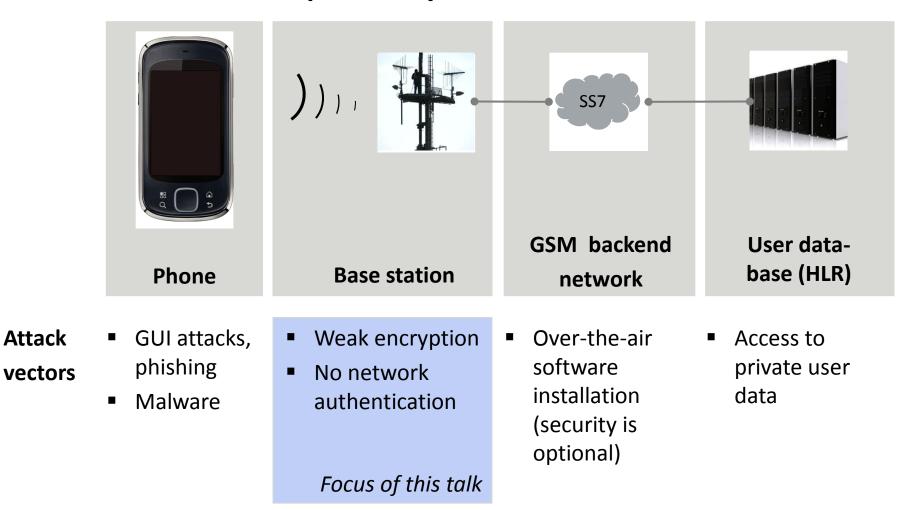
### **GSM Sniffing**

Karsten Nohl, nohl@srlabs.de Sylvain Munaut, 246tnt@gmail.com

Sylvain Munaut, 246tnt@gmail.com



## GSM networks are victim and source of attacks on user privacy



### GSM intercept is an engineering challenge

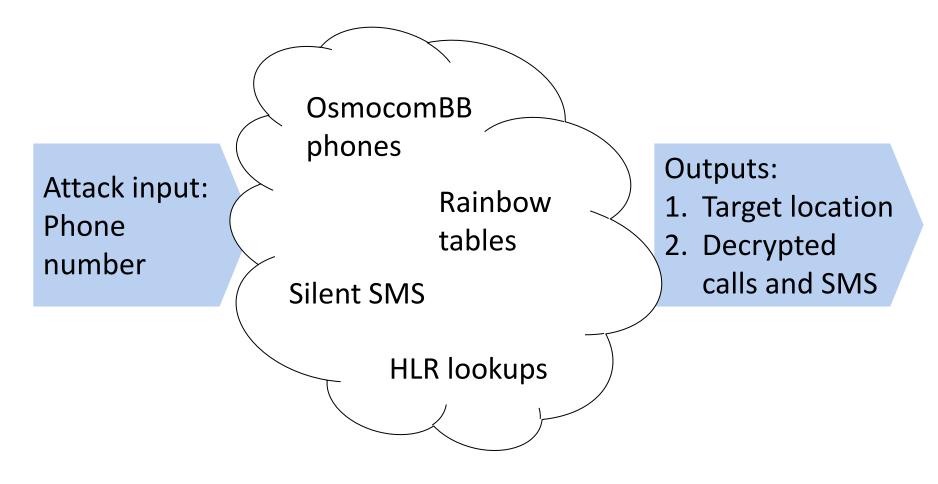
"... the GSM call has to be **identified** and **recorded** from the radio interface. [...] we strongly suspect the team developing the intercept approach has underestimated its practical complexity.

