Implementing an Affordable and Effective GSM IMSI Catcher with 3G Authentication

Max Suraev(✉)

Security in Telecommunications,Technische Universität Berlin, Berlin, Germany
max@sec.t-labs.tu-berlin.de

Abstract. Recently revealed information on secret agencies eavesdropping on the politicians' phone calls all over the world, have shown how common practice it is. Although the insecurity of the mobile telecommunication system GSM has been known in the scientific community, these events made it clear to the public. Particularly, the extent and usage of such techniques demonstrates its relevance in the current society. In this paper, we will demonstrate techniques used to intercept mobile calls and analyze the feasibility of man-in-the-middle attacks in real-life scenarios. We show how to build an affordable and effective IMSI catcher which works even when mutual authentication between phone and a network is enforced. The methods to detect it and other potential countermeasures are discussed as well.

Keywords: Security · Mobile · Privacy

1 Introduction

The recent news about Edward Snowden's ongoing disclosure reveal the National Security Agency's (NSA) mass surveillance program. The Leaked document indicates that the NSA spied on 35 world leaders [8]. Moreover, the NSA is not the only intelligence organization performing such activities, and it seems that it became a common practice [12]. The core issue here is not the very fact of surveillance but the lack of warrant for such programs. The tool often utilized for implementing such programs in the field is an IMSI catcher.

In GSM only the subscriber is authenticated to the network. The network does not have to authenticate to the subscriber [5, Sect. 4.3.2b]. This allows the communication to be billed to the appropriate subscriber, but because of the lack of mutual authentication, any base station (BTS) can pretend to belong to any operator, and lure the corresponding subscriber group to itself. Such BTS devices are called IMSI catchers. Their original purpose was merely to collect the International Mobile Subscriber Identity (IMSI) of the subscribers, which the phone sends while trying to attach to their base station and register on the falsely advertised network. This reveals the presence of GSM devices nearby and allows to geolocate them. The same would apply to 3G and 4G networks as well — mobile device is expected to first reveal its basic identity information

J. Tian et al. (Eds.): SecureComm 2014, Part I, LNICST 152, pp. 239–256, 2015.
DOI: 10.1007/978-3-319-23829-6_18

before attempting to run any security protocols. However, in GSM the lack of end-to-end security allows IMSI catcher to function as a full base station. While forwarding the traffic from the subscriber to the real network, the attacker intercept the ongoing communication. Such capability was offered by the GA 900 from Rohde & Schwarz in May 1997 [9]. Furthermore, this flaw allows additional man-in-the-middle attacks to be performed, although with somewhat relaxed definition of an attack [17]. Normally attacker is standing between communicating parties representing each one of them at the same time. This is not the case in the attack described in [17] — attacker is unable to pretend to be the mobile and the network at the same time, traffic forwarding have to be organized by some other means. The practical limitations of such approach are further discussed in Sect. 4. Nowadays it is even possible to build an IMSI catcher using commodity hardware and open source software [25].

In most of the countries legislation mandates telecommunication operators to provide an interface to their network for lawful interception of traffic and geolocation of the subscribers. This allows the appropriate authorities to perform their duties in preventing crimes, provided they obtained the appropriate warrant. IMSI catchers are, however, allow eavesdropping telecommunication where the interested party has no access to these lawful interception interfaces, particularly in foreign countries.

IMSI catchers work quite well in GSM because of the lack of mutual authentication. One could argue that this has already been fixed in 3G networks like UMTS, as well as the 4G network LTE. Modern phones support 3G and 4G,[1] however, very few phones allow you to enforce 3G and 4G only, and not by default. Moreover, GSM still dominates the network coverage: while nearly 100 % of the population and 90 % of the territory is covered by GSM in Europe, 3G coverage is only available in 68 % of the territory, where 90 % of the subscribers live [11]. In developing countries the difference is even greater, where 3G is only available in major metropolitan cities due to higher cost and lower per-cell coverage of 3G. Thus, turning off GSM on phones would leave a significant number of users without mobile connectivity.

