WHITEPAPER

CYBERSECURITY

SMS DOESN´T STAND FOR SECURE MESSAGING SERVICE:

SMS (IN)SECURITY REVISITED

DEKRA

Authors

Anders Olof Möller
Fernando González Trigo
Julio Negueruela Palomo
Juan Jurado Cuesta

Contact

Anders Olof Möller
anders.olofmoller@dekra.com

Antonio Vizcaíno Gómez
antoniodavid.vizcaino@dekra.com

Want to know more? Visit our website or get in touch with our Experts!

About Digital & Product Solutions

Innovating safety and security by creating the intelligent testing solutions that contribute to making the digitalized and connected world a safer place. We are the experts in testing and certifying products and new digital technologies.
We deliver solutions from Cybersecurity, Artificial Intelligence, Big Data, to Connectivity, Product Safety, Electromagnetic Compatibility & Radiofrequency, Product Certification, Medical Devices and Automotive Testing.
Through a global network of 48 state-of-the-art test laboratories and facilities, we offer a broad portfolio of product testing services based on national and international standards as well as industry and customer requirements.

www.dekra-dps.com

SMS, Short Message Service, is an extremely successful communication service for text messages between mobile devices that was introduced in the early 1990s. Behind its success is the simplicity, reliability and the possibility to communicate with almost any mobile device in the world. It is commonly used for a large number of different applications including personal and business communication, service alerts, second factor authentication and increasingly also between applications. However, SMS security has severe limitations. For example, texts sent via SMS have no built-in encryption and authentication. Further, while SMS is a good option for some use cases, there are more secure options for others. This includes secure communications and second factor authentication. In this paper, security threats against SMS from a user perspective are analyzed.

1 Executive summary and outline of paper

Figure 1 Sending Basic SMS over a mobile network.

The SMS functionality was first developed as a part of the Global System for Mobile Communications (GSM) standard more than 30 years ago and has since its introduction been included also in the following generations of mobile networks [1]. When the SMS protocol was introduced, the security aspects were not as critical as they are today. Since then, the technology and threat landscape has evolved considerably, while the security of SMS is still dependent on the legacy security principles used when it was first designed. As a comparison, there are many modern communication applications that implement state-of-the-art end-to-end security with methods that are appropriate for the modern threat landscape.

A conclusion in this paper is that the SMS protocol cannot guarantee the basic security properties typically requested by a user of a message service. This includes the confidentiality, integrity and authenticity of the messages. Instead, the user places its trust in the security of the radio access, in the security of the network and in the secure management of the user data by the operator. These trust assumptions can typically neither be verified by the user, nor be detected if they are violated.

Related to the user trust assumptions there are vulnerabilities that can be exploited by attackers and a review of reported attacks shows that attacks are being executed in real networks. Examples of this include SMS interception, SMS spoofing, SMS denial of service and location tracking using SMS functionality. The practicality and low level of cost and effort needed to perform these attacks are demonstrated through the implementation of a number of proofs-of-concept.

Given the security concerns, a user of SMS may reconsider in which situations to use and how to interpret SMS. This is especially important for messages that contain information that can be sensitive for private or financial reasons, and for the use of SMS as a second authentication factor. In both mentioned cases there are other applications that usually can replace the functionality of SMS and that can guarantee the security end-to-end.

1.1 Outline

In the first part of the paper, an introduction to SMS security is given, where the importance of SMS security is described. A comparison with an ideal, secure messaging application is presented from a security perspective.

Section 3 provides a brief introduction of mobile networks and SMS in mobile networks. A more detailed description of the SMS functionality in different generations of mobile networks is given in Appendix B for completeness.

An SMS threat analysis in Section 4 is based on identified user trust assumptions. The user trust assumptions identified are treated in three areas:

- trust in the security of the radio channel to the network,
- trust in the security of the core network and
- trust in the operators´ management of user data.

Threat scenarios related to the trust assumptions are described and illustrated.

This is followed by a section with a review of real, publicly reported attacks on SMS security from a user perspective. Finally, a number of proofs-of-concept attacks have been implemented, which provide insight into the low level of cost and skills actually needed by an attacker to perform these attacks.

2 Introduction to SMS security

This section provides first a motivation of the importance of SMS security from a user perspective. This is followed by some basic concepts necessary to understand SMS security. The security properties of the SMS protocol is then compared to those of an ideal secure protocol and to typical state-of-the-art communication applications.

2.1 User assets

A motivation for studying the security of SMS is based on the type of information that can be included in SMS and the consequences that attacks on the SMS security could have for the users.

Examples of types of information that can be handled in SMS for a user are provided below.

- Personal information
- Financial information
- Authentication credentials, such as username, passwords and one-time passwords used for second factor authentication
- Confidential information of personal and business nature

An attack on the security of SMS could lead to the loss of this information, but additionally give further consequences as listed below.

- Privacy violation
- Part of identity theft
- Personal of corporate financial losses
- Damage of reputation
- Non-authorized access to services

In summary, there are user assets that are protected by the SMS security, and if the security is violated, this can have important negative consequences for the SMS user.

2.2 Basic security concepts

To understand the security of SMS, understanding the basic security concepts and the trust model of mobile networks is important.

Most secure communication protocols implement at least the following security properties:

- Confidentiality: Only the intended user can read the plain text.
- Integrity: The receiving user can verify that the message is not modified.
- Authentication: The receiving user can verify the sender's identity.

The table below maps reasonable user questions about SMS security and the corresponding security terminology.

Question	Security property
Can I trust that no one else can read my SMSs?	Confidentiality
Can I trust that the content of the SMS that I receive is not modified?	Integrity
Can I trust the identity of the sender of the SMS that I receive?	Authenticity
Can I trust that SMSs sent really get to their intended destination?	Availability
Can I be located through the SMS services of the mobile network?	Privacy

Table 1 Typical user requirements on message security with the corresponding security property.

Trust relationships, and the failures of them, are the basis for many of the vulnerabilities and attacks present in mobile networks.

Security properties that cannot be verified and security that is dependent on another entity will be referred to as (security) trust assumptions in this paper.

Using trust assumptions may be motivated in specific applications, but is vulnerable if any trusted party fails. The SMS protocol has no built-in security but instead relies on trust assumptions and possible security functions of other layers of communication.

The typical way to gain trust in security for communication between two end users is through security properties that are verifiable to the same end users. This can be achieved with cryptographic functions and the use of

cryptographic keys for confidentiality, integrity and authenticity. Trust is then limited to hold between the end users and to the strength of the cryptographic algorithms, the secrecy of the cryptographic key and in the security of the communication protocol. In fact, in different forms this is the basis for most secure communication in our modern society. More information about cryptography and verifiable trust can be found in Appendix A.

2.3 Comparison of SMS and secure communication protocols

In this section the SMS security properties are compared to those of an ideal secure communication protocol and to typical secure communication applications. This is shown in Table 2.

Security property \ Protocol	SMS	Ideal protocol
Confidentiality	No*	Yes
Integrity	No*	Yes
Authentication	No*	Yes

Table 2 Comparison between SMS and an ideal messaging protocol in terms of security properties.
** There is no built-in security functionality in the SMS protocol. However, there can be other security measures, such as security functions for other layers of communication for parts of the SMS delivery.*

Most modern mobile phones use a large set of different applications, including for secure communications. These applications can provide secure end-to-end communications between users, including confidentiality, integrity and authenticity.

While the user experience may not differ noticeably between messaging through a communication application and using SMS, there may be a large difference in how the message is processed, which affects the security properties. A short summary of the typical differences in terms of keys and connectivity is given in the table below.

Messaging function	Keys location	Key esablishment	Connectivity	Security
Application	On the phone	Asymmetric methods	Internet connectivity	End-to-end, with confidentiality, integrity and authenticity
SMS	On the SIM-card	Shared key with the operator	Mobile network connectivity	Based on security assumptions and non-verifiable trust

Table 3 Comparison between a typical application for secure communication and SMS in terms of key management, connectivity and security.

In particular, it is noted that SMS security is based on user trust assumptions that cannot be verified by the user. This trust model and its vulnerabilities will be further investigated in Section 4.

The use of second factor authentication in highly recommended and using SMS is far better than using none. However, in some cases a user can choose between different options, and there are more secure options than SMS. Guidance on the availability of authentication methods can be found in the 2FA Dictionary [2].

3 SMS over mobile networks

In this section, a schematic overview of how SMS is handled by mobile networks is described. This is needed in order to understand the concepts of the security of SMS. In Appendix B more information about the mobile networks from GSM to 5G and more specifics on how the SMS protocol is implemented in the networks can be found.

Common for mobile networks are a division into two main parts based on their main functionality, the radio access network and the core network.

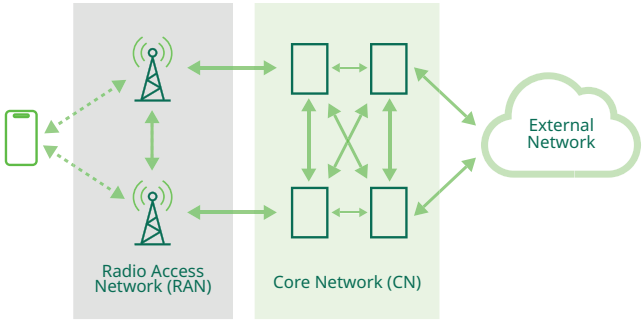

Figure 2 Illustration of the main components of a mobile network, the Radio Access Network (RAN) and the Core Network (CN).

The radio access network handles the wireless communication between base stations and the mobile users. This comprises the physical equipment, for example base stations, the protocols and algorithms for reliable radio transmission, such as coding, frequency allocation and transmission power control. Furthermore, functionality such as handover, when a user moves between base stations, is also often handled in the radio access networks. The security of the wireless link is also typically implemented here.

The core network handles other functions necessary to provide services. This includes user authentication, call set-up, roaming, billing, policy control and interconnection to external networks such as the Internet or other mobile networks. The SMS handling across different networks is also handled by the core network.

For SMS, there are similarities in how they are handled across the generations of mobile networks. In its simplest form, an SMS is transmitted from one user, via the mobile network, to an SMS Center (SMSC). The SMS Center then delivers the SMS via the network to the recipient. Because of this two-step procedure, the SMS protocol is sometimes referred to as store-and-forward, as opposed to for example a session-based connection between sender and receiver.

There are different methods of SMS handling for each generation of mobile network. This includes the initial way of sending SMS in the control channel introduced for the first SMS functionality in GSM, to packet-switched SMS handling in later generations of mobile networks. In Appendix B, these ways of sending SMS are introduced in a step-by-step manner, following the development of the mobile networks.

4 Threat analysis of SMS security based on the trust model

From a user perspective, there are three main areas of trust that are identified for SMS security in mobile networks.

1. Trust in the security of the radio access to the network.
2. Trust in the security of the core network.
3. Trust in the operators' secure management of user data.

An important point is that the verification of these assumptions on trust is out of the user control. The user is typically unable to prevent any attacks based on the vulnerabilities that the failure of these trust assumptions could cause. Additionally, the user is also unable to detect a possible attack in most cases.

The threat scenarios following from the vulnerabilities based on the user trust assumptions are explained in the following. For each threat scenario, attackers with different capabilities are introduced. Later, attacks based on the threat scenarios will be presented and complemented with proofs-of-concept for a number of attacks. The threat scenarios in this section does not claim to include every possible threat, but illustrate one way to represent relevant threats for SMS users.

4.1 Trust in the security of the radio access to the network

The security of the radio access between the mobile network and the user is fundamental for the security of SMS. In this area there are multiple threat scenarios.

First it is noted that there are vulnerabilities in the security functions of 2G, which makes practical attacks possible. It is, however, important to point out that the attacks are not restricted to 2G, but applies to all generations of mobile networks that have implemented a fallback solution to 2G. For example, an attacker can relatively easily perform a downgrade attack to change 5G service to 2G service, which makes the user vulnerable to the threat scenarios for 2G.

Threat scenario 1

The first threat scenario involves an active attacker within radio range, that presents itself as the mobile network to the mobile. The attacker can then present itself as a legitimate user to the real network in a man-in-the-middle attack. The man-in-the-middle could forward the messages to each party, having the ability to e.g. intercept, modify and stop communication, including SMS.

This is a threat for 2G, or after performing a downgrade attack from 3G/4G/5G to 2G, for two reasons.

- There is no mutual authentication in 2G, e.g. no way for the mobile to verify the identity of the network.
- Additionally, the cryptographic algorithms used in 2G are provenly weak [3] [4] [5] which means that the cryptographic keys of the user can be obtained. This is for example needed for a successful impersonation attack of the man-in-the-middle as the user to the network.

A user can typically not detect a MITM-attack. However, depending on the mobile phone, the generation of the mobile network can be found in the settings of the mobile.

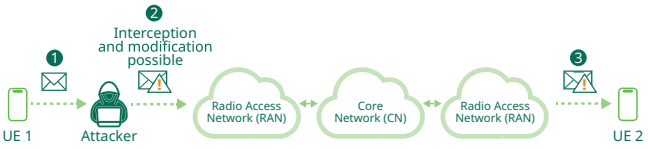

Figure 3 Active attacker within radio range performs a Man-In-The-Middle attack.

Threat scenario 2

The second threat scenario is similar to the first scenario in that there is an attacker within radio range. The attacker in this case is passively intercepting the traffic between the mobile network and the user.

This is a threat for 2G, or after performing a downgrade attack, for 3G/4G/5G, again since the cryptographic algorithms used in 2G are weak [3] [4] [5]. The attacker could intercept the SMS and then decrypt the message.

Another version of this scenario is the possibility of the radio link being configured without security. The operator has the possibility to control which cryptographic algorithms are used, and also the possibility to turn off the protection of SMS. In such a scenario an attacker in radio range could intercept the messages in clear text. If integrity protection is removed, the messages could also be modified without the possibility to verify the correctness.

