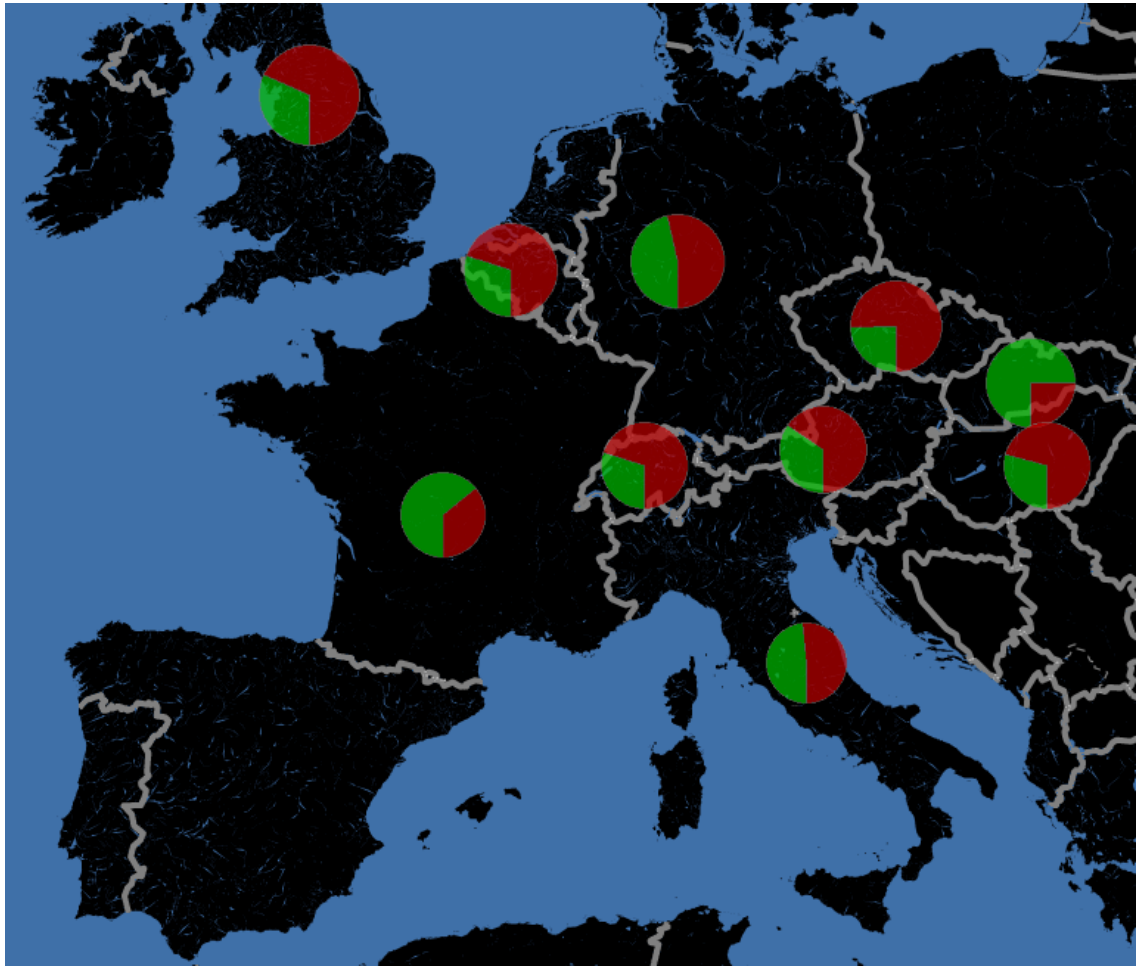
The *GSM security metric* quantifies the protection against 3 attacks relative to best practices

Relevant attacks	Example security parameters	Reference network 2011
Impersonation	▪ Encryption	A5/1
	▪ Authentication frequency	100%
Intercept	▪ Padding randomization	✓
	▪ SI randomization	✗
Tracking	▪ HLR blocking	✓
	▪ TMSI change	100%

Reference will be updated yearly to reflect ongoing technology evolution

Help us create transparency around networks' defense abilities

gsmmap.org network comparison



Please help in collecting data for the rest of the world and in keeping the map up to date

All you need is an Osmocon-capable phone

Agenda

- Mobile impersonation
- GSM network defenses
- **GSM self-defense**

IMSI catcher attacks can be detected

Fake base stations ("IMSI catchers") are used towards three illegitimate purposes

1. **Phone inventory** — Phone and SIM card identifier (IMEI, IMSI) are harvested to build location profiles
2. **Pinpointing** — The phone is forced into a silent call that is tracked as a radio token
3. **Man-in-the-middle** — Calls and SMS are routed through the fake base station and intercepted

Fake base stations leave suspicious traces

Evidence on phone	Evidence in network
▪ Location rejects	▪ Unusual location update queries
▪ Silent call at highest send power	
▪ Unencrypted transactions	▪ Authentication delays (for encrypting attacks)

The *CatcherCatcher* project detects this evidence on Osmocom phones

Questions?

GSM map, Osmocom patches	**gsmmap.org**
CatcherCatcher project	**opensource.srlabs.de**
Mailing lists (gsmmap, CatcherCatcher)	**lists.srlabs.de**

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