29. VDE/ITG Fachtagung Mobilkommunikation, Osnabrück, 20 – 21 May 2025

A5/1 is in the Air: Passive Detection of 2G (GSM) Ciphering Algorithms

Matthias Koch, Christian Nettersheim, Thorsten Horstmann, Michael Rademacher

Fraunhofer FKIE

Hochschule Bonn-Rhein-Sieg University of Applied Sciences

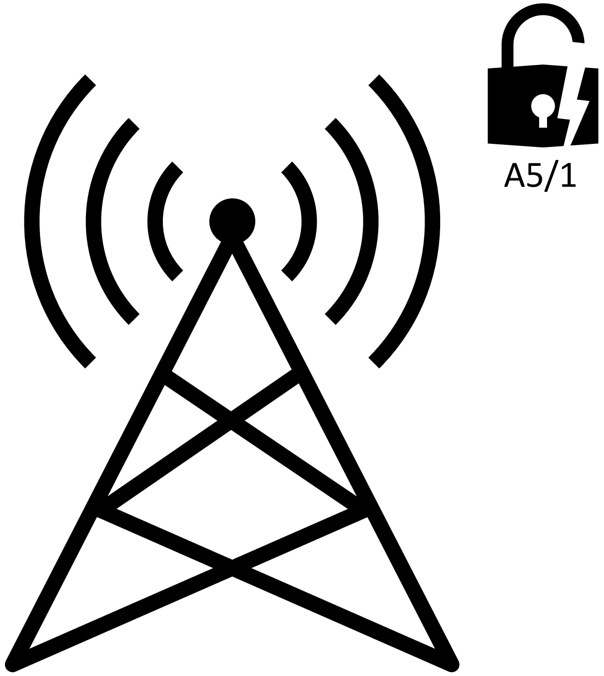
Motivation
2G is insecure

« 2G is insecure »

- Commonly accepted statement among security researchers

- Mostly because the cryptographic algorithm A5/1 is deemed broken
- Thus A5/1 is not in use anymore? Right?

How much A5/1 is still used
in today’s mobile networks in Germany?



Motivation

Relevance

Why is a mobile communications standard from the 1980s/90s still relevant today?

GSM is widely used (at least in Germany) and is still used for:

- Old phones
- (legacy) IoT devices
- Remote areas
- Fallback
- etc.

GSM is used by malicious actors for:

Destination for **4G/5G Downgrade-Attacks**

Hochschule Bonn-Rhein-Sieg University of Applied Sciences

Fraunhofer FKIE

GSM Encryption Overview

A5 Algorithm-Family

A5/0	A5/1	A5/2	A5/3	A5/4
No encryption	Stream Cipher	Prohibited by 3GPP	Block Cipher in Counter Mode	Block Cipher in Counter Mode
	64-bit key length		effective 64-bit key length	128-bit key length

- Designed in late 1980s
- Reverse engineered in 1990s
- Since 2010: Realtime session key recovery possible, vulnerable to rainbow table attacks

GSM Encryption Overview

MS Connection Procedure

Note: condensed high-level overview

1. BTS broadcasts *System Information* on Broadcast Common Control Channel (BCCH)
2. MS monitors nearby BCCHs and measures signal strength
3. MS selects BTS with strongest signal matching provider ID
4. MS and BTS establish signaling channel
5. MS triggers location update procedure via *Location Update Request*
   - Including *Mobile Station Classmark* message that contains the supported A5-algorithms
6. MS and network perform Ident & Auth
   - Session key is derived
7. Network selects ciphering algorithm and sends *Cipher Mode Command*
   - Including selected A5-algorithm
8. MS enables ciphering and sends encrypted *Cipher Mode Complete*
9. Procedure complete if network deciphers the message

GSM Encryption Overview

MS Connection Procedure

Note: condensed high-level overview

1. BTS broadcasts *System Information* on Broadcast Common Control Channel (BCCH)
2. MS monitors nearby BCCHs and measures signal strength
3. MS selects BTS with strongest signal matching provider ID
4. MS and BTS establish signaling channel
5. MS triggers location update procedure via *Location Update Request*
6. MS and network perform Ident & Auth
7. Network selects ciphering algorithm and sends *Cipher Mode Command*
8. MS enables ciphering and sends encrypted *Cipher Mode Complete*
9. Procedure complete if network deciphers the message