A user cannot detect a passive eavesdropping attack. However, depending on the mobile phone, the generation of the mobile network can be found in the settings of the mobile.

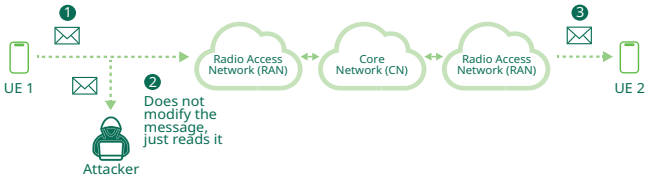

Figure 4 Passive attacker within radio range intercepts the SMS.

Threat scenario 3

The third threat scenario consists of an attacker performing denial-of-service through radio emissions or a downgrade attack based on manipulation with signaling messages. This can be performed in several ways, for example by an attacker transmitting radio energy, acting as noise, on the same frequency channels as the communication between the mobile and the base station [6].

The purpose of this attack can be denial-of-service, or for example to perform a downgrade attack to 2G.

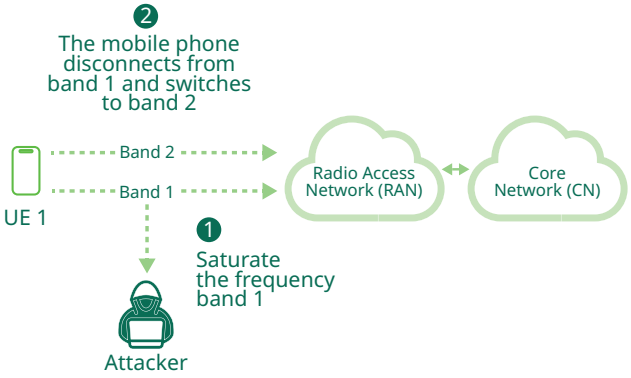

Figure 5 Attacker within radio range performing denial of service through radio emissions.

4.2 Trust in the security of the core network

The trust assumption in the security of the core network implies several threat scenarios.

The property that the operators, or authorized entities, can access contents on the network is a part of the design criteria of the networks. It follows since the secret key on the SIM-card of the user is shared with the operator. In terms of trust, this means that the user places trust in the operators, and additionally authorized third parties, of the mobile networks to store, read, modify or deny messages.

Less clear, but important, is that the operator implicitly also provides the same rights to read and affect the SMS messages to other operators or entities with access to the underlying interconnection protocols of the core network. The main security of the core network protocols, such as SS7 and Diameter, comes from that it´s access is closed for all, but network operators. While this may be a reasonable security assumption for a small, trusted community, it is provenly no longer the case. In fact, there is a very large number of entities with access to the signaling network, and it is reported that access can be bought [7].

Vulnerabilities are based on exploiting the available, legitimate protocol functionality, posing as a legitimate entity in the core network. This involves the threat of an attacker spoofing as a fake Home Subscription Library (HSL), as an SMS Central (SMSC) or as other network entities. More information on this can be found in Section 5.

Many operators have implemented additional security measures such as monitoring of the core network traffic, filtering, firewalls and methods to detect and mitigate for example attacks on SMS. More on security functions for the core networks in a European perspective can be found in [8].

Threat scenario 4

The operator to which the user subscribes, or an authorized entity in the legal area of the user, get access to the SMSs of the user. A user cannot detect if its messages are intercepted or modified.

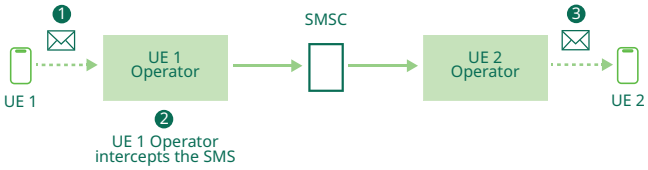

Figure 6 The operator of the user can intercept the SMSs.

Threat scenario 5

An operator, not being the operator of the user, or an authorized entity, not belonging to the legislation area of the user, gets access to the SMSs of the user. A user cannot detect if its messages are intercepted or modified.

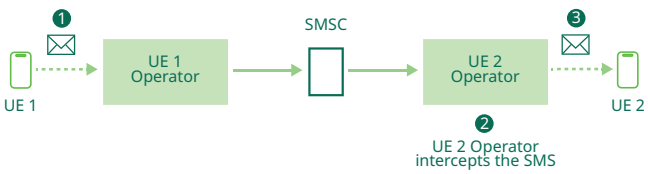

Figure 7 An operator other than the user's operator intercepts the SMSs.

Threat scenario 6

An attacker with access to the core network performs SMS interception, SMS spamming, SMS spoofing and phishing and denial of service.

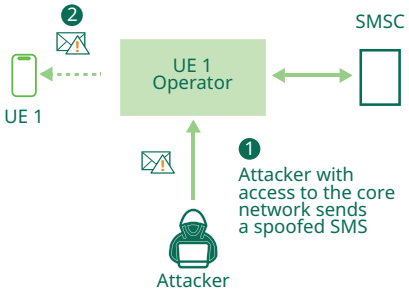

Figure 8 An attacker with access to the core network can for example send spoofing and phishing SMSs to users of the network.

4.3 Trust in the operators' secure management of user data.

Another important trust assumption concerns the operators´ management of the user data. In order to authenticate a user, each SIM-card has a cryptographic key that is coupled to a specific number, called IMSI. The IMSI is unique for each user across all networks. Additionally, there is a mapping of the IMSI to the telephone number of the user.

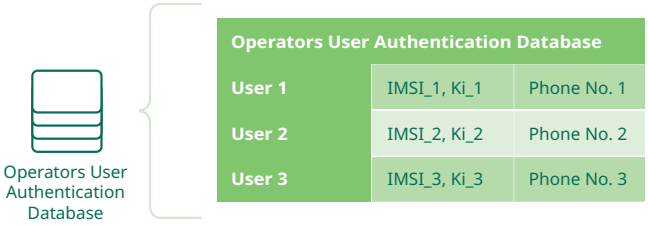

Figure 9 Illustration of an operator´s user authentication database, that handles the mapping between the users´ data in terms of identity (IMSI) and key (Ki) on the one hand, and the phone number on the other.

The coupling between telephone number, and the IMSI and key, can be altered. For example, when a user wants to keep its telephone number, but switch to a subscription with another operator, the telephone number will be coupled with another IMSI and key. This coupling between the IMSI and telephone number is important, since an attack could be mounted if the coupling is modified. The threat consists in that an attacker could impersonate a victim and receive the SMS messages destined to the victim. This is a so-called SIM swapping attack. The secure management of the coupling between the telephone number and the user credentials is hence another point of trust that the user places in the operator.

Threat scenario 7

An attacker performs a so-called SIM swapping attack, where the attacker makes the operator associate the telephone number with another SIM-card. This could be done in a social engineering attack, by non-trustworthy personnel at the operator or by attacks on the operators' systems.

An attacker performing a SIM swapping attack could impersonate the user and intercept the SMSs of the user. Additionally, a SIM swapping attack works as a denial-of-service attack.

The user is likely to detect that something is wrong, since the connection to the network will stop working.

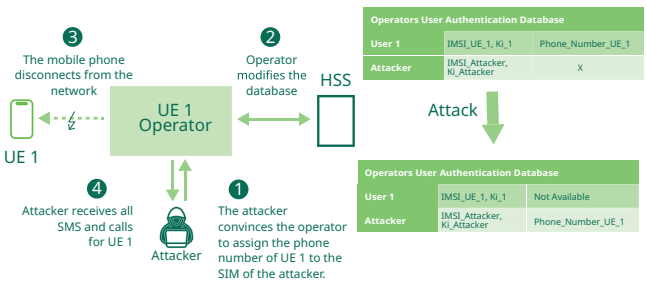

Figure 10 SIM swapping attack where the attacker convinces the operator to assign the victim´s phone number to the attacker´s SIM-card.

Threat scenario 8

An attacker copies the SIM-card from the user or obtains the secret key of the user from the operator. From a user perspective, the user can control the handling of the SIM-card, which additionally is protected against attacks. The user, however, trusts the operator for the secure storage of the key. The difference from threat scenario 7 is that, in this case, both the user and the attacker have the telephone number coupled to a SIM-card that has the correct information.

Similar to threat scenario 7, the attacker can impersonate the victim and receive the SMSs intended for the victim. The network service of the attacked user will be denied, which means that the user can detect that something is wrong.

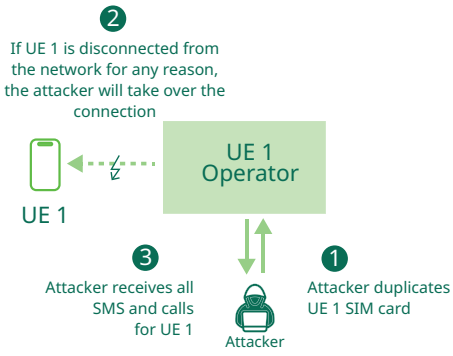

Figure 11 SIM swapping (Duplicate SIM) attack, where the attacker manages to produce a SIM-card with the same contents as the victim.

4.4 Summary of trust assumptions

In summary, each user places its trust, without possibility of verification, in the security of

1. the radio access to the network. The user assumes that the network is really the mobile network, and that a secure channel is created.
2. the core networks. The user assumes that each network handles the SMS securely within and between networks, and each connected party to the core network respects the privacy and security of each user.
3. user data at the operator. The user assumes that the operator will protect users against SIM swapping, where an attacker through e.g. social engineering or hacking, takes over the phone number of a user.

The verification of these assumptions is out of the user control, and the user is unable to prevent any attacks based on these vulnerabilities. In most cases, the user is also unable to detect a possible attack.

5 Attacks of SMS in mobile networks

In this section attacks based on the previous threat analysis and threat scenarios for SMS are presented.

The table below lists a number of selected attacks related to vulnerabilities in trust assumptions. The objective here is to in a simple way illustrate the relation between the security objectives of a user, the trust assumptions that the user cannot verify, and the possible attacks.

Question / Trust assumption	Radio access to the network	Core network security	Operator security management
Can I trust in the confidentiality of my SMSs?	SMS interception	SMS interception	SIM swapping
Can I trust that the content of the SMS I receive is not modified?	SMS interception (MITM)	SMS interception (MITM)	
Can I trust the identity of the sender of the SMS that I receive?	SMS spoofing	SMS spoofing	SIM swapping
Can I trust that SMSs sent really get to their intended destination?	Denial of service	Denial of service	SIM swapping
Can I be located thought the SMS services of the mobile network?	Location tracking	Location tracking	
Can I trust that the content of the SMS that I receive is secure?	SMS phishing, Malicious code injection	SMS phishing, Malicious code injection	

Table 4 Mapping of main SMS attacks from a user perspective, based on what security aspect and which trust assumption that is violated by the attack.

A main objective of this section is to provide an updated review of real, reported attacks on SMS security put in the perspective of the user. Other reviews of attacks on SMS can be found in [8] [9] [10] [11] [12]. In fact, reports on threats and attacks on SMS have continuously been published over time. The attacks are mostly the same, but the possibility of performing the attacks have been affected for several reasons, including the necessary equipment to perform the attacks, larger complexity with additional services and additional security measures.

As a current and interesting example, during the war in Ukraine, the mobile networks of Ukraine have played a role in the cybersecurity arena. More on this topic can be found in e.g. [13] [14] [15], and examples reported from the war in Ukraine relevant for SMS security have been included in this section.

SMS Interception

In an SMS interception attack, the attacker gains access to SMS messages transmitted to or from a victim. This attack can be used to obtain sensitive information, for example private information or user credentials.

Given access to the core network, attackers can redirect the victim's SMS to the attackers own phone numbers [9] [16]. A real case of such an attack occurred in 2017, in which hackers intercepted second factor authentication credentials to authenticate transactions from bank accounts of a German bank to accounts of the attackers [17]. This corresponds to threat scenario 6.

Reports from the Snowden leaks is an example of large-scale SMS interception [18]. A more recent example of SMS interception is from Ukraine, where it is reported that the communication from Ukraine to Russia was intercepted by the Ukrainian intelligence, which is likely to include SMS [19].

Another possible way to intercept SMS, related to threat scenario 2, is to intercept the communication between the victim´s mobile device and the network [20]. As described in threat scenario 2, due to the legacy cryptography used in the 2G standard, it is possible to decipher the communication. Even if the mobile device supports 3G/4G/5G, it is possible to perform a downgrade to 2G with a fake base station, which corresponds to threat scenario 1.

Threat scenario 2 also contains the case where the encryption of the network access link is disabled. This could be the result of a misconfiguration, e.g. as reported in [21], or intentionally disabled by an operator colluding with the authorities to facilitate interception.

SMS Denial of Service (DoS)

In general for mobile networks, there are multiple attack scenarios causing denial of service. One way is by flooding the network with a large volume of SMS traffic, causing overload and service disruption. The attack can be carried out either from the core network, threat scenario 6 [9] [10], or from radio emissions, threat scenario 3 [22].

SMS Spoofing

SMS spoofing is a way to falsify the identity of the sender of an SMS, typically to deceive a victim that they are interacting with someone else. There are many ways that SMS spoofing can be used by attackers. SMS spoofing is often used in SMS phishing and SMS spamming. An interesting case involving SMS spoofing is the report about the

operator MTN Uganda. The study analyzed the level of fraud in mobile money transactions and the control systems in mobile network operators, concluding that up to 61.5% of customers had lost money due to SMS spoofing at some point [23].

SMS Phishing (Smishing)

In SMS phishing attacks, the typical objective of the attacker is to steal personal information from a victim. An example of phishing attacks is to send deceptive SMS messages to trick recipients into revealing personal information, such as passwords or financial data.

In 2022, employees of the Twilio company were the victims of an SMS phishing attack, receiving SMS messages pretending to be from the IT department (spoofing) asking for passwords and confidential information [24].