A hacker would need a radio receiver system and the signal processing software necessary to process the raw radio data." – GSMA, Aug. '09

This talk introduces cheap tools for capturing, decrypting and analyzing GSM calls and SMS



## We will demonstrate how to find phones and decrypt their calls



### Agenda

#### Locating a phone

- Sniffing air traffic
- Cracking A5/1



## Telcos do not authenticate each other but leak private user data

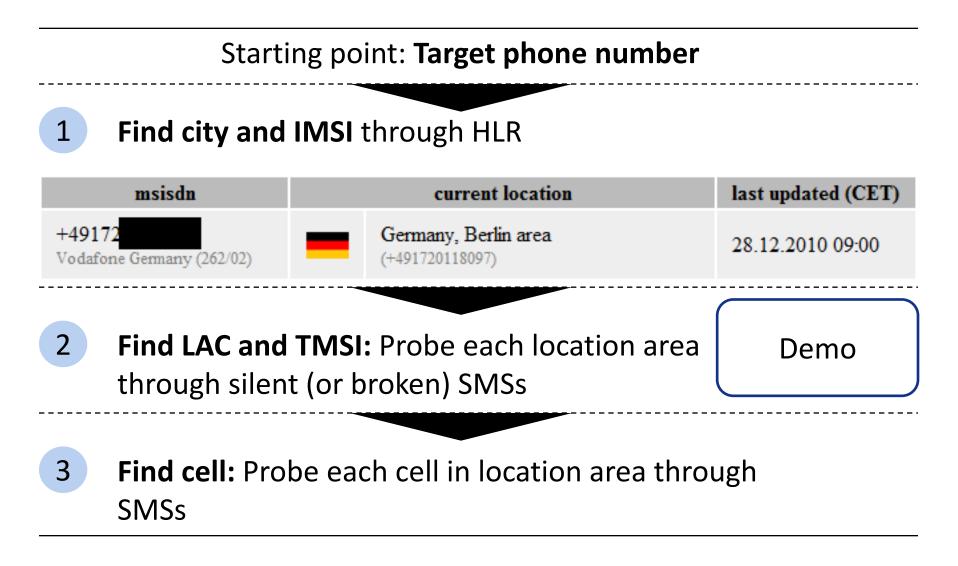


- All telcos trust each other on the global SS7 network
- SS7 is abused for security and privacy attacks; currently for SMS spam

## Information leaked through SS7 network disclose user location

Query	Accessible to	Location granularity		
HLR query	Anybody on the Internet	<ul> <li>General region (rural) to city part (urban)</li> </ul>		
Anytime	Network	Cell ID: precise		
interrogation	operators	location		
	T-Mobile Germany	Vodafone Germany		
F	irst digit of area code	First digit of ZIP code		
Berlin	+491710360000	+491720012097		
Hamburg	+49171040000	+49172002:2097		
Frankfurt	+491710650000	+491720061097		
-location grar	nularity accessible	from the Internet-		
SECURITY RES	EARCHLABS			