Including *Mobile Station Classmark* message that contains the supported A5-algorithms

Session key is derived

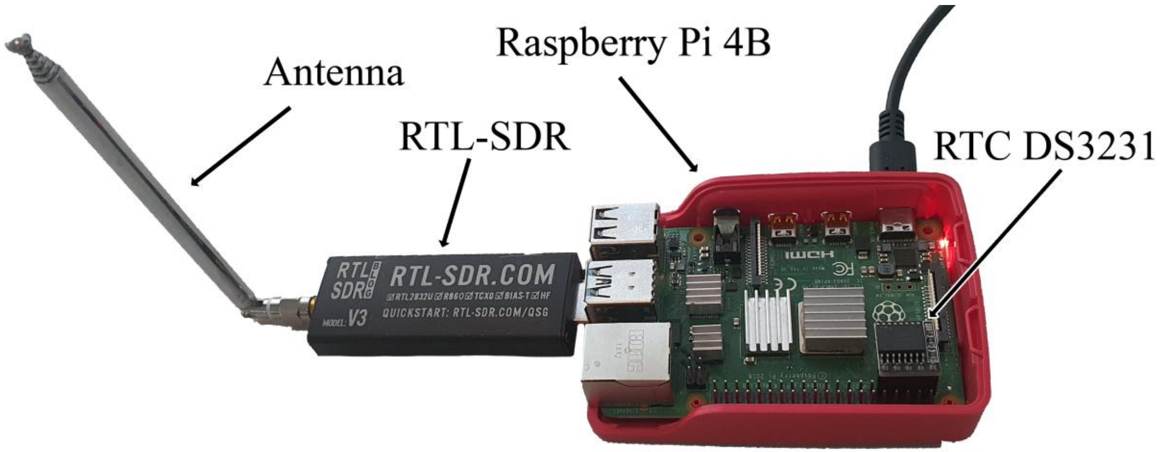
Including selected A5-algorithm

Methodology

Passive Monitoring

Sniffing for *Cipher Mode Command (CMC)* messages

SDR-based sensor	• COTS Hardware • Low-cost
Locking in GSM-Frequency for chosen provider	• GSM900 band • One sensor per provider
Sniffing GSM traffic	• Filtering for CMC-packages • Using *gr_gsm*
Measurement Points	• Tuple (timestamp, provider_id, algorithm)
Passive approach	• No active interaction with network required



Software and building guide:

https://github.com/mclab-hbrs/GSM-Cipher-Sensor

Methodology

Measuring campaign

10 locations

- Up to 3 sensors per location
- In and around Bonn
- Mix of rural, suburban and urban environments