A recent case of SMS phishing attacks, related to the war in Ukraine, is reported in early 2023 against the Caspian Pipeline Consortium (CPC). Phishing links were sent in SMS to the employees, with the objective of exfiltrating user credentials in a later stage [25].

Malicious Code Injection

Another attack method consists in sending SMS messages containing links or malicious code (malware) to compromise the security of the device or the network. These malicious code injection attacks through SMS can be used to obtain private data, passwords, modify or erase data on a smartphone [26].

A real case attack example is EMOTET, a Trojan that in 2020 posed as US banks to steal sensitive information and credentials [27]. Another example is based on the Snowden leaks, where it is reported that the NSA developed malicious code for attacks on SIM-cards with possibility to e.g. intercept SMS [28] [29].

SMS Spamming

SMS spamming consists of the unwanted sending of messages to one or more targets, potentially in large quantities. In many cases, spam attacks are linked to SMS spoofing, since the attacker intends to deceive the victim that the SMS is from a trusted source.

A recent case is from the war in Ukraine, where the Russian secret services are reported to use SMS spamming methods to send SMSs with intimidating content to private phone numbers of Ukrainian military personnel [30]. In a similar case, Ukraine´s intelligence service accused Russia of sending 5000 SMS messages to Ukrainian military officers to surrender [31].

SIM swapping

In SIM swapping attacks, the attacker exploits vulnerabilities in the operators' security management to change the phone number of the user, to the SIM card of the attacker. The attack can be carried out in a number of ways, for example calling the operator of the victim with the change request. For this social engineering attack to succeed, typically, information about the victim, such as phone number, ID card number and additional information is gathered [32] [33] [34] [35].

With this attack, the victim´s SIM card is deactivated and the attacker receives all calls and SMSs, and can also use two-factor authentication, password reset codes, receive banking information etc.

Location tracking

Although not directly related to SMS, the core network can be used to locate users [8]. As a recent example, it is likely that Ukrainian intelligence has taken advantage of the Russian military using mobile phones for interception and location tracking. It is reported that in at least one instance, Ukraine intercepted a Russian general´s call, tracked the location and successfully attacked with military means [19] [36] [37].

6 Proofs-of-concept of SMS attacks

In this section the implementation and results of a number of proofs-of-concept (PoC) attacks that DEKRA has performed are presented. This illustrates the practicality of a subset of the attacks possible based on the vulnerabilities in the threat scenarios previously described. The PoCs implemented violate the confidentiality, integrity, authenticity and availability of the user SMSs in different ways. Both the cost and difficulty of the attacks have a level that makes them feasible for a large set of attackers.

Some of the proofs-of-concept are attacks on their own, and some can be combined to advanced attacks involving different methods and stages. The proofs-of-concept implemented are grouped based on which type of user trust assumption that they violate.

Violation of the user trust assumption in the security of the radio access to the network

- Passive radio channel interception of unencrypted SMS in 4G with disabled crypto.
- Downgrade attack of 4G network service by external attacker using the radio channel.
- Cryptographic attack on the 2G (GPRS) encryption algorithm GEA-1.
- Cryptographic attack on the 2G (GSM) encryption algorithm A5/1.

Important to note is that the proofs-of-concept listed can be combined to more advanced attacks in a series of steps. For example, consider a mobile user with connection to the 5G network. As a first stage, the connection can be downgraded to the 2G network with for example a downgrade attack. In the second stage, the attacker intercepts the network traffic passively, and in the third stage, the attacker decrypts the traffic, including potential SMS. There are several possible variations on this attack, for example to act as a man-in-the-middle between the mobile user and the mobile network. These attacks correspond to threat scenario 1-3 in Section 4.

Violation of user the trust assumption in the security of the core network

- Interception of SMS by operator or attacker with operator access rights in 4G.
- Interception of SMS by operator or attacker with operator access rights in 2G.
- SMS spoofing attack for attacker with operator access rights in 4G.
- SMS spoofing attack for attacker with operator access rights in 2G.
- Web application spoofing attack.

The proofs-of-concept in this section demonstrates that the SMSs are not protected end-to-end but are available in clear text at the operator. This additionally implies that the integrity and authenticity of the messages are not protected by the protocol. The proof-of-concept using a web application service for spoofing SMS demonstrates how easy it is for anyone to spoof SMS.

From a user perspective, the spoofed SMSs are apparently authentic, as the spoofed SMS is treated by the mobile phone as if the sender is the same as previous messages received with the same name.

The proofs-of-concept in this part correspond to the threat scenarios 4-6 in Section 4.

Violation of the user trust assumption in the operators' secure management of user data

- SIM Swapping attack in the 4G network.

The SIM swapping proof-of-concept demonstrates that the SIM swapping attacks work, and the security of the operator handling of user data is critical for the security. This type of attack can be detected by the user, since the user is disconnected from the mobile network. However, in attacks against two-factor-authentication by SMS, the time of detection and response of the user is very likely to be too long to stop the attacker.

The proof-of-concept corresponds to threat scenario 7 in Section 4.

Selection of proofs-of-concept

The selection of PoCs has been from a user perspective, as a contrast to, for example, an operator perspective. Legal and practical aspects have also been taken into account when selecting the PoCs to implement.

To limit the number of PoCs, but still obtain coverage of mobile technology, some PoCs are performed in only one generation of mobile networks, and others are performed with one PoC in 2G, where 3G would be very similar, and one PoC in 4G, were 5G would be very similar. This is motivated by how SMS are handled differently depending on technology.

A detailed description of each proof-of-concept can be found in the corresponding part of the appendix.

7 Conclusions

SMS is still after more than 30 years a great success and used worldwide. Behind the success is the ease of communication with literally anyone with a mobile, across mobile technologies and countries. While successful and easy to use, there are also security concerns. In this paper, the security of SMS from a user perspective has been analysed.

The basic security properties desired for a message service are confidentiality, integrity and authenticity. The SMS protocol cannot guarantee these properties, and the user instead places its trust in security assumptions that typically cannot be verified by the user. In this paper, it has been clarified and analyzed which trust assumptions that a user has to make for SMS security, and how vulnerabilities, threats and attacks are related to this.

The threats to SMS security are put into the context of real-life attackers in a review of publicly reported attacks and by presenting performed proofs-of-concept for a number of attacks.

SMS users should be aware of the security risks and consider in which cases to use SMS. Messaging of information that can be sensitive for private or financial reasons and the use of SMS as a second authentication factor are examples of use cases where instead other, secure services should be considered. Furthermore, it should be kept in mind that SMSs are not authenticated and that the displayed sender may not be the actual sender.

Glossary

AMF	Access and Mobility Function
APN	Access Point Name
AuC	Authentication Center
BSC	Base Station Controller
BTS	Base Transceiver Station
CN	Core Network
CS	Circuit Switching
eNB	Evolved Node B
EPC	Evolved Packet Core
GEA	GPRS Encryption Algorithm
gNB	Next-Generation Node B
GPRS	General Packet Radio Services
GSM	Global System for Mobile Communication
HLR	Home Location Register
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
LTE	Long Term Evolution
MITM	Man-in-the-middle
MME	Mobility Management Entity
NAS	Non-Access-Stratum
NodeB	Node Base Station
PGWU	Packet Data Network Gateway User Plane
PoC	Proof-of-concept
PS	Packet Switching
RAN	Radio Access Network
RNC	Radio Network Controller
SIM	Subscriber Identity Module
SG	Signaling Gateway
SIP	Session Initiation Protocol
SMS	Short Message Service
SMSC	Short Message Service Center
SMSF	Short Message Service Function
SS7	Signaling System 7
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UPF	User Plane Function
3GPP	3rd Generation Partnership Project

Appendix A. Cryptography for verifiable trust

In this section a brief background on the cryptographic properties used to establish verifiable trust is given. This includes the use of symmetric and asymmetric keys and algorithms to obtain confidentiality, integrity and authenticity, which are the basis for secure communication.

The availability of a shared secret key among two communicating users is sufficient to achieve a secure channel with confidentiality, integrity and authenticity. There are two main ways to achieve a shared secret key; using asymmetric cryptography based on certificates and a so-called public key infrastructure, or using a separate, trusted channel to distribute the symmetric secret keys.

- Asymmetric: When you visit a webpage, the TLS protocol is used to establish a secure connection, typically represented by a padlock icon in the browser. The secure connection is established, even though there is no previous secret key shared between you and the application that you are communicating with. Asymmetric cryptography is used to create the secure channel, which includes confidentiality, integrity and authenticity. But how is this achieved? Although different cryptographic functions are used, in terms of trust, it comes down to the trust in a common third entity, and the mutual verification of this trust by different means including certificates and public key infrastructure.
- Symmetric: Another way to establish shared secret keys is through the use of a separate, secure channel. There are many ways to do this, for example by loading a secret key in a system during production, offline distribution on e.g. paper or disc, or through some other trusted secure channel. This is the case for mobile networks, where a secret key is stored in the SIM-card, and additionally by the operator in the network.

For some security mechanisms, the properties of confidentiality, integrity and authenticity are achieved jointly, but in other cases they are not. This can be adapted depending on the security requirements of the use case. To see why each of the properties is important, consider the following examples.

Example 1: Integrity and authenticity, but not confidentiality. The communicating users know who they communicate with, that the information is unmodified, but other parties can eavesdrop on their communication. In fact, this is a desirable property in many cases, for example for certificates in a public key infrastructure.

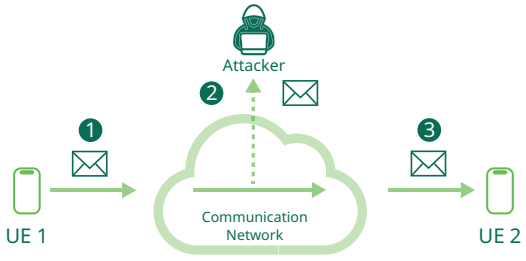

Figure 12 Communication with integrity and authenticity, but without confidentiality.

Example 2: Confidentiality without integrity. The communicating users encrypt their communication, but do not know whether the communication has been modified or not. An example of this is when a so-called stream cipher is used for encryption. An attacker can then modify bits of the message, without knowing the content, and without the receiver being able to detect, given that no other integrity protection mechanism is used. Stream ciphers are often used for mobile communications.

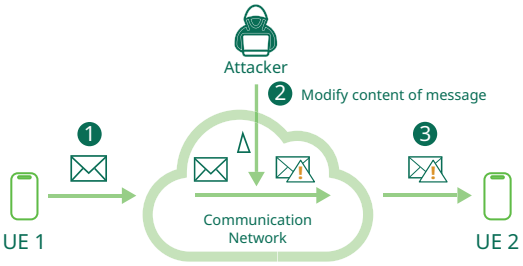

Figure 13 Communication with confidentiality, but without integrity.

Example 3: To see the importance of authenticity, consider a case using cryptographic methods for confidentiality and integrity, but not for authenticity. The main problem is that the communicating parties cannot be sure about the identity of who they are talking to. In some cases, this opens up for so-called man-in-the-middle (MITM) attacks, where an attacker is acting as a middle-man on the communication link, decrypting information from one user, and then re-encrypting for the other user. Under some circumstances, MITM scenarios are possible both for asymmetric and symmetric cases.

- In the asymmetric case, a MITM-attack is possible if there is not a trusted third party, which can authenticate the users to each other.
- In the symmetric, shared key case, the MITM-attack is possible when the keys are shared with an intermediate party. This is the case of mobile networks, where the operator shares a key with each user – but the users do not share a common key.

Figure 14 Man-in-the-middle attack scenario.

B Appendix B. Mobile networks from GSM to 5G

In order to understand the security of SMS in mobile networks, more background is provided in this section. This is motivated by the fact that different generations of mobile networks interact, work side by side and additionally share architecture and protocols. The main focus in this section is on the functions regarding security of SMS and to understand the settings of different attacks and proofs-of-concept.

SMS was first introduced in GSM, often referred to as 2G. The GSM network was mainly designed for voice service and was built on circuit-switched networks. It had limited capability of data transmission and it was in this setting that SMS was first introduced. A special feature of SMS is that it was included in the control plane, as opposed to the user plane. The control plane is typically used for communication regarding the mobile status, mobility and radio access. The inclusion of SMS in the control plane made sense in the GSM network to optimize the network bandwidth.

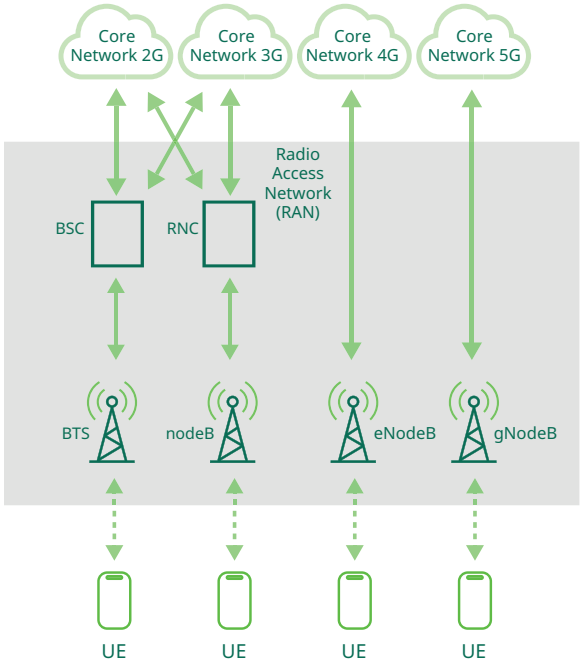

Figure 15 Illustration of the main components of a Radio Access Network (RAN) of the different mobile generations.

Terminology	2G	3G	4G	5G
Base Station	BTS	nodeB	eNodeB	gNodeB
Controller Base Station	BSC	RNC		

Table 5 Summary of terminology for the Radio Access Network for different generations of mobile networks.

