Mobile network security report: Russia

GSM Map Project
gsmmap@srlabs.de

Security Research Labs, Berlin

August 2019

Abstract. Mobile networks differ widely in their protection capabilities against common attacks. This report details the protection capabilities of four mobile networks in Russia.
All 3G networks in Russia implement sufficient 3G intercept protection.
MTS 2G users are predominantly using latest encryption technology. Impersonating 2G users of MTS is possible with simple tools. MTS allows user tracking.

Contents

1 Overview

		Protection dimension (higher means better)		
Operator		Intercept	Impersonation	Tracking
MTS	2G	53%	35%	13%
	3G	92%	–	
Beeline	3G	91%	–	
MegaFon	3G	89%	–	
Tele2	3G	93%	–	

Table 1: Implemented protection features relative to 2014 best practices (according to SRLabs GSM metric v2.5)

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.

This document provides a security analysis of Russia's four mobile networks, based on data collected between December 2011 and August 2019. 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.

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

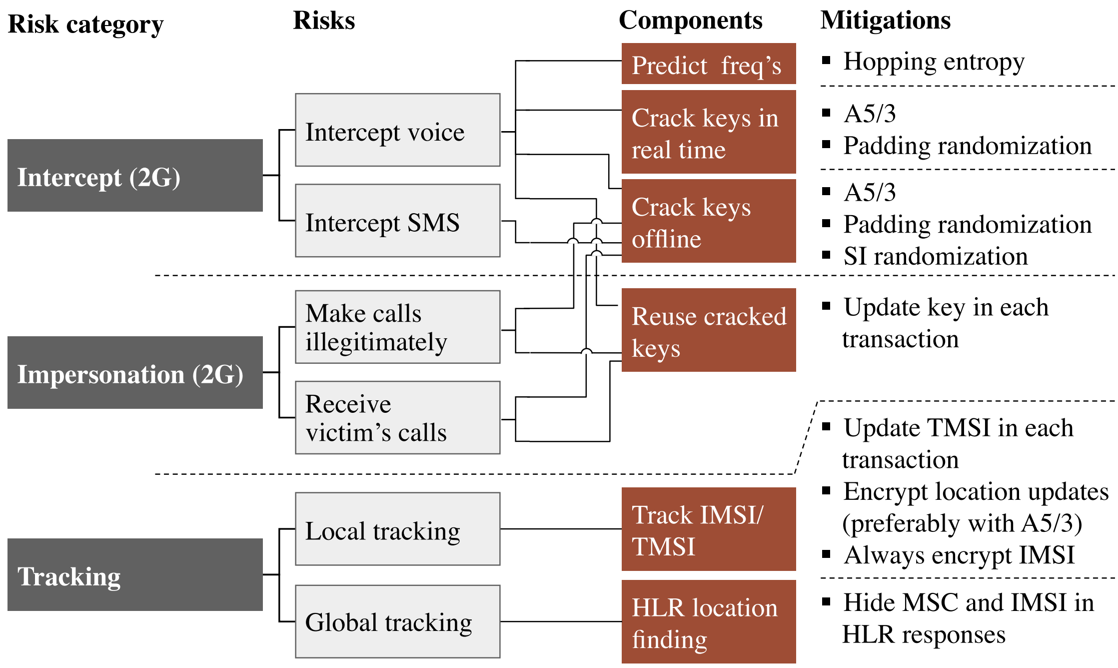

Figure 1: Best practice protection measures can mitigate three attack scenarios.

2 Protection measures

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

- **Intercept.** An adversary records 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 to an extensive list of protection measures, some of which are listed in Figure 1. For 3G networks, GSMmap currently assesses intercept protection only. We understand that that the mandatory integrity checking in 3G protects from simple impersonation attacks. Table 2 details the implementation depth of some of the mitigation measures present in Russia's mobile networks.

