# GSM security country report: Germany

GSM Map Project
gsmmap@srlabs.de

Security Research Labs, Berlin

December 2013

**Abstract.** GSM networks differ widely in their protection capabilities against common attacks. This report details the protection capabilities of the four networks in Germany. We find T-Mobile to have implemented the most protection features and O2 to be the network offering the most attack surface in Germany.

Users of E-Plus, O2, and Vodafone are not sufficienty protected from interception.

Impersonating users of all of the networks is possible with simple tools.

O2 allows user tracking.

# Contents

# 1  Overview

| | Protection dimensions (higher means better) | | |
|---|---|---|---|
| **Operator** | Intercept | Impersonation | Tracking |
| E-Plus | 39% | 53% | 54% |
| O2 | 28% | 21% | 49% |
| T-Mobile | 59% | 58% | 89% |
| Vodafone | 41% | 44% | 90% |

Table 1: Implemented protection features relative to 2013 best practices (according to SRLabs GSM metric v2.2)

This document provides a security analysis of Germany's four GSM networks, based on data collected between January 2011 and December 2013. The analysis is based on data samples submitted to the GSM Map project[1]. It compares implemented protection features across networks.

The GSM Map website reports protection features condensed into three attack categories as shown in Table 1. This report details the logic behind the analysis results, lists some of the implemented protection features, and maps the protection capabilities to popular attack tools.

> **Disclaimer.** This report was automatically generated using data submitted to gsmmap.org by volunteers. (Thank you!) The analysis does not claim accuracy. Please do not base far-reaching decisions on the conclusions provided herein, but instead verify them independently.
> If you detect inaccuracies, we are looking forward to hearing from you.

---

[1]GSM Map Project: https://gsmmap.org

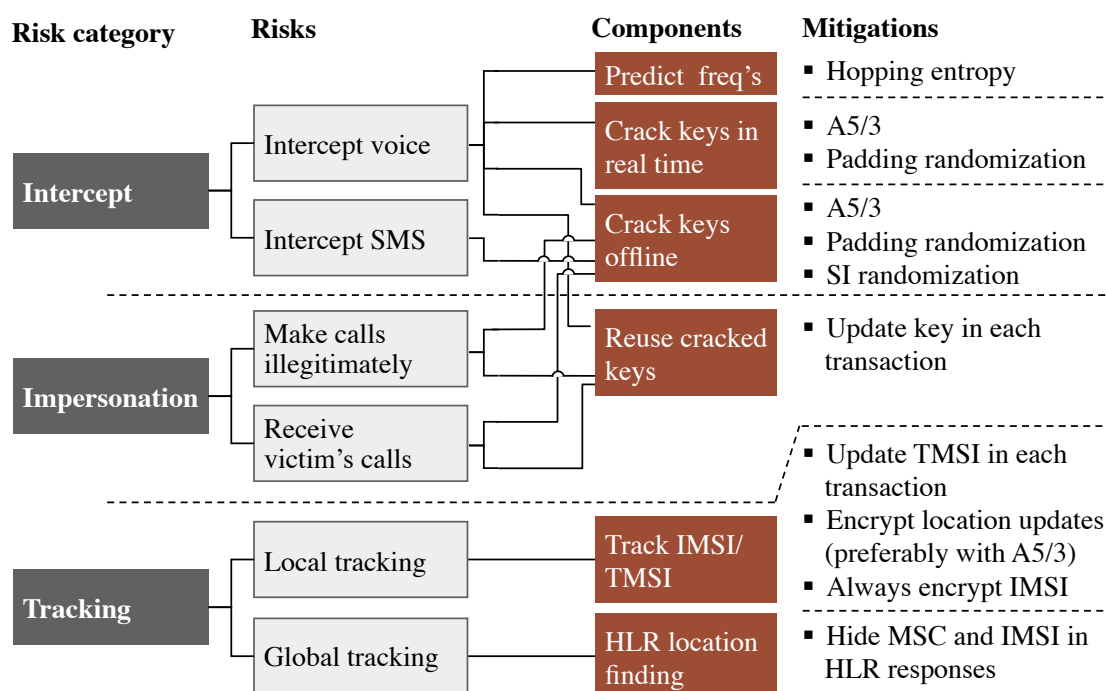| Risk category | Risks | Components | Mitigations |
|---|---|---|---|
| **Intercept** | Intercept voice / Intercept SMS | Predict freq's | ▪ Hopping entropy |
| | | Crack keys in real time | ▪ A5/3<br>▪ Padding randomization |
| | | Crack keys offline | ▪ A5/3<br>▪ Padding randomization<br>▪ SI randomization |
| **Impersonation** | Make calls illegitimately / Receive victim's calls | Reuse cracked keys | ▪ Update key in each transaction |
| **Tracking** | Local tracking | Track IMSI/TMSI | ▪ Update TMSI in each transaction<br>▪ Encrypt location updates (preferably with A5/3)<br>▪ Always encrypt IMSI |
| | Global tracking | HLR location finding | ▪ Hide MSC and IMSI in HLR responses |