During the second half of the 1990s, packet data was introduced with General Packet Radio Services (GPRS). GPRS is sometimes referred to as 2.5G. This mainly changed the core network, which added support for packed-switched networks, along with the circuit-switched networks.

The 3G mobile network introduced significant improvements in many respects. Especially the radio access network technology with the base stations changed, while the structure of the core network has a similar structure to that of GSM and GPRS. Among the requirements in the development of 3G was the backward compatibility to the second-generation mobile networks, including the circuit-switched technology [38].

An important addition in the 3G network was the addition of mutual authentication between a user (SIM-card) and the network. There were also improvements in the cryptographic algorithms used in the authentication and encryption.

In parallel to 3G, Long Term Evolution (LTE) was developed. In contrast to 3G, the requirements for the development were less restrictive in terms of backward compatibility and LTE, later named 4G, was designed for packet-based traffic directly. Different technology was introduced on the radio access network, well suited for packed-based and high throughput services with low delay.

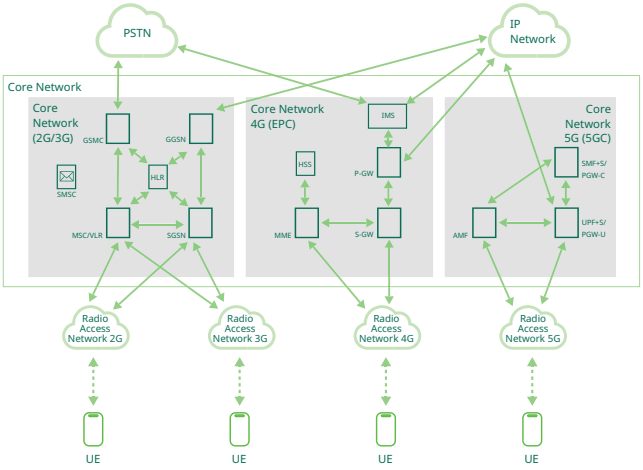

Figure 16 Illustration of the main components of the Core Network (CN) of the different mobile generations.

The complexity of the radio access network was reduced by removing the element Radio Network Controller from 3G, and including most of its functionality in the base stations, now denoted eNodeB. Also, the core network was updated into the Evolved Packet Core (EPC), entirely dedicated to the packet-based domain. Some functionality from the radio access network was also moved to the core network, for example the Mobility Management Entity, MME, which e.g. handles the functionality to maintain calls during mobility.

The framework for services over the IP-network is called the IP Multimedia Subsystem (IMS) and constitutes an additional way to transmit SMS over the network. The previous control-plane-based SMS protocol was also implemented, both on its own, and indirectly by interoperability between SMS in 3G and 4G. SMS in the control-plane is referred to as SMS per Non-Access-Stratum (NAS).

Similar to previous solutions, the core network contains the subscriber information, in 4G denoted Home Subscriber Server (HSS), which is the corresponding of the previous Home Location Register (HLR) and the Authentication Center (AuC). These databases are critical for the authentication and the security of the network in general and SMS in particular, since they contain the subscriber keys.

The security objectives for the development of LTE was to make the security of LTE equivalent, or better, than that of 3G. Secure connections between the mobiles and the network, including encryption and mutual authentication, but at the same time enable lawful interception of the traffic, was standardized. Additional layers of privacy, communication confidentiality, location privacy and identity protection are added to protect from unauthorized third parties. Authorized parties are typically government agencies, but can also include others, for example location services.

The 5G mobile network is also based on an overall network architecture with a separation between a radio access network and a core network. The radio access network schematics are similar to 4G, but the nodes are now called gNodeB, which stands for “5G Node B”. The network core is schematically divided into the Access and Mobility Function (AMF), controlling the radio access, and the User Plane Function (UPF), handling the user data. The 5G network is based on network functions rather than network entities.

Mobile networks have a layered architecture, with similarities to how the Internet works. In the core networks there are different protocols handling the SMS distribution. For 2G and 3G, an important core network protocol for SMS, and many other functionalities, is the Signaling System 7 (SS7) protocol.

The SS7 protocol was developed 1975, in a time when security implementations of encryption and authenticity did not have the same maturity and recognized importance as it has today. The SS7 protocol provides basic services such as call setup and teardown, routing, roaming and SMS across the networks. An example of this is the network communication needed to locate the recipient of an SMS. Although the SS7 protocol is a part of the core network protocols for 2G and 3G, it is still used in the later generations of mobile networks, mostly for compatibility and interconnection of services, such as SMS, over different networks.

With 4G and the packet-based EPC, the IP-based Diameter protocol was introduced. Diameter is for example used for the communication regarding authentication between the MME and the HSS in the core network. 5G also has a packet-based core network, which supports interaction with the 4G and 2G/3G networks.

B.1 SMS in GSM to 5G

In 2G and 3G networks, there are two modes of sending SMS [39]:

- SMS over CS (Circuit-Switched): It operates over the circuit-switched network, which means that a dedicated connection is established between the sender and receiver for the duration of the SMS transmission.
- SMS over PS (Packet-Switched): It operates over the packet-switched network, which means that data is divided into packets and sent independently across the network to its destination.

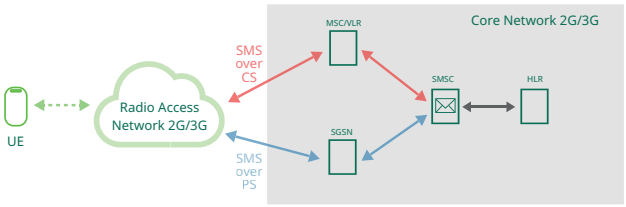

Figure 17 Illustration of the main components of the Core Network (CN) for the use of SMS in 2G/3G networks.

In 4G networks, there are three modes of sending SMS [39]:

- SMS over SG: It was the first 4G sending mode, without the need for IMS. It is a hybrid approach to SMS transmission between LTE and the CS infrastructure.
- SMS over NAS: For SMS transport between MME and SMSC, the Diameter protocol is used. Therefore, the UE does not have to be registered in the 2G/3G network. In addition, the NAS protocol is used for sending encapsulated SMS between the UE and the MME.
- SMS over IMS: This is the most typical sending mode in 4G. In this case, the SMS is sent via SIP, which means that communication via IMS is necessary.

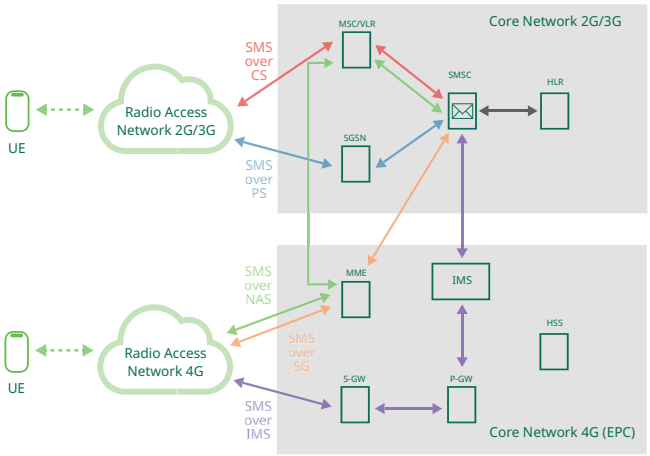

Figure 18 Illustration of the main components of the Core Network (CN) for the use of SMS in 4G networks.

In 5G networks, it is possible to make use of the existing IMS network or to make use of the new network element known as SMSF, which supports SMS over NAS.

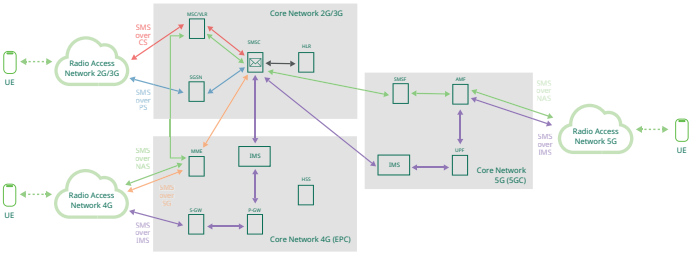

Figure 19 Illustration of the main components of the Core Network (CN) for the use of SMS in 5G networks.

Appendix C. Proofs-of-concept

In the following, the performed proofs-of-concept are presented, starting with a summary on the setup.

C.1 PoC setup

In the realization of the PoCs, both legal and practical aspects need to be considered. All PoCs have been performed in a controlled environment in a DEKRA laboratory. This means that DEKRA has set up its own mobile infrastructure to perform the attacks. This has been in an isolated environment, not connected to or interfering with public mobile networks.

Equipment	2G	3G	4G	5G
User equipment	Standard mobile phones have been used, that also work perfectly on any other public mobile network: Samsung Galaxy A3, Redmi 7A			
Radio access network	Ettus USRP B210 [40]	Ettus USRP B210	Amarisoft Classic [41]	Amarisoft Classic
Core network	OsmoNITB	OsmoNITB	Amarisoft	Amarisoft
Interception equipment	HackRF One	HackRF One	Ettus USRP B210/ HackRF One	Ettus USRP B210/ HackRF One

Table 6 Equipment used in the execution of the proofs-of-concept for different generations of mobile networks.

Figure 20 and Figure 21 show some of the setups used for the proofs-of-concept.

Figure 20 Ramsey box with Ettus USRP B210, Hack RF and two phones.

Figure 21 Amarisoft Classic with two phones.

The objective has been to provide a testing environment that corresponds to real scenarios. Additionally, it is interesting to note that it is neither very complex nor expensive to simulate a base station and provide a network. Software defined radio, for example as HackRF One or Ettus USRP B210, is affordable, and open source software can be used to model a base station.

Testing of the functionality of the network can be done for example by using standard user equipment. Since the objective is to study the security from a user perspective, it is interesting to note whether the mobile phones used indicate any differences when the network and the configurations for functionality and security are controlled.

Just as there are many different types of user equipment, there are different base stations with different HW and SW and different configurations and the PoCs only cover the tested cases.

C.2 Interception of SMS by operator or attacker with operator access rights in 4G

Objective

Illustrate that the operator, or an attacker with operator access, can intercept the user SMS traffic in clear text, without the user being able to detect.

Setup

The setup to this PoC is:

- PC: To configure the 4G network via SSH.
- 4G network (Amarisoft Callbox Classic): Simulates a real operator network and a base station.
- Two mobile phones: Simulating real communication.
- Two writeable SIM cards: To be able to connect them to the base station.

Figure Conceptual: Figure 6

Figure Simulated:

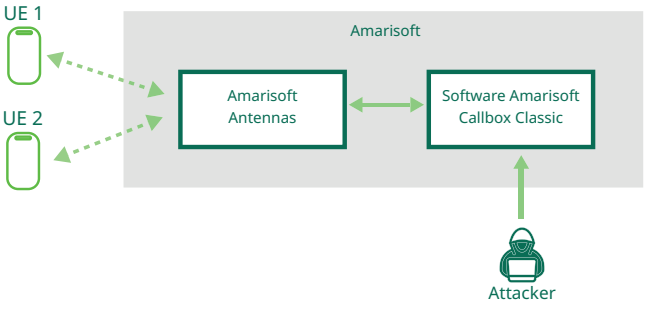

Figure 22 Simulated scenario of interception of SMS by operator or attacker with operator access rights in 4G

Configuration of setup

The configuration to this PoC is:

1. Downlink frequency 2680MHz (Band 7).
2. Bandwidth 5MHz.
3. RRC/UP layer ciphering algorithm: 128-bit AES or Snow 3G.
4. Access Point Name: Default and Internet.
5. NAS layer ciphering algorithm: 128-bit AES or Snow 3G.
6. SMS over IMS.
7. Layers IMS in debug mode.
8. Configuration SIM 1:
   a. Algorithm SIM: XOR
   b. IMSI: 001010102345678
   c. Ki: 00112233445566778899aabbccddeeff
   d. Number Phone: 0600000000
9. Configuration SIM 2:
   a. Algorithm SIM: milenage
   b. IMSI: 0010101023456788
   c. Ki: 00112233445566778899aabbccddeeff
   d. Number Phone: 0600000001

Procedure

The procedure to this PoC is:

1. Configure the operator with the given configuration parameters.
2. Configure the Access Point Name (APN) on the phone.
3. Connect the phone to the 4G network.
4. Capture network-wide traffic.
5. Send the SMS from phone 2 to phone 1.
6. Intercept the SMS from the network interface.

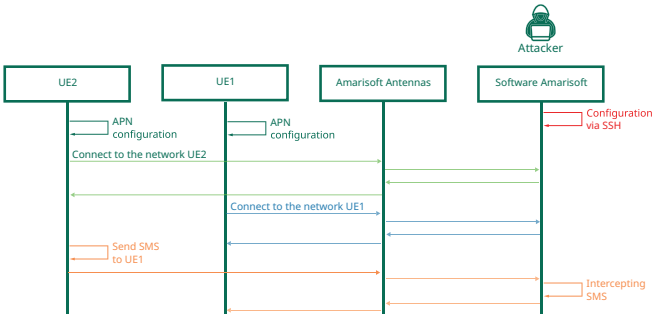

Figure 23 Procedure of interception of SMS by operator or attacker with operator access rights in 4G.

Results

The 4G network has been set up via SSH with the above parameters. Once configured, the service is established.

The configuration of the SIM-card is the following:

```
ue_db: [{
    sim_algo: "xor", /* USIM authentication algorithm: xor, milenage or tuak */
    imsi: "001010123456789", /* Amarisoft or Anritsu Test USIM */
    amf: 0x9001, /* Authentication Management Field */
    sqn: "000000000000", /* Sequence Number */
    K: "00112233445566778899aabbccddeeff", /* Amarisoft or Anritsu Test USIM */
    impi: "901312122799083@ims.mnc001.mcc001.3gppnetwork.org",
    impu: ["901312122799083", "tel:0600000000", "tel:600"],
    //force_sms_over_sg: true,
 }, {
    sim_algo: "milenage",
    imsi: "001010123456788",
    amf: 0x9001,
    sqn: "000000000000",
    opc: "11111111111111111111111111111111",
    K: "00112233445566778899AABBCCDDEEFF",
    //force_sms_over_sg: true,
    impu: ["001010000000001", "tel:0600000001", "tel:601"],
    impi: "001010000000001@ims.mnc001.mcc001.3gppnetwork.org",
}, {
```

Figure 24 The database for subscribers, including the SIM-card information.