Attack vector		Networks			
		MTS	Beeline	MegaFon	Tele2
2G Over-the-air protection					
- Encryption algorithm	A5/0	2%			
	A5/1	43%			
	A5/3	**55%**			
- Require IMEI in CMC		◑			
- Hopping entropy		◔			
- Authenticate calls (MO)		◔ 17%			
- Authenticate SMS (MO)		◔ 14%			
- Authenticate paging (MT)		◔ 14%			
- Authenticate LURs		◔ 28%			
- Encrypt LURs		● 100%			
- Update TMSI		◔ 32%			
3G Over-the-air protection					
- Encryption		●	●	●	●
- Update TMSI		◔ 15%	○ 6%	○ 3%	◔ 32%
HLR/VLR configuration					
- 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 common mobile network attack tools.

3.1 Passive intercept

Passive 2G intercept requires two steps: First, all relevant data needs to be intercepted. This step cannot be prevented completely, but made more difficult by using less predictable frequency hopping sequences. Regular rotation of the TMSI makes it harder to target a phone for intercept (*Update TMSI*).
Secondly, the intercepted call and SMS traces need to be decrypted. In 2G networks, this can be prevented by hardening the A5/1 cipher or by upgrading to modern encryption algorithms. Currently, there is no publicly known cryptanalytic attack against the Kasumi cipher used by the

A5/3 encryption algorithm. All 3G networks in Russia use this encryption algorithm.

Hardening the A5/1 cipher . The A5/1 cipher was developed in 1987 and is still the most common encryption algorithm for 2G calls. First weaknesses of this cipher were discussed in 1994[2], but it took until the mid-2000's until successfull attacks on 2G 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 2G frames.

Nowadays, several generations of passive A5/1 decipher units exist, that attack different parts of the transaction. Early generations attack the Cipher Mode Complete message.

More modern decipher units leverage predictable Null frames. These frames contain little to no relevant information and are filled up with a fixed uniform padding, facilitating known-plaintext attacks. These attacks can be prevented by using an unpredictable padding (*Padding randomization*). Recently updated intercept boxes further leverage System Information (SI) messages. These messages can be randomized, or not sent at all during encrypted transactions (*SI randomization*).

The randomization values cannot currently be measured using the SnoopSnitch software since the underlying Qualcomm chipsets do not disclose this level of information. We will continue to look for alternative measurement sources, but cannot currently measure whether networks in Russia use randomization.

Upgrading to modern encryption algorithms. With the introduction of 3G mobile telecommunications technology, the A5/3 cipher was introduced to 2G. Only theoretical attacks on this cipher were so far presented publicly, none of which have practical significance. Modern phones can use this cipher for 2G communication, if the network supports it. MTS enabled A5/3 for the majority of their customers. To intercept subscribers of MTS in A5/3-enabled areas, attackers will need to use active equipment. All 3G networks in Russia encrypt relevant transactions.

With passive intercept being prevented, attackers must use active intercept equipment, e.g. fake base stations, as described in Section 3.2.

3.2 Active intercept

Attacks through fake 2G 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 of 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, connectivity to the real network is not necessarily required, so no protection can be achieved from outside the phone.

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

- 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 not allowing unencrypted calls. Secondly, by decreasing the authentication time given to an attacker to break the encryption key. This timeout can be as much as 12 seconds according to common standards. The GSM Map database currently lacks reliable data on authentication times in Russia. However, the GSMmap currently lacks data to decide whether the networks would accept subscriber-originated unencrypted transactions.

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 Russia, 2G call impersonation is possible against MTS. The same is possible for SMS messages from MTS.

3G networks are generally protected from this type of impersonation attacks.

3.4 User tracking

Mobile 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*). MTS allows MSC-based tracking. In addition, users' IMSI's can leak in HLR requests. This is the case for MTS.
- 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*). MTS has not addressed this threat thoroughly.

4 Conclusion

The mobile networks in Russia implement only few of the protection measures observed in other networks.

MTS has begun upgrading their network to the more secure A5/3 encryption algorithm.

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. A stronger push for implementing modern protection measures is needed to revert this erosion of mobile network security.