### Our target phone is currently in Berlin



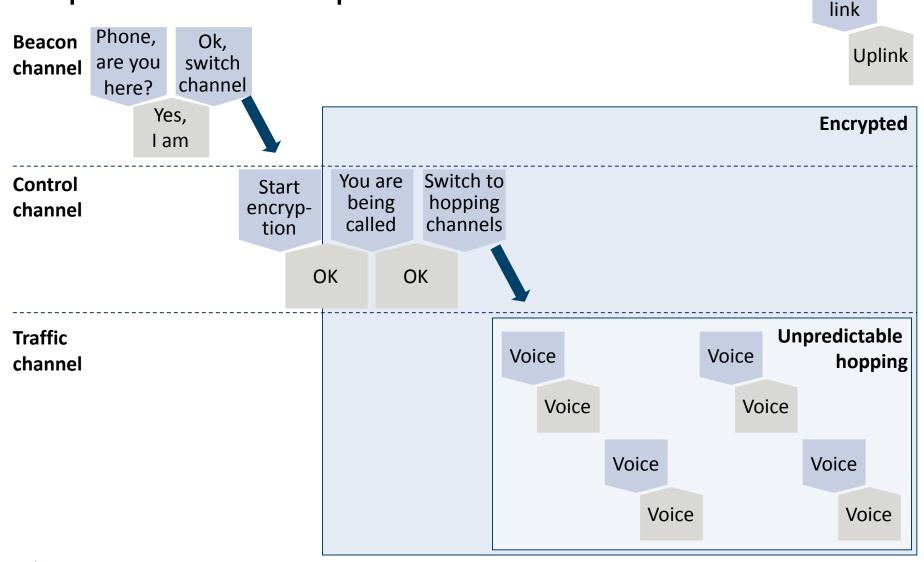
### Agenda

Locating a phone

Sniffing air traffic

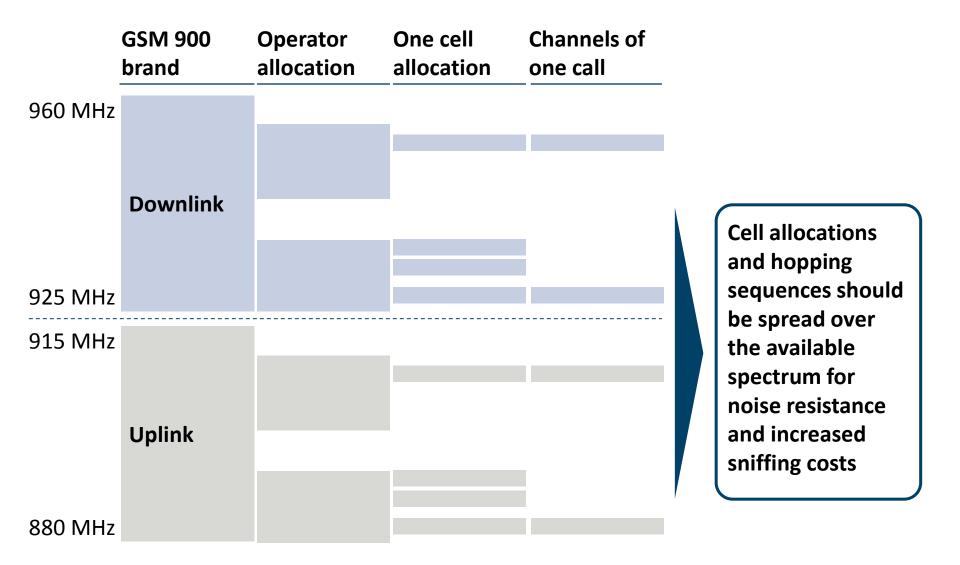
Cracking A5/1

## GSM calls are transmitted encrypted over unpredictable frequencies



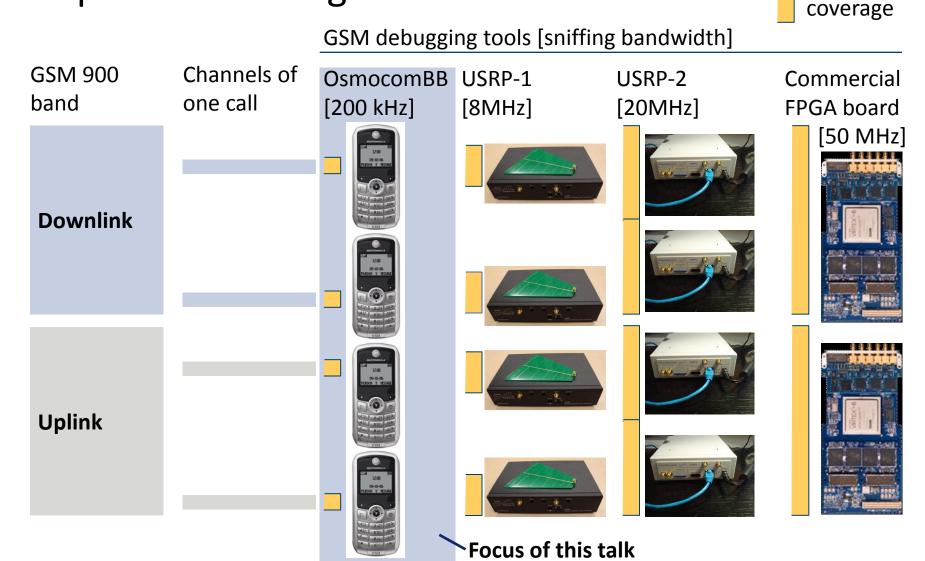
Down-