In Settings, Mobile Networks and Access Point Name, the following APN has been added:

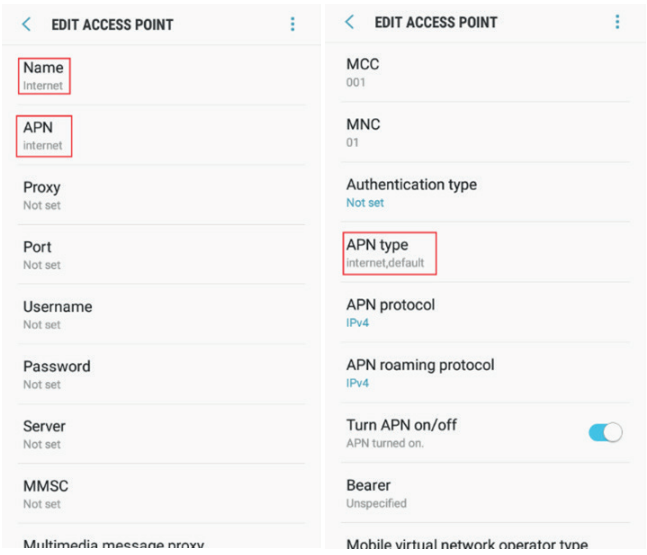

Figure 25 Configuration Access Point Name (APN)

Both mobiles are connected automatically to the network after configuring the APN, as can be seen in the figure below.

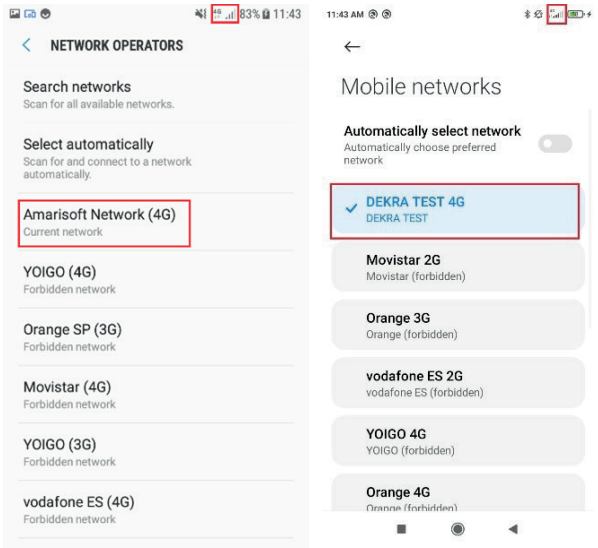

Figure 26 Phones connected to the same 4G network created with Amarisoft.

The operator's IMS layer has been configured in debug mode to display the messages being sent.

Figure 27 below shows how an SMS has been sent between phone 2 and phone 1.

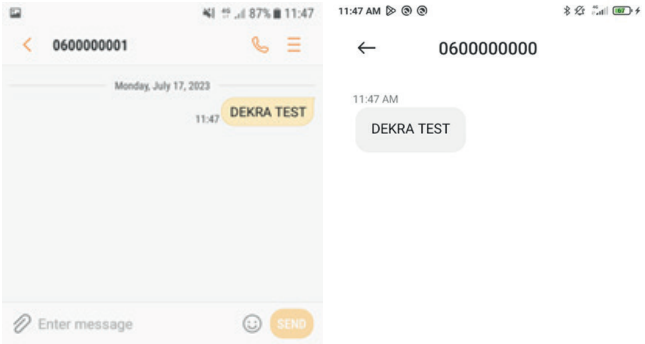

Figure 27 Sending SMS between phones

From the operator interface, the SMS can be seen in clear text, as shown in Figure 28.

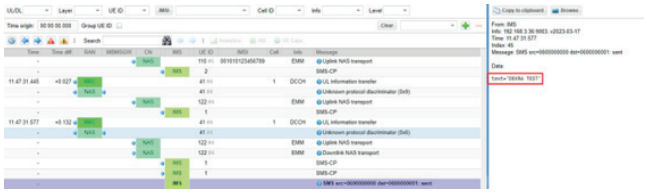

Figure 28 Interception of SMS from the operator.

Conclusions

The PoC illustrates the vulnerability caused by the user trust in the network and the operator. An attacker, or authorized entity, with the access rights of an operator can intercept messages independently of whether encryption is used for the radio access.

The user cannot detect the attack. The user would need an additional layer of protection in order to protect the security of the message.

C.3 Interception of SMS by operator or attacker with operator access rights in 2G

Objective

Illustrate that the operator, or an attacker with operator access, can intercept the user SMS traffic in clear text, without the user being able to detect.

Setup

The setup to this PoC is:

- PC: To configure the 2G network via SSH.
- 2G network (OsmoNITB): Simulates a real operator network and a base station (Ettus USRP B210).
- Two mobile phones: Simulating real communication.
- Two writeable SIM-cards: To be able to connect them to the base station.
- Ramsey Box: To work at the 2G operating frequency band without interfering with public networks.

Figure Conceptual: Figure 6

Figure Simulated:

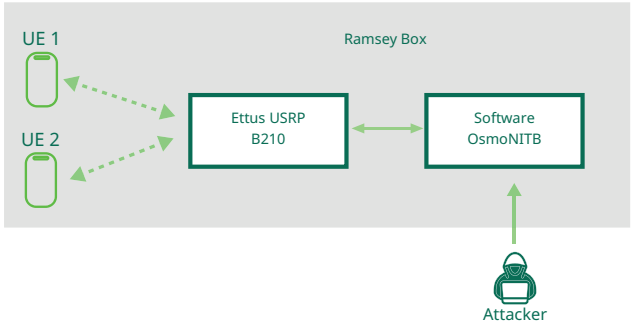

Figure 29 Simulated scenario of interception of SMS by operator or attacker with operator access rights in 2G.

Configuration of setup

The configuration to this PoC is:

1. Band GSM900.
2. Access Point Name: Default and Internet.
3. SMS over NAS.
4. Configuration SIM 1:
   a. IMSI: 101023456789
   b. Number Phone: 195
5. Configuration SIM 2:
   a. IMSI: 310260123456064
   b. Phone number: 156

Procedure

The procedure to this PoC is:

1. Configure the operator with the given configuration parameters.
2. Configure the APN on the phone.
3. Connect the phone to the 2G network.

4. Capture network traffic.
5. Send an SMS from phone 1 to phone 2.
6. Interception of the SMS from the network interface.

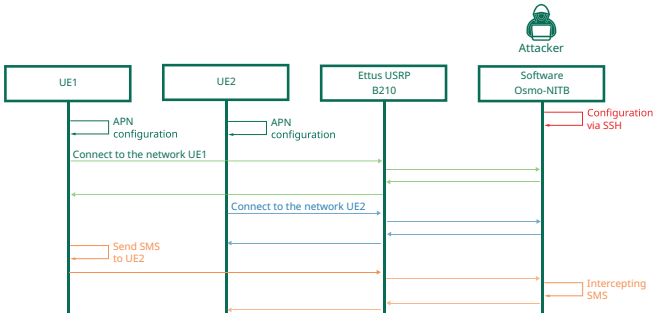

Figure 30 Procedure of Interception of SMS by operator or attacker with operator access rights in 2G.

Results

The 2G network has been set up with the given parameters. Once configured, the service is established.

The APN configuration on the mobiles is the same as in Figure 25.

After configuring the APN of the mobile phone, the mobile connects automatically to the network.

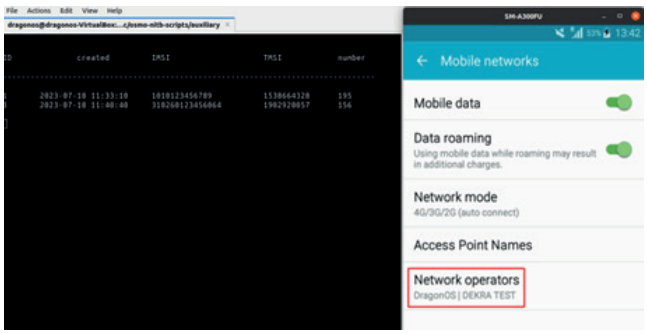

Figure 31 To the left, the terminal shows the connected phone with connection date, IMSI, TMSI and number. To the right, the phone displays connection to the DragonOS network.

A message has been sent between phone 1 and phone 2.

Figure 32 shows how an SMS from UE1 has been received by UE2.

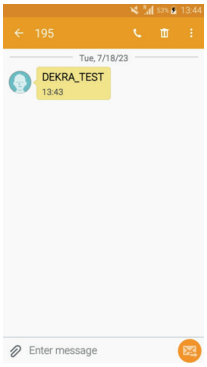

Figure 32 SMS sent between two phones.

The SMS can be read in clear text from the operator interface, which is shown in Figure 33. This is the case independently of whether the communication between the mobile phone and the base station is encrypted or not.

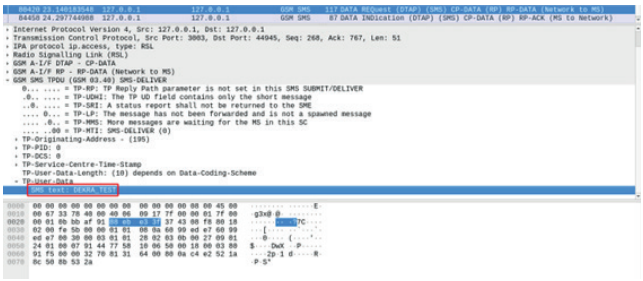

Figure 33 Interception of SMS by the operator. The figure shows a capture of the network traffic at the base station using the program Wireshark.

Conclusions

The PoC illustrates that SMSs are not end-to-end encrypted, but gives the operator, and any attacker with operator access, the possibility to read the message in clear text. In fact, since there is no other protection given by the SMS protocol, there is also the possibility of an attack modifying the SMS. This holds independently of whether the radio channel is encrypted or not. The user has to trust the operator, but has no possibility of verifying the trust.

The user cannot detect the attack. The user would need an additional layer of protection in order to protect the security of the message.

C.4 SMS spoofing attack for attacker with operator access rights in a 4G network

Objective

Illustrate with a PoC that an SMS in the mobile network is not authenticated and a spoofing attack against the users therefore is possible. This PoC attack is performed in the 4G network.

Setup

The setup to this PoC is:

- PC: To configure the 4G network via SSH.
- 4G network (Amarisoft Callbox Classic): Simulates a real operator network and a base station.
- One mobile phone: Simulating real network subscribers.
- One writeable SIM-card: To be able to connect the mobile to the base station.

Figure Conceptual: Figure 8

Figure Simulated:

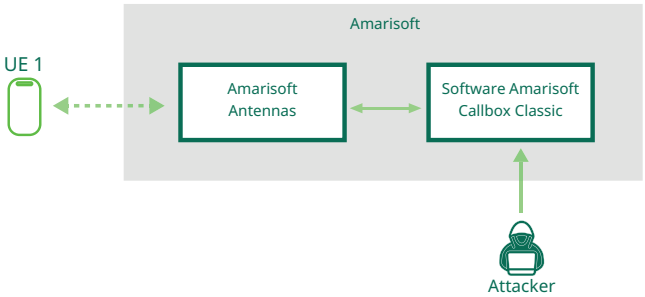

Figure 34 Simulated SMS spoofing attack scenario for attacker with operator access rights in a 4G network.

Configuration

The configuration to this PoC is:

1. Downlink frequency 2680MHz (Band 7).
2. Bandwidth 5MHz.
3. RRC/UP layer ciphering algorithm: 128-bit AES or Snow 3G.
4. Access Point Name: Default and Internet.
5. NAS layer ciphering algorithm: 128-bit AES or Snow 3G.
6. SMS over IMS.
7. Configuration SIM:
   a. Algorithm SIM: XOR
   b. IMSI: 0010101023456789
   c. K: 00112233445566778899aabbccddeeff
   d. Phone Number: 0600000000

Procedure

The procedure to this PoC is:

1. Configure the operator with the correct configuration parameters.
2. Configure the APN on the phone.
3. Connect the phone to the 4G network.
4. Send the spoofed SMS.
5. Confirm the SMS reception and handling on the phone.

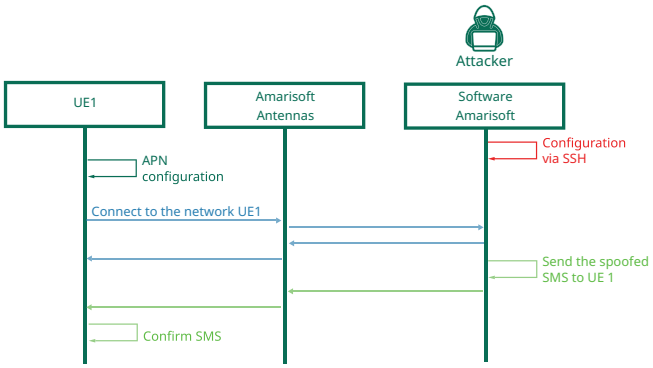

Figure 35 Procedure of SMS spoofing attack for attacker with operator access rights in a 4G network

Results

The 4G network has been set up via SSH with the above parameters. Once configured, the service has been re-established.

