Mobile network security report: Poland

GSM Map Project
gsmmap@srlabs.de

Security Research Labs, Berlin

August 2016

Abstract. Mobile networks differ widely in their protection capabilities against common attacks. This report details the protection capabilities of four mobile networks in Poland.
All 3G networks in Poland implement sufficient 3G intercept protection.
Some popular passive 2G intercept devices will not work against Orange, Plus, and T-Mobile. Impersonating 2G users of Orange, Play Mobile, and Plus is possible with simple tools. Plus allows user tracking.

Contents

1 Overview

		Protection dimension (higher means better)		
Operator		Intercept	Impersonation	Tracking
Orange	2G	61%	64%	68%
	3G	92%	–	
Play Mobile	2G	58%	36%	54%
	3G	99%	–	
Plus	2G	64%	48%	31%
	3G	92%	–	
T-Mobile	2G	69%	71%	85%
	3G	90%	–	

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 Poland's four mobile networks, based on data collected between December 2011 and August 2016. The analysis is based on data samples submitted to the GSM Map project[1]. It compares implemented protection features across networks.

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

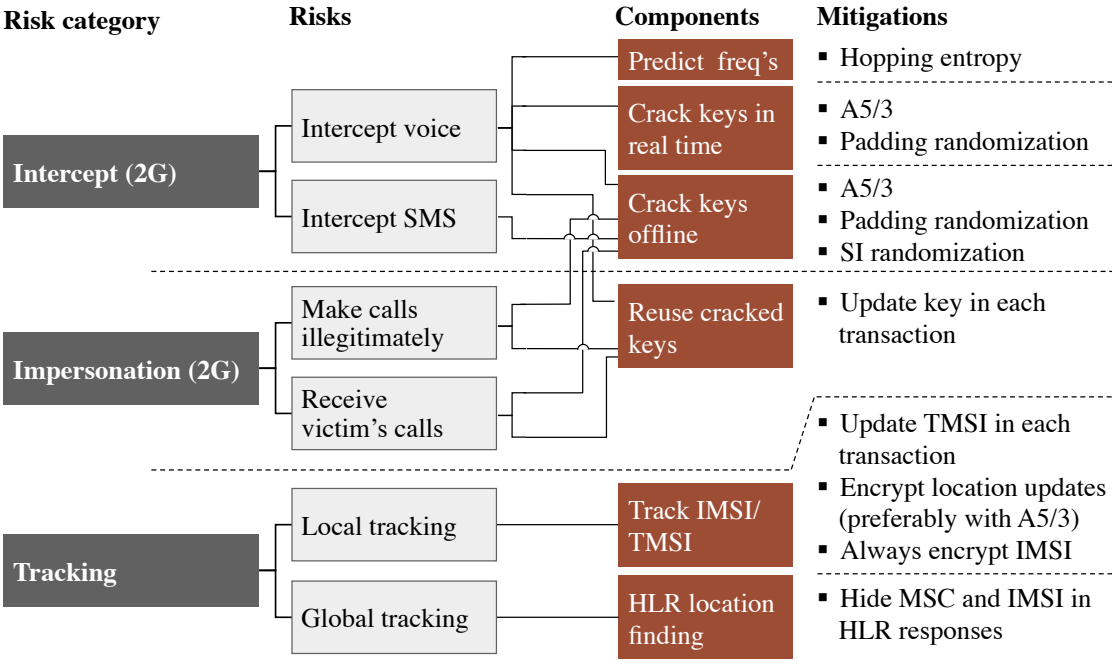

Figure 1: Best practice protection measures can mitigate three attack scenarios.

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.

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 Poland's mobile networks.

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. All 2G networks in Poland use such less predictable hopping sequences. Regular rotation of the TMSI makes it harder to target a phone for intercept (*Update TMSI*). Play Mobile has implemented a particularly high TMSI rotation rate in the 3G network.

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 common 3G encryption algorithm, A5/3. All 3G networks in Poland 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. Play Mobile and Plus are fully vulnerable (*Require IMEI in CMC*).

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*). None of the networks in Poland have deployed protection against this type of attack.

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*). None of the networks in Poland are protected against this type of attack.

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. Orange, Plus, and T-Mobile have begun rolling out A5/3. To intercept subscribers of Orange, Plus, and T-Mobile in A5/3-enabled areas, attackers will need to use active equipment. In Poland, Orange and Play Mobile continue to mostly rely on outdated encryption.

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

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

Using USIM cards. While A5/1 and A5/3 in 2G operate on a key length of only 64 bits, the 3G encryption algorithm relies on a key length of 128 bits. To benefit from the increased 3G attack complexity, subscribers need to use SIM cards that feature 128bit key generation, also called USIMs. When GSM SIM cards are used instead, the key entropy is limited to 64bits, resulting in vastly reduced attack complexity. Orange and Play Mobile predominantly use USIM cards with 128bit keys. GSMmap currently lacks data on USIM prevalence for Plus and T-Mobile.

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.
- 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 Poland. Orange, Play Mobile, and Plus use encryption in all 2G call and SMS transactions. All 3G networks in Poland encrypt relevant transactions. 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 Poland, 2G call impersonation is possible against all 2G networks in Poland. The same is possible for SMS messages from Play Mobile and Plus.

3G networks are generally protected against 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*). All 2G networks in Poland suppress MSC information for their customers in Poland. In addition, users' IMSI's can leak in HLR requests. This is the case for Play Mobile and Plus. Orange and T-Mobile protect this information.
- 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*). Orange and Play Mobile have implemented this feature. Plus and T-Mobile have not addressed this threat thoroughly.

4 Conclusion

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

Plus and T-Mobile have begun upgrading their network to the more secure A5/3 encryption algorithm. Orange and T-Mobile 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. A stronger push for implementing modern protection measures is needed to revert this erosion of mobile network security.

Attack vector		**Networks**			
		Orange	Play Mobile	Plus	T-Mobile
2G Over-the-air protection					
- Encryption algorithm	A5/0	0%	0%	0%	1%
	A5/1	**99%**	**100%**	**68%**	**62%**
	A5/3	1%	0%	32%	37%
- Padding randomization		○	○	○	○
- SI randomization		○	○	○	○
- Require IMEI in CMC		◑	○	◔	◑
- Hopping entropy		◑	◕	◕	◑
- Authenticate calls (MO)		◕ 80%	○ 8%	◑ 38%	◕ 71%
- Authenticate SMS (MO)		● 97%	◔ 10%	◔ 34%	● 93%
- Authenticate paging (MT)		◔ 27%	○ 9%	◔ 26%	◕ 68%
- Authenticate LURs		◕ 76%	◑ 38%	● 94%	◑ 57%
- Encrypt LURs		● 100%	● 100%	● 100%	● 100%
- Update TMSI		◑ 53%	● 97%	◔ 27%	◔ 25%
3G Over-the-air protection					
- Encryption		●	●	●	●
- Update TMSI		◔ 21%	● 91%	◔ 17%	○ 3%
- USIM usage		●	●	–?–	–?–
HLR/VLR configuration					
- Mask MSC		◑	●	◑	●
- Mask IMSI		●	○	○	●

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