### GSM spectrum is divided by operators and cells

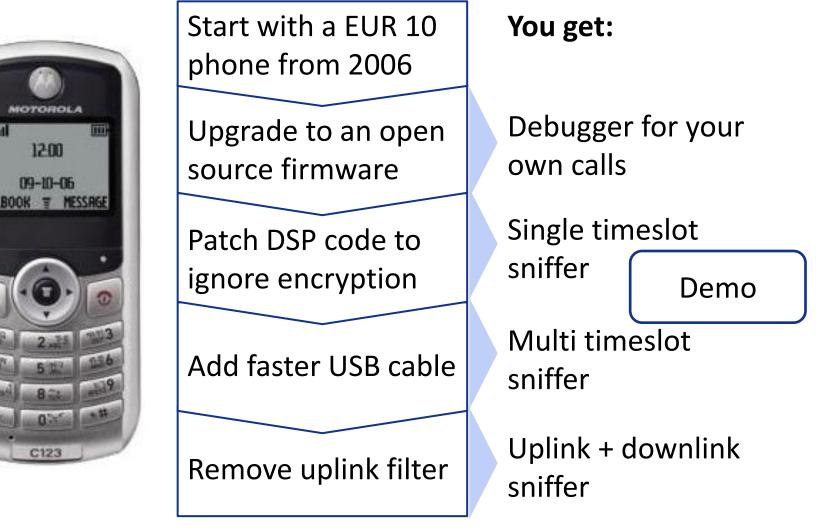


## GSM debugging tools have vastly different sepctrum coverage

Frequency



## Even reprogrammed cheap phones can intercept hopping calls



### Agenda

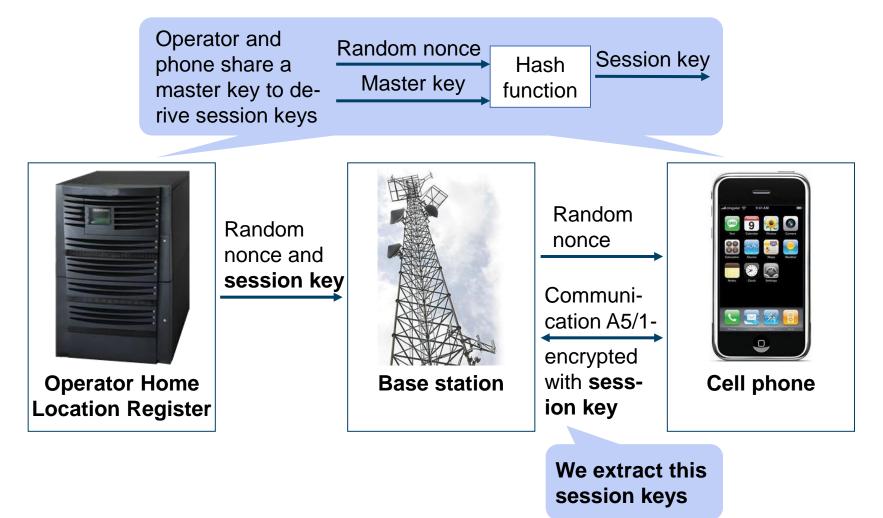
Locating a phone

Sniffing air traffic

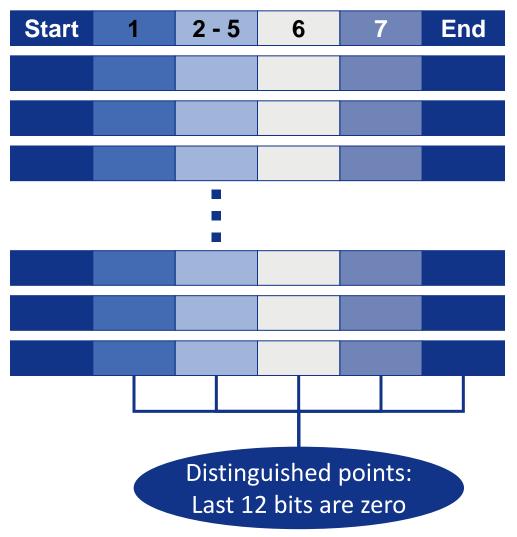