The configuration of the SIM-card is the following:

```
ue_db: ({
    sim_algo: "xor", /* USIM authentication algorithm: xor, milenage or tuak */
    imsi: "001010123456789", /* Amarisoft or Anritsu Test USIM */
    amf: 0x9001, /* Authentication Management Field */
    sqn: "000000000000", /* Sequence Number */
    K: "00112233445566778899aabbccddeeff", /* Amarisoft or Anritsu Test USIM */
    impi: "901312122799083@ims.mnc001.mcc001.3gppnetwork.org",
    impu: ["901312122799083", "tel:0600000000", "tel:600"],
    //force_sms_over_sg: true,
```

Figure 36 The database for subscribers, including the SIM-card information.

The APN configuration on the mobiles is the same as in Figure 25.

Both mobiles are connected automatically to the network after configuring the APN.

The spoofed SMS has been sent through the web API of the network to find out how the network and the phone react.

The mobile phone has received the following message:

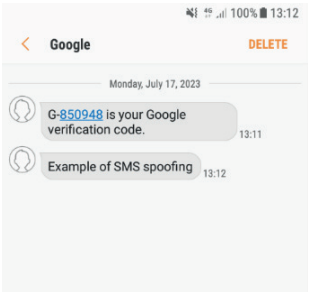

Figure 37 SMS spoofing PoC. Note how the spoofed message is placed in the same folder as previous non-spoofed messages with the same name, as if they were from the same sender.

Conclusions

In this PoC an SMS has been spoofed in a 4G mobile network setup and neither the network protocol nor the mobile phone has protection against SMS spoofing attacks. This is expected, since the SMS protocol doesn´t have authentication mechanisms. It is problematic that the spoofed SMS is placed in the same SMS inbox as the authentic sender, as is shown in this test. This may give a feeling of authenticity and trust to the user, that is not verifiable.

This type of attack can also be carried out from publicly available websites.

C.5 SMS spoofing attack for attacker with operator access rights in a 2G network

Objective

Illustrate with a PoC that an SMS in the mobile network is not authenticated and a spoofing attack against the users therefore is possible. This PoC attack is performed in the 2G network

Setup

The setup to this PoC is:

- PC: To configure the 2G network via SSH.
- 2G network (osmo): Simulates a real operator network and a base station (Ettus USRP B210).
- One mobile phone: Simulating real communication.
- One writeable SIM-card: To be able to connect to the base station.
- Ramsey Box: To work in the 2G operating frequency band without interfering with the public network.

Figure Conceptual: Figure 8

Figure Simulated:

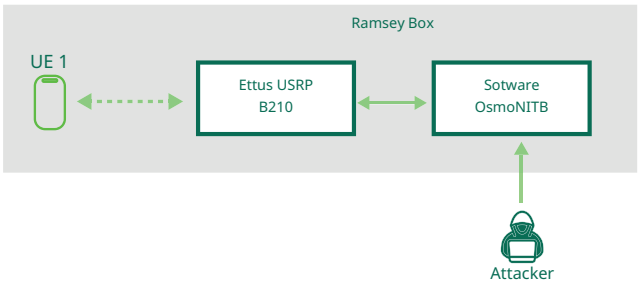

Figure 38 Simulated scenario of an SMS spoofing attack for attacker with operator access rights in a 2G network.

Configuration

The configuration to this PoC is:

1. Band GSM900.
2. Access Point Name: Default and Internet.
3. SMS over NAS.
4. Configuration SIM 1:
   a. IMSI: 101023456789
   b. Phone number: 195

Procedure

The procedure to this PoC is:

1. Configure the operator with the correct configuration parameters.
2. Configure the APN on the phone.
3. Connect the phone to the 2G network.
4. Perform the SMS spoofing by sending an SMS.
5. Check the spoofed SMS on the phone.

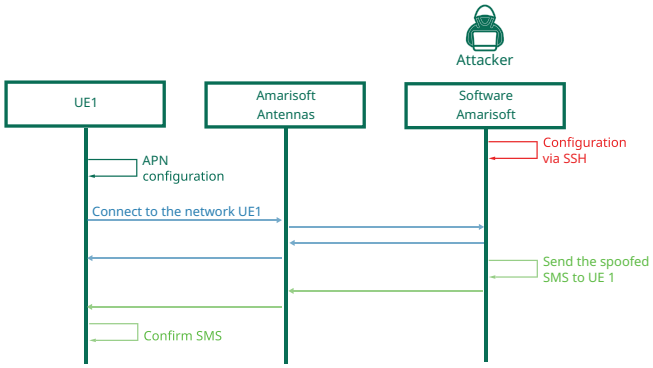

Figure 39 Procedure of an SMS spoofing attack for an attacker with operator access rights in a 2G network.

Result

The 2G network has been set up via SSH with the above parameters. Once configured, the service has been established.

The APN configuration on the mobiles is the same as in Figure 25.

Both mobiles are connected automatically to the network after configuring the APN.

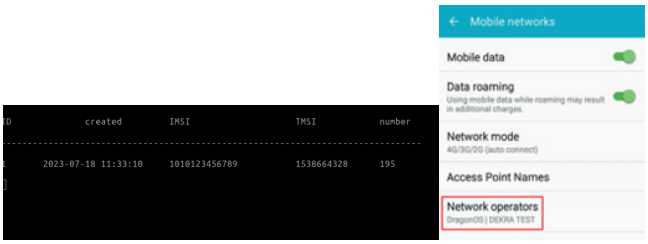

Figure 40 To the left, the terminal shows the connected phone with connection date, IMSI, TMSI and number. To the right, the phone displays connection to the DragonOS network.

The spoofed SMS has been sent through the network to see how the mobile phone reacts and receives the SMS.

The mobile phone has received the SMS as shown in Figure 41. As can be seen, the SMS displays the sender as "0", which was the sender name that was chosen for the test.

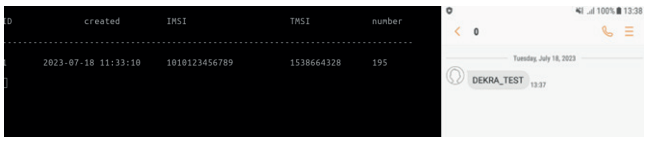

Figure 41 On the left are the registered users in the network. In this case the forged SMS was chosen from a scenario where the forged sender, „0", is not in the network. On the right the message as it was received on the mobile phone can be seen.

Conclusions

In this PoC, an SMS has been spoofed in a 2G mobile network setup and neither the network protocol nor the mobile phone has protection against SMS spoofing attacks. This is expected, since the SMS protocol doesn´t have authentication mechanisms. The PoC suffers from the same security problems as in the PoC of SMS spoofing in 4G mobile networks, which illustrates that this kind of attack is not dependent on the generation of the mobile network.

Note that this type of attack can also be carried out from publicly available websites.

C.6 Web application spoofing attack

Objective

Illustrate with a PoC that an SMS in the mobile network is not authenticated and a spoofing attack against the users therefore is possible. This PoC attack is done from a publicly available web application.

Setup

The setup to this PoC is:

- One mobile phone: With any SIM-card with a valid telephone number.
- Access to the web application (https://octopush.com/es/) in charge of sending the SMS.

Figure Conceptual: Figure 8

Figure Simulated:

Figure 42 Simulated scenario of Web application spoofing attack.

Configuration

No specific configuration to this PoC is necessary.

Procedure

The procedure to this PoC is:

1. Access to https://octopush.com/es/.
2. Send spoofing SMS from the application web.
3. Check the spoofed SMS on the phone.

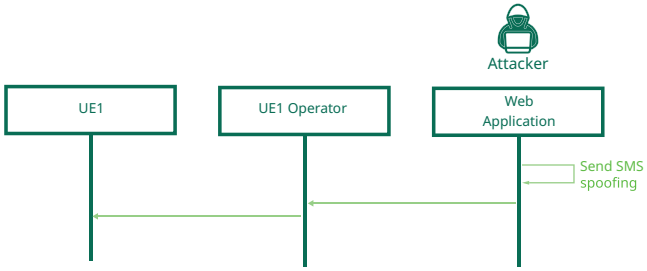

Figure 43 Procedure of Web application spoofing attack

Results

The message and sender was entered in the web application. The SMS was sent and received with the same information as entered.

Figure 44 The web application interface where the sender ID and message content was entered.

Figure 45 Screenshot of the mobile receiving the SMS.

Conclusions

In this PoC an SMS has been spoofed from a web application and neither the network protocol nor the mobile phone has protection against SMS spoofing attacks. This is expected, since the SMS protocol doesn´t have authentication mechanisms. This gives a feeling of authenticity and trust to the user, that is not verifiable.

The cost of this attack is zero, you only need an Internet connection to access the web application.

C.7 SIM swapping attack in the 4G network

Objective

Illustrate the effects of a SIM swapping attack on a 4G network.

Setup

The setup to this PoC is:

- PC: To configure the 4G network via SSH.
- 4G network (Amarisoft Callbox Classic): Simulates a real operator network and a base station.
- Two mobile phones: Simulating real network subscribers.
- Two writeable SIM cards: To be able to connect them to the base station.

Figure Conceptual: Figure 10

Figure Simulated:

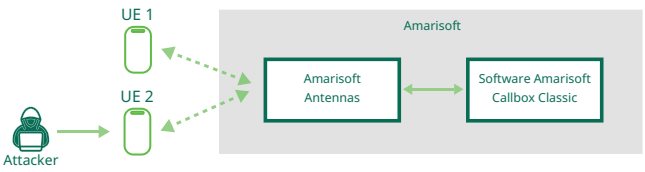

Figure 46 Simulated scenario of SIM swapping attack in the 4G network.

Configuration

The configuration to this PoC is:

1. Downlink frequency 2680MHz (Band 7).
2. Bandwidth 5MHz.
3. RRC/UP layer ciphering algorithm: 128-bit AES or Snow 3G.
4. Access Point Name: Default and Internet.
5. NAS layer ciphering algorithm: 128 bit-AES or Snow 3G.
6. SMS over IMS.
7. Configuration SIM 1:
   a. Algorithm SIM: XOR
   b. IMSI: 0010101023456789
   c. K: 00112233445566778899aabbccddeeff
   d. Number Phone: 0600000000
8. Configuration SIM 2 (After):
   a. Algorithm SIM: milenage
   b. IMSI: 0010101023456788
   c. K: 00112233445566778899aabbccddeeff
   d. Number Phone: 0600000000

Procedure

The procedure to this PoC is:

1. Configure the operator with the correct configuration parameters.
2. Configure the APN on the phone.
3. Connect the phone to the 4G network.
4. Perform the SMS test.
5. The attacker calls the operator to request a SIM change with the same phone number.
6. Configure the APN on the attacker's phone.
7. Connect the attacker's phone to the 4G network.
8. Perform the SMS test.

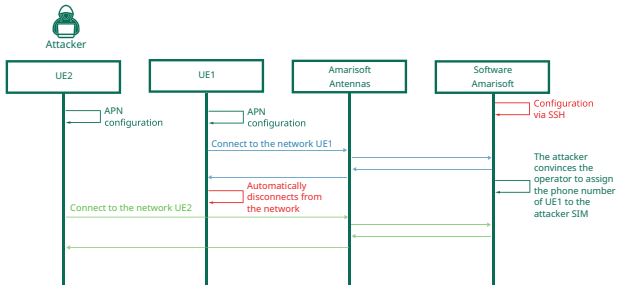

Figure 47 Procedure of SIM swapping attack in the 4G network.

Results

The 4G network has been set up with SSH with the given parameters. Once configured, the service is established.

The configuration of the SIM-card is given in Figure 48.

```
ue_db: [{
    sim_algo: "xor", /* USIM authentication algorithm: xor, milenage or tuak */
    imsi: "001010123456789", /* Amarisoft or Anritsu Test USIM */
    amf: 0x9001, /* Authentication Management Field */
    sqn: "000000000000", /* Sequence Number */
    K: "00112233445566778899aabbccddeeff", /* Amarisoft or Anritsu Test USIM */
    impi: "901312122799083@ims.mnc001.mcc001.3gppnetwork.org",
    impu: ["901312122799083", "tel:0600000000", "tel:600"],
    //force_sms_over_sg: true,
```

Figure 48 The database for the subscriber SIM-card previous to the SIM swapping attack.

The APN configuration on the mobiles is the same as in Figure 25.

After configuring the APN of the mobile phone, it connects automatically to the network.

A test message has been sent to the mobile phone to show that the SMSs are correctly delivered to the intended subscriber.

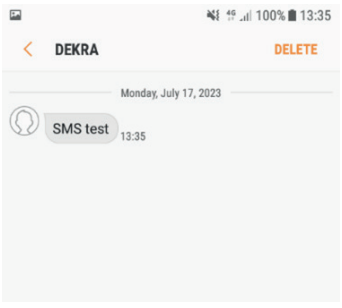

Figure 49 A test SMS is sent to the subscriber to verify that the subscriber receives SMSs as usual before the SIM swapping attack.

The attacker is then assumed to have contacted the operator and convinced the operator to change the phone number of the victim to the SIM-card of the attacker.

The configuration of the SIM-card database is changed to the information in Figure 50, which corresponds to mapping the victim´s phone number to the attacker´s SIM-card.

```
ue_db: [{
    sim_algo: "milenage",
    imsi: "001010123456788",
    amf: 0x9001,
    sqn: "000000000000",
    opc: "11111111111111111111111111111111",
    K: "00112233445566778899AABBCCDDEEFF",
    impi: "901312122799083@ims.mnc001.mcc001.3gppnetwork.org",
    impu: ["901312122799083", "tel:0600000000", "tel:600"],
    //force_sms_over_sg: true,
}]
```

Figure 50 Updated database after the attacker has solicited to move the telephone number of the victim to a SIM-card under the control of the attacker.

The victim´s phone is automatically disconnected from the network and the attacker starts receiving the messages addressed to the victim. This can be seen in Figure 51.