Figure 1: Best practice GSM protection measures mitigate three attack scenarios.

# 2 Protection measures

The SRLabs GSM security metric is built on the understanding that GSM subscribers are exposed to three main risks:

- **Interception.** An adversary can record GSM calls and short messages from the air interface. Decryption can either be done in real time or as a batch process after recording transactions in bulk.

- **Impersonation.** Calls or SMS are either spoofed or received using a stolen mobile identity.

- **Tracking.** Mobile subscribers are traced either globally using Internet-leaked information or locally by repeated TMSI pagings.

The SRLabs metric traces these three risks and six sub-risks to an extensive list of protection measures, some of which are listed in Figure 1.

Table 2 details the implementation depth of some of the mitigation measures present in Germany's GSM networks.

# 3 Attack scenarios

The protection measures impact the effectiveness of various common GSM attack tools.

| Attack vector | | Networks | | | |
|---|---|---|---|---|---|
| | | E-Plus | O2 | T-Mobile | Vodafone |
| Over-the-air protection | | | | | |
| - Encryption algorithm | A5/1 | **100%** | **100%** | **91%** | **95%** |
| | A5/3 | 0% | 0% | 9% | 5% |
| - Padding randomization | | ◯ | ◯ | ◕ | ◯ |
| - SI randomization | | ◔ | ◯ | ◯ | ◯ |
| - Require IMEI in CMC | | ◔ | ◯ | ● | ◕ |
| - Hopping entropy | | ◐ | ◐ | ◐ | ◐ |
| HLR/VLR configuration | | | | | |
| - Authenticate calls | | ◐ 49% | ◔ 13% | ◔ 21% | ◔ 11% |
| - Authenticate SMS | | ◐ 40% | ◯ 8% | ● 99% | ● 97% |
| - Authenticate LURs | | ◔ 28% | ◔ 23% | ◔ 31% | ◐ 55% |
| - Encrypt LURs | | ● 100% | ● 100% | ● 100% | ● 100% |
| - Update TMSI | | ◕ | ◐ | ◕ | ◕ |
| - Mask MSC | | ◯ | ◯ | ● | ● |
| - Mask IMSI | | ◑ | ◑ | ◑ | ◑ |

Table 2: Protection measures implemented in analyzed networks, compared to best practice references observed in 2013.

## 3.1 Passive intercept

Passive interception of GSM calls requires two steps: First, all relevant data needs to be intercepted. This step can not be prevented completely, but aggravated significantly by using less predictable frequency hopping sequences. All of the networks use such less predictable hopping sequences. Secondly, the intercepted call and SMS traces need to be decrypted. This can be prevented by hardening the A5/1 cipher or by upgrading to modern encryption algorithms.

**Hardening the A5/1 cipher** . The A5/1 cipher was developed in 1987 and is still by far the most common encryption algorithm for GSM calls. First weaknesses of this cipher were discussed in 1994[2], but it took until the mid-2000's until successfull attacks on GSM were demonstrated publicly. These attacks exploit (partially) known plaintexts of the encrypted GSM messages to derive the encryption key. Consequently, countermeasures need to reduce the number of predictable bits in GSM frames.

Nowadays, several generations of passive A5/1 decipher units exist, that attack different parts of the transaction. Early generation boxes attack the Cipher Mode Complete message. T-Mobile generally protects from these boxes. O2 is fully vulnerable (*Require IMEI in CMC*).

---

[2]See https://groups.google.com/forum/#!msg/uk.telecom/TkdCaytoeU4/Mroy719hdroJ

More modern decipher units leverage predictable Null frames. These Null frames contain little to no relevant information and are filled up with a fixed uniform padding, facilitating known-plaintext attacks. T-Mobile offers no attack surface through predictable null frames. E-Plus, O2, and Vodafone are particularly prone to this type of attack.