Cracking A5/1



## GSM uses symmetric A5/1 session keys for call privacy



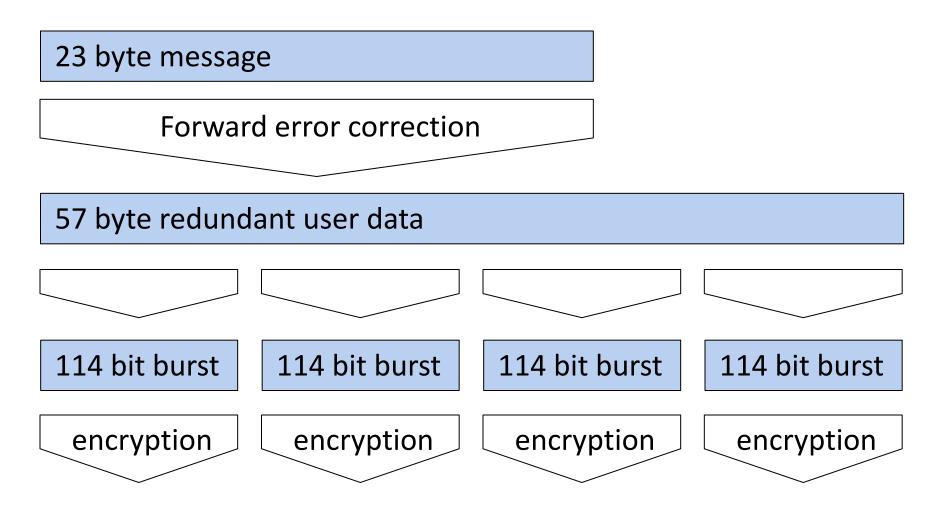
### A5/1's 64-bit keys are vulnerable to timememory trade-off attacks



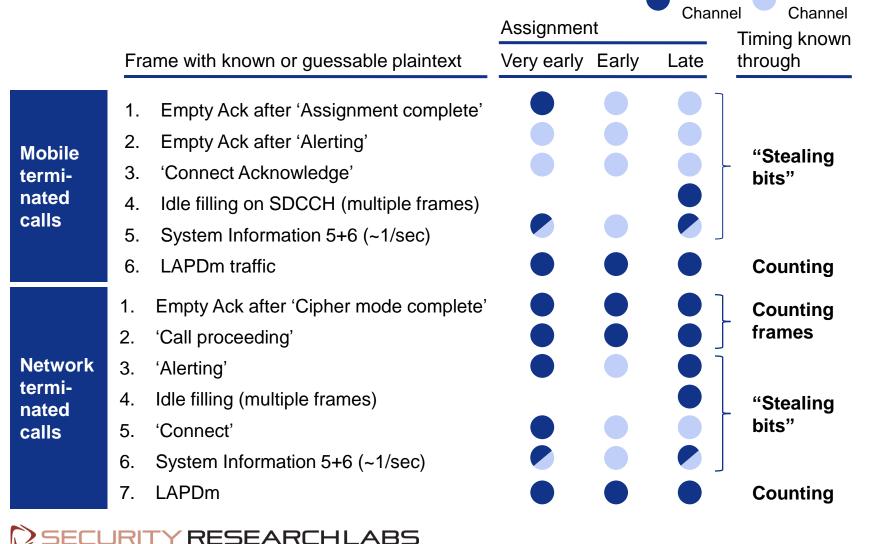
 A5/1 keys can be cracked with rainbow tables in seconds on a PC (details: 26C3's talk "GSM SRLY?")