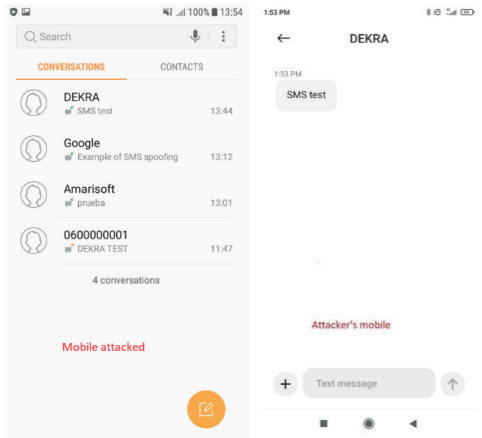

Figure 51 SIM Swapping Attack. The victim's phone to the left did not receive the test SMS after the SIM swapping attack. The attacker's phone, to the right, did receive the victim's SMS after the attack.

Conclusions

It has been illustrated how a SIM swapping attack works and that the SMS security of a user is dependent on the trust of the user data management of the operator. Note that the attack scenario could be a technical attack, but is typically the result of an attack involving social engineering.

C.8 Passive radio channel interception of unencrypted SMS in 4G with disabled crypto

Objective

Illustrate that the operator can disable encryption on the radio channel without the user detecting it, and that an attacker can capture packets on the radio channel, which in this case means plain text SMS interception.

Setup

The setup to this PoC is:

- PC: To configure the 4G network via SSH.
- 4G network (Amarisoft Callbox Classic): Simulates a real operator network and a base station.
- USB Software Defined Radio (Ettus USRP B210): Intercept downlink traffic between mobile phone and base station.
- Two mobile phones: Simulating real network subscribers.
- Two writeable SIM-cards: To be able to connect them to the base station.

Figure Conceptual: Figure 4

Figure Simulated:

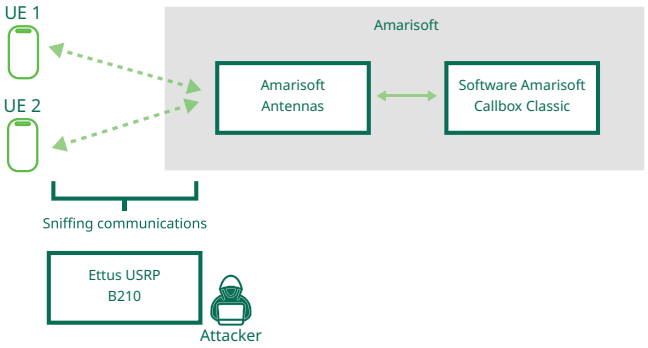

Figure 52 Simulated scenario of radio channel interception of SMS in 4G by passive external attacker.

4. Intercept the traffic downlink.
5. Send the SMS test.
6. Verify if the SMS has been captured on the downlink.

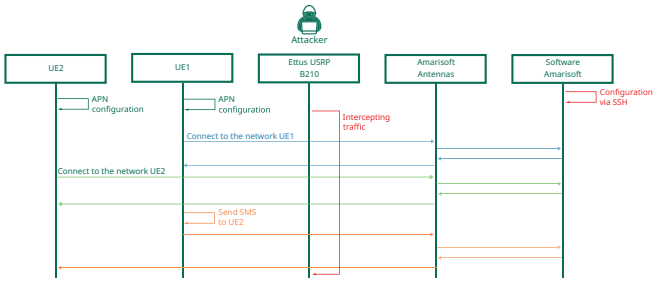

Figure 53 Procedure of radio channel interception of SMS in 4G by passive external attacker.

Configuration

The configuration to this PoC is:

1. Downlink frequency 2680MHz (Band 7).
2. Bandwidth 5MHz.
3. RRC/UP layer ciphering algorithm: None.
4. Access Point Name: Default and Internet.
5. NAS layer ciphering algorithm: None (EEA0).
6. SMS over NAS.
7. Configuration SIM 1:
   a. Algorithm SIM: XOR
   b. IMSI: 0010101023456789
   c. K: 00112233445566778899aabbccddeeff
   d. Number Phone: 0600000000
8. Configuration SIM 2 :
   a. Algorithm SIM: milenage
   b. IMSI: 0010101023456788
   c. K: 00112233445566778899aabbccddeeff
   d. Phone number: 0600000001

Procedure

The procedure to this PoC is:

1. Configure the operator with the correct configuration parameters.
2. Configure the APN on the phones.
3. Connect the phones to the 4G network.

Results

The 4G network has been set up with SSH with the given parameters. Once configured, the service is established.

The configuration of the SIM-card is given in Figure 54.

```
ue_db: [{
    sim_algo: "xor", /* USIM authentication algorithm: xor, milenage or tuak */
    imsi: "001010123456789", /* Amarisoft or Anritsu Test USIM */
    amf: 0x9001, /* Authentication Management Field */
    sqn: "000000000000", /* Sequence Number */
    K: "00112233445566778899aabbccddeeff", /* Amarisoft or Anritsu Test USIM */
    impi: "901312122799083@ims.mnc001.mcc001.3gppnetwork.org",
    impu: ["901312122799083", "tel:0600000000", "tel:600"],
    //force_sms_over_sg: true,
}, {
    sim_algo: "milenage",
    imsi: "001010123456788",
    amf: 0x9001,
    sqn: "000000000000",
    opc: "11111111111111111111111111111111",
    K: "00112233445566778899AABBCCDDEEFF",
    //force_sms_over_sg: true,
    impu: ["001010000000001", "tel:0600000001", "tel:601"],
    impi: "001010000000001@ims.mnc001.mcc001.3gppnetwork.org",
}, {
```

Figure 54 The database for the subscribers, including the SIM-card information.

The APN configuration on the mobiles is the same as in Figure 25.

After configuring the APN of the mobile phone, it connects automatically to the network.

The traffic between the mobile and the base station is intercepted with the LTESniffer configured with frequency 2680MHz, two antennas and downlink capture.

A message has been sent from one mobile phone to another as can be seen in Figure 55.

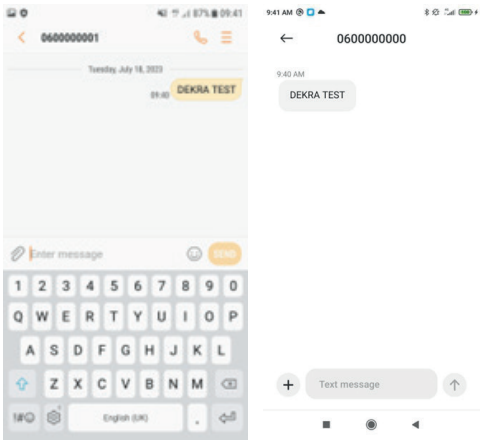

Figure 55 An SMS has been sent from mobile 2 to mobile 1, which can be observed on the screenshots of the mobile phones in the figure.

In Figure 56, the program Wireshark is used to interpret the capture created by LTESniffer and using the search term 'gsm_sms', the package with the SMS can be found in the intercepted traffic.

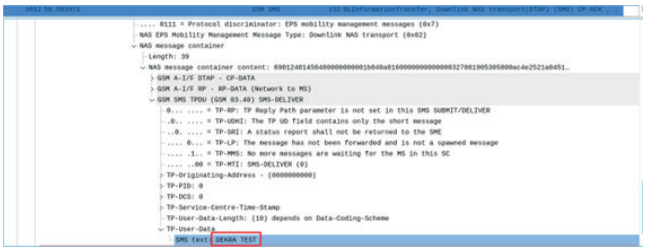

Figure 56 Screenshot from the program Wireshark, which displays the intercepted traffic on the radio channel between the network and the mobile phone receiving the SMS. The SMS content can be read in clear text.

Conclusions

In this PoC the encryption was disabled by the operator. We note that there was no notification given to the users to detect this. Using software defined radio, an attacker can easily capture the traffic on the radio channel, and in this case, with the encryption disabled, the attacker can intercept the SMSs.

C.9 Downgrade attack of 4G network service by external attacker using the radio channel

Objective

Illustration of a downgrade attack from a connection to the 4G mobile network, which would force a switch to the 2G mobile network. This can be used as a part of a composed attack.

Setup

The setup to this PoC is:

- PC: To configure the 4G network via SSH and realize the downgrade attack.
- 4G network (Amarisoft Callbox Classic): Simulates a real operator network and a base station.
- USB Software Defined Radio (HackRF): Used to saturate the frequency band in which the base station operates.
- One mobile phone: Simulating a real network subscriber.
- One writeable SIM-card: To be able to connect it to the base station.

Figure Conceptual: Figure 5

Figure Simulated:

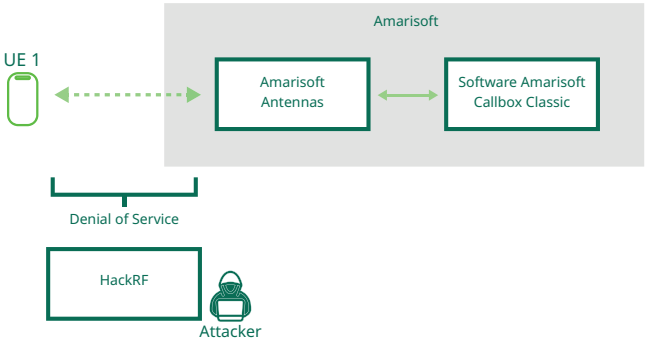

Figure 57 Simulated scenario of downgrade attack of 4G network service by external attacker using the radio channel.

Configuration

The configuration to this PoC is:

1. Downlink frequency 2680MHz (Band 7).
2. Bandwidth 5MHz.
3. RRC/UP layer ciphering algorithm: 128-bit AES or Snow 3G.
4. Access Point Name: Default and Internet.
5. NAS layer ciphering algorithm: 128-bit AES or Snow 3G.
6. SMS over IMS.
7. Configuration SIM 1:
   a. Algorithm SIM: XOR
   b. IMSI: 0010101023456789
   c. K:00112233445566778899aabbccddeeff
   d. Phone number: 0600000000

Procedure

The procedure to this PoC is:

1. Configure the operator with the correct configuration parameters.
2. Configure the APN on the phone.
3. Connect the phone to the 4G network.
4. Saturate the frequency band in which the base station operates.
5. Verify if the phone disconnects from the 4G network.

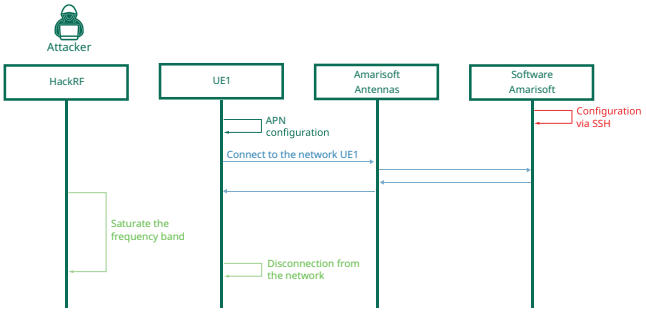

Figure 58 Procedure of downgrade attack of 4G network service by external attacker using the radio channel.

Results

The 4G network has been set up with SSH with the given parameters. Once configured, the service is established.

The configuration of the SIM-card is given in Figure 59.

```
ue_db: [{
    sim_algo: "xor", /* USIM authentication algorithm: xor, milenage or tuak */
    imsi: "001010123456789", /* Amarisoft or Anritsu Test USIM */
    amf: 0x9001, /* Authentication Management Field */
    sqn: "000000000000", /* Sequence Number */
    K: "00112233445566778899aabbccddeeff", /* Amarisoft or Anritsu Test USIM */
    impi: "901312122799083@ims.mnc001.mcc001.3gppnetwork.org",
    impu: ["901312122799083", "tel:0600000000", "tel:600"],
    //force_sms_over_sg: true,
```

Figure 59 The database for the subscriber, including the SIM-card information.

The APN configuration on the mobile is the same as in Figure 25.

After configuring the APN of the mobile phone, the mobile connects automatically to the network.

The number '*#0011#' is dialled, since this number shows the strength of the signal received by the phone from the base station.

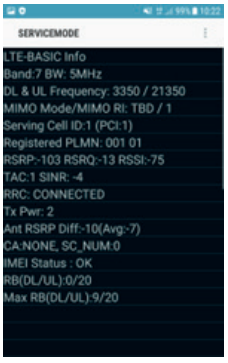

Figure 60 Network connection information such as bandwidth, bandwidth, PLMN, received signal strength parameters, connection status, etc.

The noise source was launched to saturate the signal received by the mobile phone. The important parameters for the denial-of-service attack are the center frequency (2680MHz) and the bandwidth (5MHz).

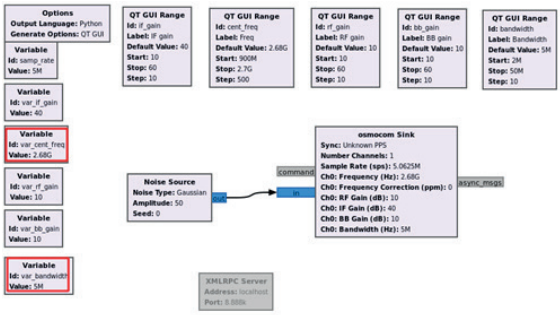

Figure 61 Signal saturator: type of Gaussian noise, the most important parameters are shown with a red box: center frequency and bandwidth.

After this program is launched, the mobile phone goes through the following disconnection process:

1) The mobile phone enters the IDLE state

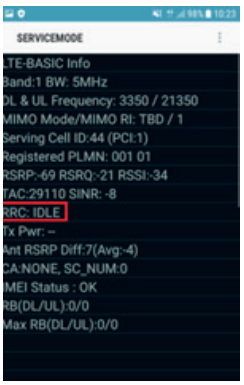

Figure 62 The phone goes into IDLE state.

2) The mobile phone is completely disconnected from the network.