Recently updated boxes further leverage System Information (SI) messages. These messages can be randomized, or not sent at all during encrypted transactions *SI randomization*. O2, T-Mobile, and Vodafone have deployed no protection against this type of attack.

**Upgrading to modern encryption algorithms.** With the introduction of third generation mobile telecommunications technology, the A5/3 cipher was introduced. Only few theroretical attacks on this cipher were so far presented publicly, none of which had practical significance.

Modern 3G phones can use this cipher for GSM communication as well, if the network supports it. With passive intercept being prevented, attackers must then use active intercept equipment, e.g. fake base stations, as described in Section 3.2. T-Mobile and Vodafone have begun rolling out A5/3 in their network. To intercept T-Mobile and Vodafone subscribers in A5/3-enabled areas, attackers will need to use active equipment. In Germany, E-Plus, O2, and Vodafone continue to fully rely on the outdated A5/1.

## 3.2 Active intercept

Attacks through fake base stations can be prevented to different degrees, based on what the fake base station is used for:

- Location finding: In this attack scenario, a phone is lured onto a fake station so that the phone's exact location can be determined. This scenario occurs independent from the phone network and hence cannot be prevented through network protection measures.

- Outgoing call/SMS intercept: A fake base station can proxy outgoing connections. In this attack, the network is not necessarily required, so no protection can be achieved from outside the phone.

- Encrypted call/SMS intercept: Modern fake base stations execute full man-in-the-middle attacks in which connections are maintained with both the phone and the real network.

Networks can make such active attacks more difficult with a combination of two measures:

First, by disabling unencrypted A5/0 calls. Secondly, by decreasing the authentication time given to a the attacker to break the encrytion key. This timeout can be as much as 24 seconds according to GSM standards. All of the networks use encryption in all call and SMS transactions; however, the GSMmap currently lacks data to decide whether the networks would accept unencrypted transactions as well.

The GSM Map database currently lacks reliable data on authentication times in Germany.

## 3.3  Impersonation

Mobile identities can (temporarily) be hijacked using specific attack phones. These phones require the authentication key deciphered from one transaction. They use this key to start a subsequent transaction. The obvious way to prevent this attack scenario is by requiring a new key in each transaction (*Authenticate calls/SMS*).

In Germany, call impersonation is possible against all of the networks. SMS impersonation is possible against E-Plus and O2.

## 3.4  User tracking

GSM networks are regularly used to track people's whereabouts. Such tracking occurs at two different granularities:

- Global tracking: Internet-accessible services disclose the general location of GSM customers with granularity typically on a city level. The data is leaked to attackers as part of SMS delivery protocols in form of the MSC address (*Mask MSC*). T-Mobile and Vodafone suppress MSC information for their customers in Germany. E-Plus and O2 allow MSC-based tracking. In addition, user's IMSI's can leak in HLR requests. All of the networks protect this information. All of the networks blocked the queries for IMSI in HLR responses from the test service used for this report, but may still disclose more information to requesters not on the black list.

- Local tracking: Based on TMSI identifiers, users' association with location areas and specific cells can be tracked, providing a finer granularity than MSC-based tracking, but a less fine granularity than location finding with the help of fake base stations. IMSI-based tracking is made more difficult by changing the TMSI in each transaction. E-Plus, T-Mobile, and Vodafone have implemented this feature, O2 has not (*Update TMSI*). In some countries, unencrypted location updates can be observed that ease the tracking of users; all of the networks show this behavior (*Encrypt LocUpdate*).

# 4 Conclusion

The GSM networks in Germany implement only few of the protection measures observed in other GSM networks.

T-Mobile and Vodafone are protecting their subscribers particularly well against tracking.

The evolution of mobile network attack and defense techniques is meanwhile progressing further: Modern A5/1 deciphering units are harvesting the remaining non-randomized frames and – thanks to faster computers – are achieving high intercept rates again.

The 3GPP, on the other hand, already completed standard extensions to reduce A5/1 attack surface to a minimum. These standards from 2009 are only hesitantly implemented by equipment manufacturers, leaving users exposed to phone intercept risks.

The available protection methods – even when implemented in full – are barely enough to protect users sufficiently. At the same time, mobile phone attacks are becoming increasingly attractive. A stronger push for implementing modern protection measures is needed to revert this erosion of mobile network security.