3 German providers

- Pseudonymized as Provider A, B and C

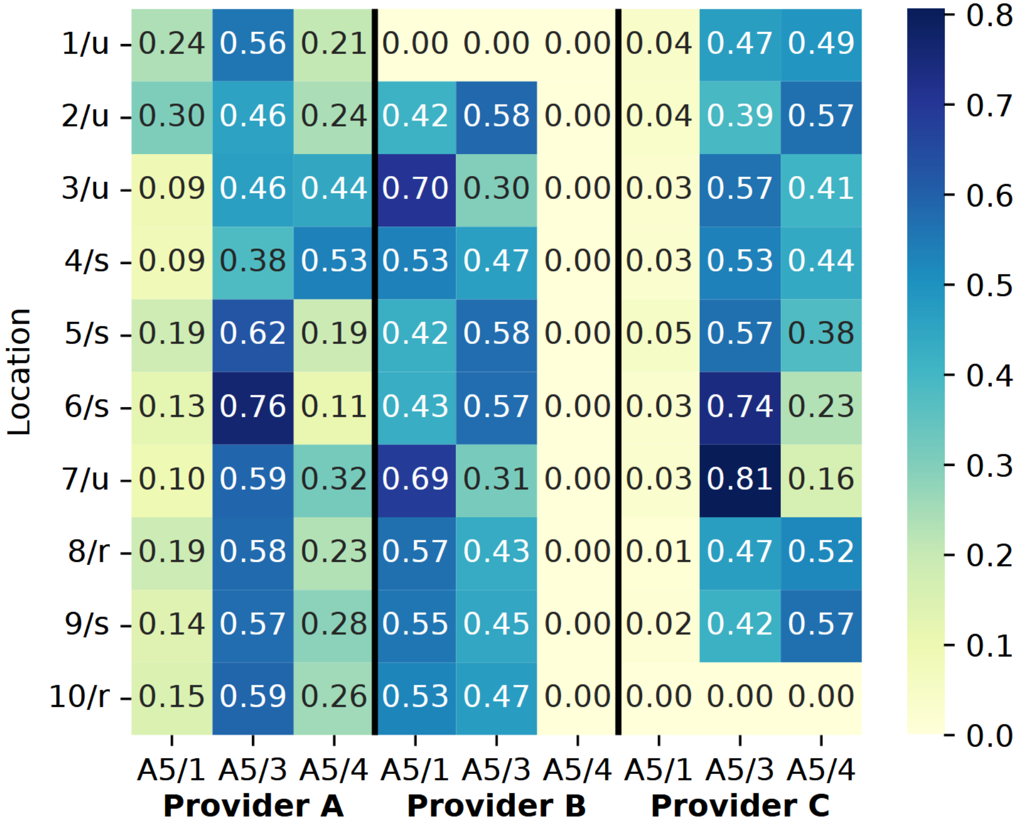
Short- and long-term measurements

565,115 CMCs analyzed

	Provider A		Provider B		Provider C	
Location	Days	#CMCs	Days	#CMCs	Days	#CMCs
1	2.67	418	0	0	3.02	6131
2	3.80	842	3.75	5669	3.77	8576
3	58.08	13852	42.95	212567	15.07	40438
4	35.76	34302	33.87	54477	18.29	54914
5	1.07	966	1.06	1945	1.06	2914
6	2.05	964	1.99	2238	3.45	9611
7	7.15	1756	7.46	11780	1.99	7454
8	4.75	1778	2.87	3999	2.87	50247
9	1.42	946	2.23	5186	2.27	9742
10	2.13	1189	3.72	20182	0	0

Results

Algorithm Usage by Provider



Usage rates of the algorithms per provider and per location.

Settlement type given by u = urban, s= suburban, r = rural

	A5/1	A5/3	A5/4
Provider A	16.1 %	55.8 %	28.1 %
Provider B	53.8 %	46.2 %	0 %
Provider C	3 %	55.1 %	41.8 %

Mean usage for each algorithm per provider

Provider A: Mixed, mostly A5/3

Provider B: Most A5/1, no A5/4

Provider C: Almost no A5/1

Results

Usage Patterns by Time

What is causing the traffic?