 Second generation rainbow tables is available through Bittorrent

## GSM packets are expanded and spread over four frames



# Lots of GSM traffic is predictable providing known key stream



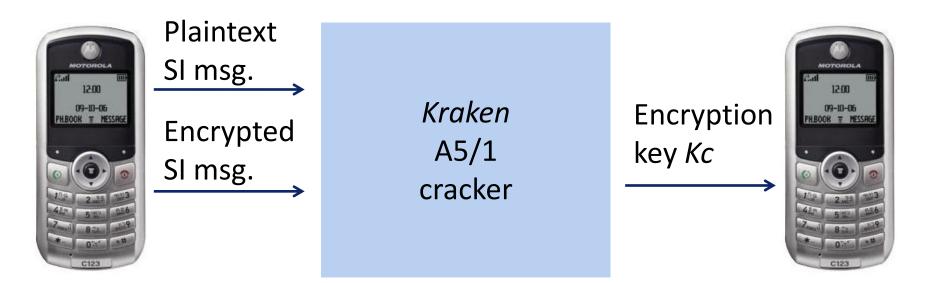
Source:GSM standards

Known

Unknown

# Two phones are enough for targeted intercept

Demo



Phone 1 records control messages for target TMSI(s)

Phone 2 hops on the same frequencies as target phone, records voice calls

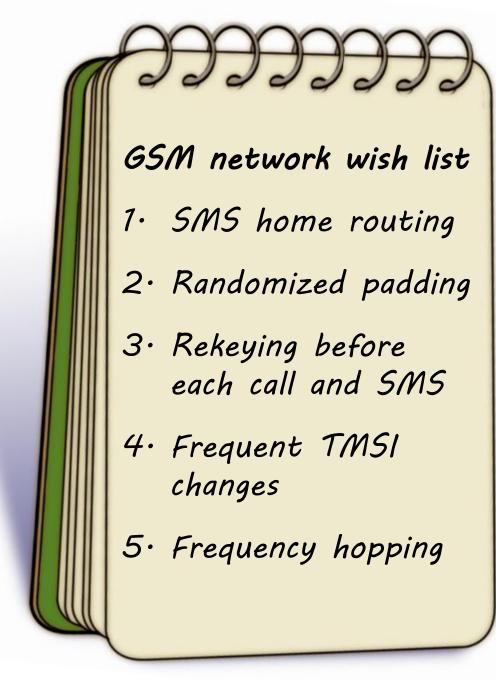


# Randomized padding makes control messages unpredictable to mitigate attacks

	SDCCH trace
238530	03 20 0d 06 35 11 <b>2b 2b 2</b>
238581	03 42 45 13 05 1e 02 ea 81 5c 08 11 80 94 03 98 93 92 69 81 <b>2b 2b</b>
238613	00 00 03 03 49 06 1d 9f 6d 18 10 80 00 00 00 00 00 00 00 00 00 00 00 00
238632	01 61 01 2b <b>2b 2b 2</b>
238683	01 81 01 2b <b>2b 2b 2</b>
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 <b>2b 2b 2</b>
238785	03 03 01 <b>2b 2b 2</b>

Padding in GSM has traditionally been predictable (2B) Every byte of randomized padding increasing attack cost by two orders of magnitude! Randomization was specified in 2008 (TS44.006) and should be implemented with high priority

Additionally needed: randomization of system information messages



# GSM should currently be used as an untrusted network, just like the Internet

Threat	Investment	Scope	Mitigation	
Fake base station	Low	Local	Mutual authenti- cation &	Cell phone
Passive intercept of voice + SMS	Low	Local	trust anchor	networks do not provide state-of-the art
Passive intercept of data	Currently not possible	_		security. Protection
Phone virus / malware	Medium to high	Large	Trust	must be embedded in the phones and
Phishing	High	Large	anchor	locked away from malware.

### **Questions?**



Rainbow tables, Airprobe, Kraken	srlabs.de
OsmocomBB firmware	osmocom.org
Karsten Nohl	nohl@srlabs.de