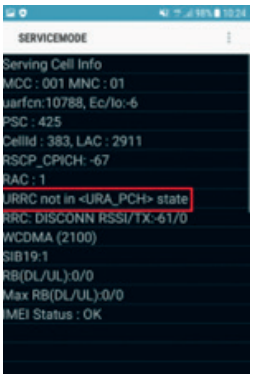

Figure 63 The phone disconnects completely.

3) The mobile phone waits for a new network, such as a 2G network.

Figure 64 The phone waits for a new network.

Conclusions

The downgrade attack has been demonstrated. The attack can be used to downgrade the service to 2G and perform other attacks using known vulnerabilities. For a practical attack, aspects of the radio channel need to be taken into account, such as proximity and sufficient signal strength to saturate the 4G network for the mobile.

The cost of this attack is low, needed is an SDR radio device, and the HackRF is priced at about $300.

C.10 Cryptographic attack on the 2G (GPRS) encryption algorithm GEA-1

Objective

Demonstrate that it is feasible to obtain the encryption key of 2G communication encrypted with the GEA-1 algorithm with a brute-force attack. This can be part of a multi-step SMS interception attack which includes downgrade to 2G, radio interception and finally decryption.

Setup

The setup to this PoC is:

- Reference implementation: To generate the target keystream.
- Attack implementation: To execute the key recovery attack.
- PC: To execute the reference implementation and the attack. The processor is an AMD Ryzen 5 3600.

Configuration

The configuration to this PoC is:

1. IV: 0
2. Direction: 1
3. Key: 0x255dc69f503597b2
4. Output keystream of reference implementation (based on input configuration): 0x734382151ab9811f

Procedure

The procedure to this PoC is:

1. Compute the target keystream of 64 bits based on the configuration input values using the reference GEA-1 implementation. This corresponds to the keystream that could be intercepted by an attacker. The encryption key used to produce the keystream is not provided to the attack, but only used to determine whether the attack was successful.
2. Perform the first stage of the attack, which consists of precomputation of the attack tables needed. This takes about 25 minutes and 73 GiB of storage.
3. Perform the second stage of the attack, which consists of an exhaustive search of the internal state, which generates different keystreams. When the reference key stream from stage 1 is found, go to the next stage.
4. Perform the third stage of the attack, which implies to reverse a part of the GEA-1 algorithm to find the key that generates this internal state.
5. Verify that the obtained key from the attack matches the key used to generate the keystream.

The procedure is illustrated in Figure 65.

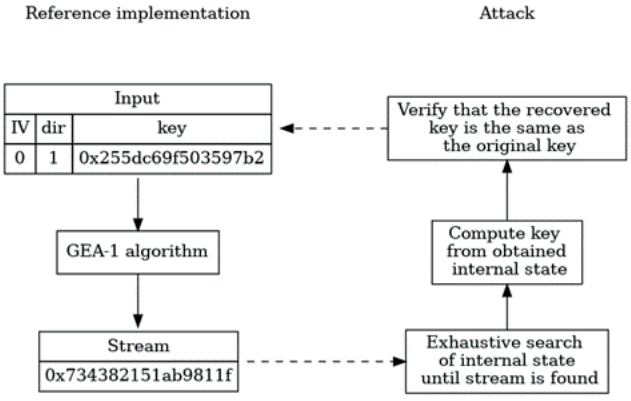

Figure 65 Procedure for the GEA-1 PoC attack.

Results

The following Python implementation of the algorithm has been used to produce 64 bits of keystream with the previous data:

https://github.com/P1sec/gea-implementation

Next, the following independent implementation has been used against the generated keystream:

https://github.com/airbus-seclab/GEA1_break

It took about 8 seconds to test 97633476 values with 12 threads to recover the state, 0x1af58754892850bf. Once the internal state was recovered, it could be reversed in a few seconds to successfully obtain the key. Lastly, it is verified that the recovered key matches the key used to generate the keystream with the independent GEA-1 implementation.

The choice of these parameters was not arbitrary. They were selected so that the internal state was one of the first tested, and so the attack would not take too much time. With a randomly selected key, the expected number of trials would be 2^39, with a maximum of 2^40. Therefore, the attack would take around 12 hours on average and a day at maximum. The testing has been done with an AMD Ryzen 5 3600. Since the search is totally parallelizable, a cluster of 12 such processors could perform the attack in less than an hour.

Conclusions

The attack is perfectly feasible with an affordable equipment and there are tools freely available to perform it. Thus, it can easily be carried out by any attacker with a low budget. The attack is related to threat scenarios 1 and 2 in Section 4, in which an attacker could passively or actively capture the radio communication between the mobile and the network and decipher it.

C.11 Cryptographic attack on the 2G (GSM) encryption algorithm A5/1

Objective

Demonstrate that it is feasible to obtain the encryption key of 2G communication encrypted with the A5/1 algorithm with a rainbow table attack. This can be part of a multi-step SMS interception attack which includes downgrade to 2G, radio interception and finally decryption.

Setup

The setup to this PoC is:

- Reference implementation: To generate the target keystream.
- Attack implementation and table: To perform the attack.
- PC: To execute the reference implementation and the attack. The processor is an AMD Ryzen 5 3600.

Configuration

The configuration to this PoC is:

1. Key: 0x6a15fd2c0300e210
2. Frame counter: 0
3. Output keystream: 11010011111100111001010 11101010111111110101110111011010110000000 10011011011000011110001110100001101100 1110000001011

Procedure

The procedure to this PoC is:

1. Use the reference implementation to obtain a target keystream of 114 bits with the input values. This corresponds to the keystream that could be intercepted by an attacker. The encryption key used to produce the keystream is not provided to the attack, but only used to determine whether the attack was successful.
2. Precompute or download the rainbow tables and prepare them with the attack implementation. The complete set of tables consume 2TB memory. It is not necessary to download the complete set to perform the attack, although the probability of success increases with the number of tables available.
3. Search the target keystream in the rainbow table using the attack implementation. The table provides the corresponding internal state. This only takes a few seconds.
4. After finding the internal state that generates the target keystream, reverse the algorithm with the attack implementation to find the key.
5. Verify that the obtained key matches the key used to generate the keystream.

The procedure is illustrated in Figure 66.

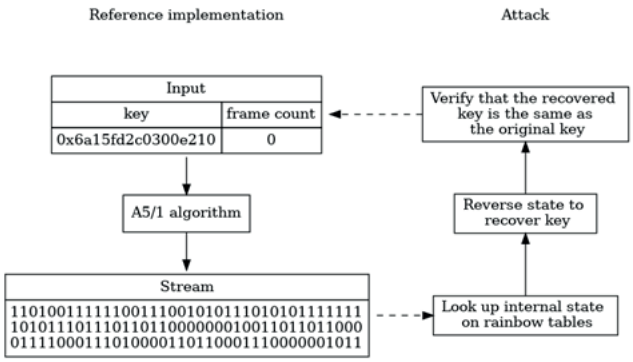

Figure 66 Procedure for the A5/1 proof-of-concept attack.

Results

The following implementation, available online, of the A5/1 algorithm was used to produce 114 bits of keystream with the previous data:

https://asecuritysite.com/encryption/a5

Next, the following, independent implementation of the attack has been used with the generated keystream as input:

https://github.com/0xh4di/GSMDecryption

The choice of parameters was made purposefully, so that not all rainbow tables had to be downloaded.

When the tables were downloaded and the software attack tool was compiled, they were allocated in a disk using the indexes/Behemoth.py script. This process takes several minutes.

Then, the Kraken/kraken tool was used to look up the internal state in the tables. It took about 4 seconds to find the state 0x952ebf0388389235, which generates the 64 bits of keystream that start at bit position 42 in the target keystream.

Then, the Utilities/find_kc script was used to reverse the state that corresponds to the 42 clock cycles and, given the frame count 0, the different possible keys for the state were displayed. Among them was the correct key that was used in the reference implementation.

Conclusions

The attack is perfectly feasible with an affordable equipment and there are tools freely available to perform it. Thus, it can easily be carried out by any attacker with a low budget. This related to threat scenarios 1 and 2 in Section 4, in which an attacker could passively or actively capture the communication between the user and the mobile network, and then decipher it, using the key recovered from an attack as demonstrated in this proof-of-concept.

References

[1] Wikipedia online, Available: https://en.wikipedia.org/wiki/SMS.
[2] 2FA Dictionary [Online]. Available: https://2fa.directory/
[3] K. Nohl, „Attacking phone privacy," in BlackHat USA, Las Vegas, 2010.
[4] C. Beierle, P. Derbez, G. Leander, G. Leurent, H. Raddum, Y. Rotella, D. Rupprecht and L. Stennes, Cryptanaly sis of the GPRS Encryption Algorithms GEA-1 and GEA-2, Cryptology ePrint Archive, Paper 2021/819, 2021.
[5] E. Barkan, E. Biham and N. Keller, „Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," in Advances in Cryptology - CRYPTO 2003, Santa Barbara, California, USA, 2003.
[6] R. B. N. A. V. N. a. J.-P. S. Altaf Shaik, «Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication System,» 2016.
[7] J. Cox, „Daily Beast," 7 March 2018. [Online]. Available: https://www.thedailybeast.com/you-can-spy-like-the-nsa-for-a-few-thousand-bucks.
[8] ENISA, „Signalling Security in Telecom SS7/Diameter/5G," 2018.
[9] Positive Technologies, „SS7 Vulnerabilities and Attack Exposure Report," 2018.
[10] Positive Technologies, „Diameter Vulnerabilities Exposure Report," 2018.
[11] Cellusys, „cellusys.com," [Online]. Available: https://www.cellusys.com/resources/ss7-vulnerabilities-ebook-download/.
[12] R. P. Jover, „queue.acm.org," September 2020. [Online]. Available: https://queue.acm.org/detail.cfm?id=3425909.
[13] C. M. Daid, „adaptivemobile.com," March 2022. [Online]. Available: https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-1.
[14] C. M. Daid, „adaptivemobile.com," March 2022. [Online]. Available: https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-2.
[15] C. M. Daid, „adaptivemobile.com," April 2022. [Online]. Available: https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-3.
[16] Positive Technologies, „Next-Generation Networks, Next-Level Cybersecurity Problems," 2017.
[17] H. Tanriverdi and M. Zydra, „Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer," Süddeutsche Zeitung, 3 May 2017.
[18] J. Ball, „theguardian.com," January 2014. [Online]. Available: https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.
[19] The New York Times, „nytimes.com," March 2022. [Online]. Available: https://www.nytimes.com/live/2022/03/16/world/ukraine-russia-war#us-officials-say-russian-troop-deaths-are-climbing-threatening-its-militarys-morale.
[20] K. Nohl and S. Munaut, „Wideband GSM Sniffing," in 27th Chaos Communication Congress, 2010.
[21] D. R. T. H. C. P. Merlin Chlosta, «LTE Security Disabled-Misconfiguration in Commercial Networks,» 2019.
[22] N. C. a. M. Olivier, A Silent SMS Denial of Service (DoS) Attack, Information and Computer Security Architectures (ICSA) Research Group.
[23] M. Benjamin, „Internal control systems and mobile money fraud: A case study of MTN Uganda," Kampala, Uganda., 2013.
[24] A. Hope, „SMS Phishing Attack Compromised Twilio Leaking Customer Data, Targeted Cloudflare," CPO Magazine, 17 August 2022.
[25] B. Leonard, „Google," 19 April 2023. [Online]. Available: https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/. [Accessed July 2023].
[26] Kaspersky, „SMS Attacks and SMS Mobile Threats," [Online]. Available: https://www.kaspersky.com/resource-center/threats/sms-attacks. [Accessed July 2023].

[27] „Emotet: How to best protect yourself from the Trojan,“ [Online]. Available: https://www.kaspersky.com/resource-center/threats/emotet.
[28] R. Brandom, „theverge.com,“ February 2015. [Online]. Available: https://www.theverge.com/2015/2/24/8101585/the-nsas-sim-heist-could-have-given-it-the-power-to-plant-spyware-on.
[29] J. Scahill and J. Begley, „theintercept.com,“ February 2015. [Online]. Available: https://theintercept.com/2015/02/19/great-sim-heist/.
[30] TCH, „TSN.ua,“ June 2022. [Online]. Available: https://tsn.ua/en/ato/russian-secret-services-have-launched-a-phycological-attack-on-ukrainian-military-using-sms-messages-of-intimidating-content-2082016.html.
[31] J. Coleman, „businessinsider.com,“ April 2022. [Online]. Available: https://www.businessinsider.com/russia-tried-incite-ukrainians-attack-their-own-capitol-via-text-2022-4?r=US&IR=T.
[32] M. Kim, J. Suh and H. Kwon, A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures, Danang, Vietnam: IEEE, 2022.
[33] ENISA, „Beware of the Sim Swapping Fraud!,“ 2021.
[34] J. Cox, „vice.com,“ January 2020. [Online]. Available: https://www.vice.com/en/article/5dmbjx/how-hackers-are-breaking-into-att-tmobile-sprint-to-sim-swap-yeh.
[35] K. Lee, B. Kaiser, J. R. Mayer and A. Narayanan, „An Empirical Study of Wireless Carrier Authentication for SIM Swaps,“ in USENIX Security Symposium, 2020.
[36] J. Koelndorfer, N. Hopper and Y. Kim, „Location Leaks on the GSM Air Interface,“ 2011.
[37] E. Bitsikas, T. Schnitzler, C. Pöpper y A. Ranganathan, «Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings,» 2023.
[38] S. P. J. S. P. B. Erik Dahlman, 3G Evolution - HSPA and LTE for Mobile Broadband, Academic Press, 2007.
[39] „Real Time Communication,“ 2022. [Online]. Available: https://realtimecommunication.wordpress.com/2022/02/18/smsc-30-years-after/.
[40] Ettus, „Ettus,“ [Online]. Available: https://www.ettus.com/all-products/ub210-kit/.
[41] „Amarisoft,“ [Online]. Available: https://www.amarisoft.com/app/uploads/2022/03/userguide_callbox_classic.pdf.