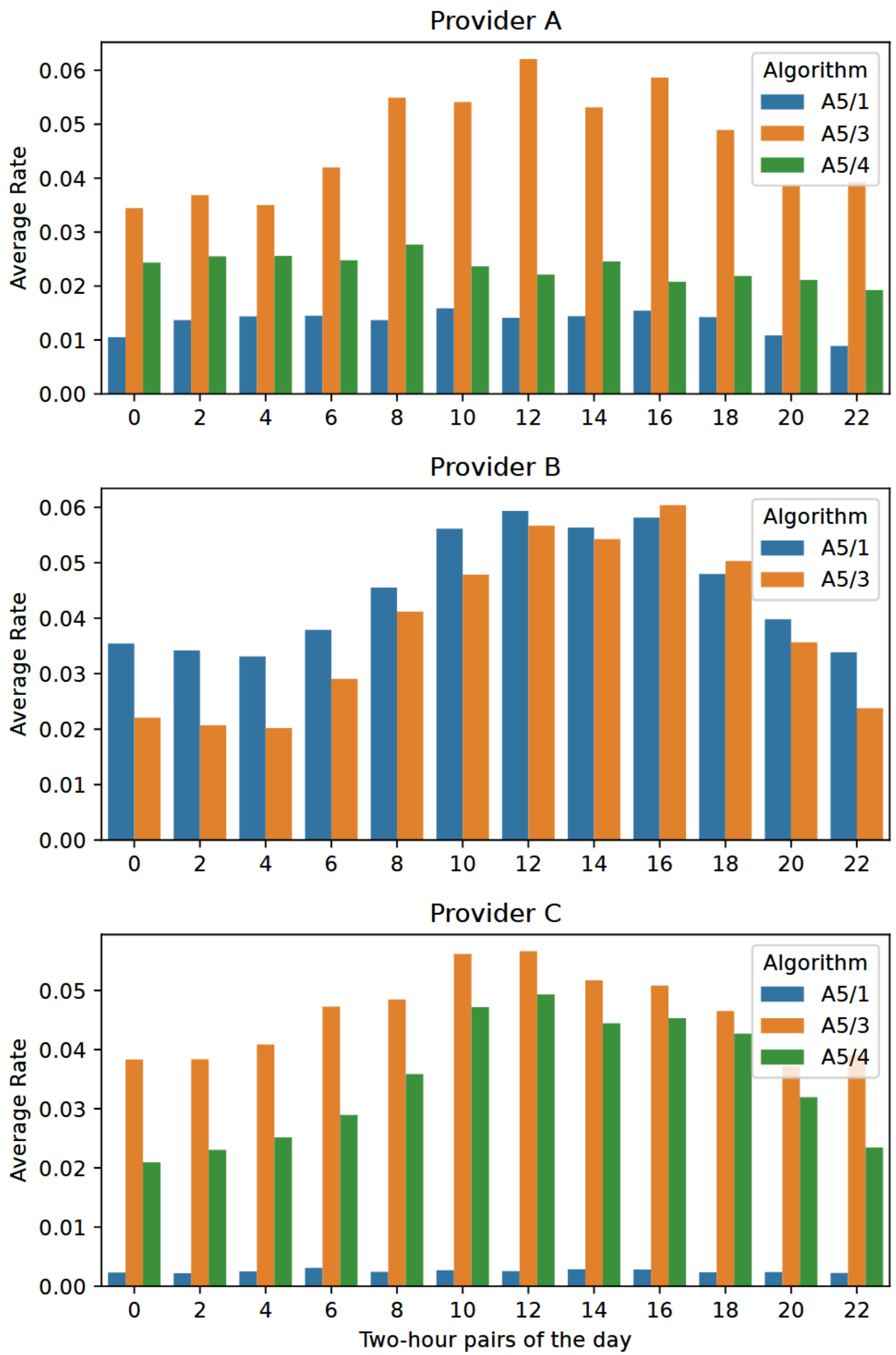
Very difficult to impossible to find out the source of the traffic

Usage over the course of a day can provide indications

Provider A
- A5/3 fits a „human daily routine“
- Unclear for A5/1 and A5/3

Provider B
- Graph seems „human“
- Traffic might be from humans or machines operated by humans

Provider C
- Human behavior for A5/3 and A5/4
- A5/1 probably IoT/sensor traffic



Fraunhofer FKIE

Security Implications

Outline of Example Attack

Smartphone is connected to public 4G network

↓

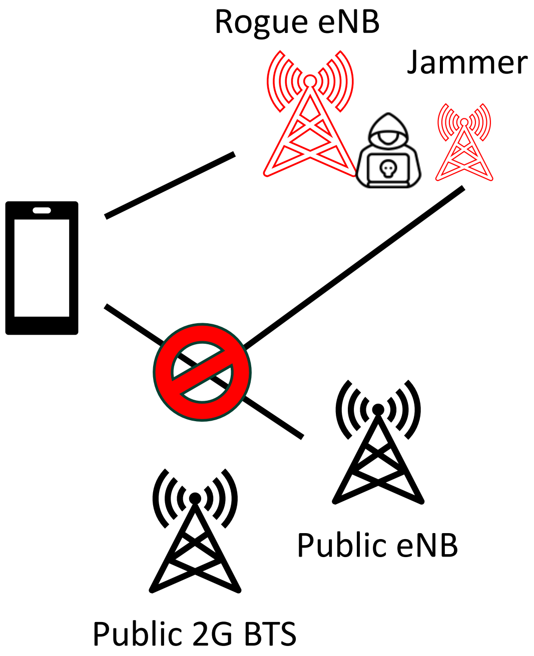
Attacker clones public base station (on parameter level)

