GSM security country report: USA

GSM Map Project
gsmmap@srlabs.de

Security Research Labs, Berlin

August 2013

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

None of the networks sufficiently protect against intercept attacks.

In all networks, user impersonation is possible with simple tools.

All networks allow user tracking.

Contents

1 Overview

	Protection dimensions (higher means better)		
Operator	Intercept	Impersonation	Tracking
AT&T	◑ 46%	◔ 30%	◑ 43%
T-Mobile	◑ 41%	◔ 27%	◔ 20%

Table 1: Implemented protection features relative to 2014 best practices (according to SRLabs GSM metric v2.4)

This document provides a security analysis of the USA's two GSM networks, based on data collected between June 2013 and August 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 dimensions 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

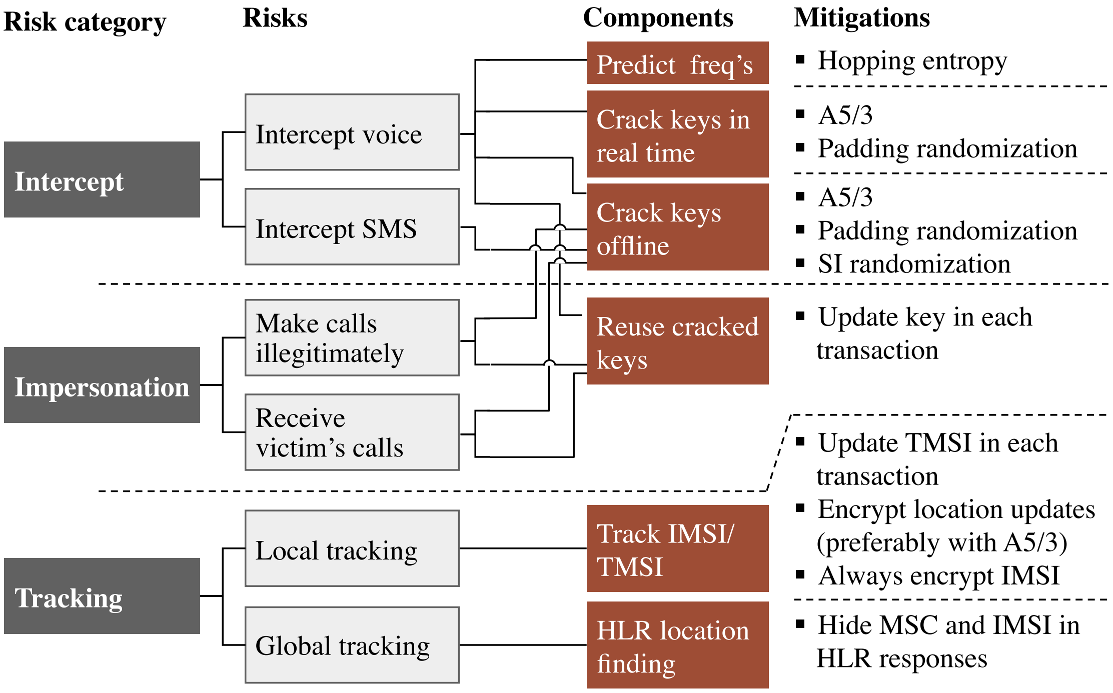

Figure 1: Best practice GSM protection measures can mitigate three attack scenarios.

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 records GSM calls and SMS from the air interface. Decryption can 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 the USA's GSM networks.

Attack vector		Networks	
		AT&T	T-Mobile
Over-the-air protection			
- Encryption algorithm	A5/1	**100%**	**100%**
- Padding randomization		○	○
- SI randomization		○	○
- Require IMEI in CMC		●	●
- Hopping entropy		◔	◑
HLR/VLR configuration			
- Authenticate calls (MO)		○ 0%	○ 8%
- Authenticate SMS (MO)		○ 1%	○ 5%
- Authenticate paging (MT)		○ 1%	○ 4%
- Authenticate LURs		● 96%	◔ 19%
- Encrypt LURs		● 100%	● 91%
- Update TMSI		◔	◔
- Mask MSC		●	●
- Mask IMSI		○	○

Table 2: Protection measures implemented in analyzed networks, compared to best practice references observed in 2014.

3 Attack scenarios

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

3.1 Passive intercept

Passive intercept of GSM calls requires two steps: First, all relevant data needs to be intercepted. This step cannot be prevented completely, but aggravated significantly by using less predictable frequency hopping sequences. T-Mobile uses 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

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

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. All networks generally protect from these boxes.

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. None of the networks in USA have deployed protection against 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*). None of the networks in USA are protected 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 theroretical attacks on this cipher were so far presented publicly, none of which had practical significance.

Modern phones can use this cipher for GSM communication, 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. In the USA, all networks continue to mostly rely on outdated encryption.

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 12 seconds according to GSM standards. All 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 the USA.

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 the USA, call impersonation is possible against all networks. The same is true for all SMS messages in USA.

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*). All networks suppress MSC information for their customers in the USA. In addition, users' IMSI's can leak in HLR requests. This is the case for all networks.

- 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 (*Update TMSI*). All networks have not addressed this threat thoroughly.

4 Conclusion

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

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.