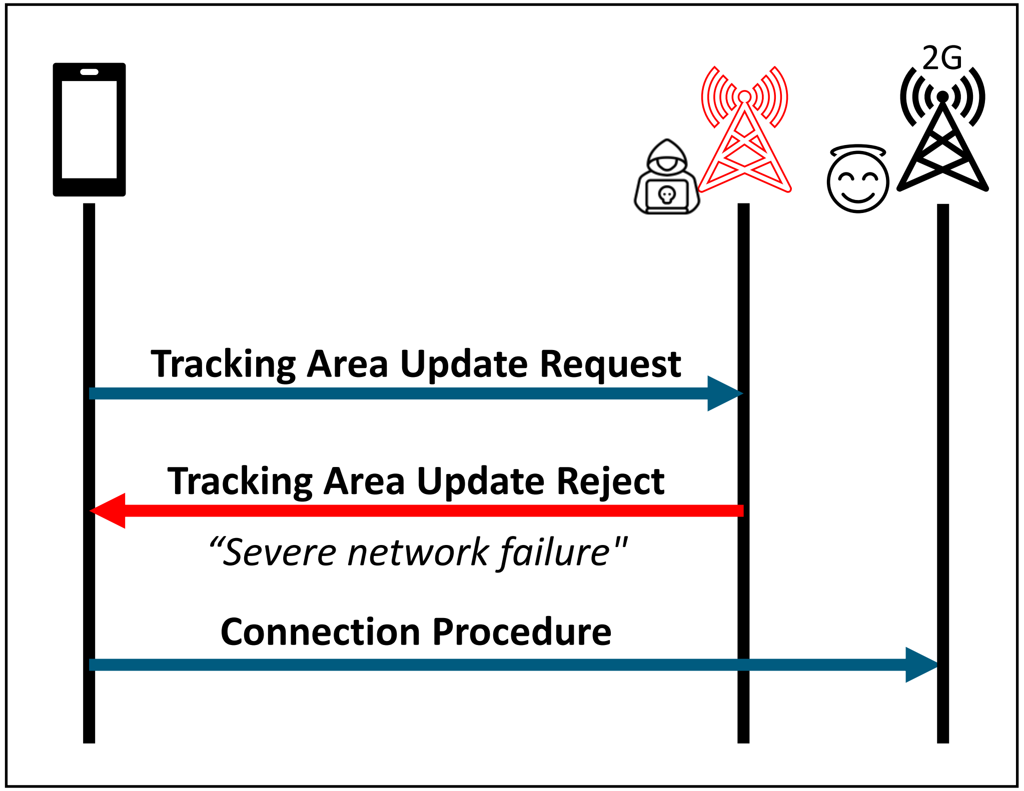
↓

Attacker forces smartphone to perform cell reselection

↓

Smartphone tries to perform TAU with rogue eNB → **Attacker sends TAU Reject**





Conclusion
And Open Questions

Key Findings

A5/1 is in the Air

- Despite deemed broken

Provider Discrepancies

- **Provider B** uses A5/1 in 53.8 %, while **Provider C** uses it in only 3 %
- IoT devices likely drive persistent A5/1 traffic for **Provider A** and **Provider C**

2G security research is still important

- While the technology is being used

Open Questions

Traffic Specific

- What causes the traffic?

Technical Challenges

- What barrier prevents providers from disabling A5/1?
  - Why do some providers prioritize backward compatibility over security?
- What barriers prevents **Provider B** from enabling A5/4?
  - Is the 2G networks that old and barely updated?

Hochschule Bonn-Rhein-Sieg University of Applied Sciences
Fraunhofer FKIE

Thanks for Your Kind Attention!

Contact

Christian Nettersheim
Mobile Communication Lab
https://mc-lab.de

Fraunhofer FKIE
Cyber Analysis & Defense
christian.nettersheim@fkie.fraunhofer.de

Hochschule Bonn-Rhein-Sieg
Institut für Sicherheitsforschung
christian.nettersheim@h-brs.de

Fraunhofer-Institut für Kommunikation,
Informationsverarbeitung und Ergonomie FKIE
Zanderstraße 5 | 53177 Bonn

https://fkie.fraunhofer.de

Hochschule Bonn-Rhein-Sieg
Grantham-Allee 20 | 53757 Sankt Augustin

https://h-brs.de