Another important aspect for continuous operation of GSM is the industry. The number of 2G connections is barely decreasing, because it is now used by various industry standards and networks. For example Machine-to-Machine (M2M) and Internet-of-Things (IoT) networks use equipment, which only has GSM modems, as these fulfill the requirement and are cost-effective. The GSM-for-Railroads (GSM-R), communication standard for railways currently rolled-out throughout Europe, is also based on GSM. In general, GSM will not disappear in the foreseeable future, and thus its inherent weaknesses is here to stay.

We can use this to our advantage. Using the off-the-shelf equipment and free software, it is possible to create an GSM base station for $1500, and build an affordable and easy to obtain IMSI catcher out of it [25]. Moreover, by knowing the inner works and characteristics of IMSI catcher techniques, it is possible

[1] Alongside with GSM which is the common denominator of supported protocols.

to integrate these aspects so to make it stealthy and hardly detectable by the user. Even with mutual authentication added to GSM, IMSI catchers remain useful: using the flaw presented in [16] allows circumventing authentication and implement successful attack, shown in this paper.

1.1 Contributions

The contributions of this paper are following:

- Shown how to configure and inexpensive, readily available base station to build an efficient IMSI catcher with UMTS authentication, and intercept communications.
- Tested the behavior of the phones from different manufacturers when exposed to GSM IMSI catcher, which support the UMTS authentication procedure over GSM air interface.
- New security vulnerability affecting vast majority of baseband vendors discovered.
- Tested GSM IMSI catcher implementation capable of circumventing the mutual authentication.
- Reviewed the methods to detect IMSI catchers, and accordingly ways to build a stealthy solution.

To the best of the author's knowledge, it has only been shown how to build an IMSI catcher [25], but not how to make it efficient and stealthy. While the mutual authentication has been proven as flawed in GSM [16], no publicly available, practical implementation and analysis has yet been done. This partially explains why vulnerability described in Sect. 5 has not been found before.

The rest of this paper is organized as follows: related work is covered in Sect. 2, hybrid mobile networks described in Sect. 3, the attack is explained in details in Sect. 4. Attack feasibility and previously undisclosed security vulnerability found while testing against basebands from various vendors discussed in Sect. 5. The paper concludes with Sect. 6. Details on software and hardware used in this work are available in Appendix.

2 Related Work

The theoretical feasibility of man-in-the-middle attack was described in [16], although the attack practicality has been questioned [19]. The reason for that is that attack presented in [16] is not, strictly speaking, classical man-in-the-middle attack when attacker pretend to be the mobile network to the phone and pretend to be the phone to the mobile network while transparently forwarding traffic between them. What actually presented is the authentication protocol flaw, which allows to circumvent mutual authentication between the mobile phone and the network. This is not enough to build complete man-in-the-middle but combining it with other techniques allows to create viable attack in some scenarios as shown in Sect. 5.

The purpose of the IMSI catcher is to become the GSM cell selected by the target phone so it will have access to all the traffic generated by the phone and will be capable of generating arbitrary traffic for the phone. Authors of [23] describe such a device in great detail. Another implementation is presented in [25]. However, both devices do not consider the operation of GSM network as a radio frontend for UMTS network, which is the most common case nowadays.

There are systems designed to detect operations of IMSI catcher [15] either via observing anomalies related to the radio interface, like disappeared encryption or by detecting location attempts with silent SMS. However, no definite method has been proposed so far: IMSI catcher can use A5/1 encryption and break it using well-known attacks like the one implemented in [13]. The absence of paging traffic on a given BTS while it is present on other BTS in the same LAC is a certain give-away for IMSI catcher. This traffic, however, could be emulated or obtained from existing operator cell and repeated. This would increase the load on the IMSI catcher due to incoming RACH requests from paged phones. The victim's location information might be obtained from other sources without the need to use silent SMS or call, which are easily detectable by the target phone.

In case of GSM-R network the scarce distribution of BTSes might lead to false positive IMSI catcher detection based on the lack of neighboring cells in broadcast traffic of the GSM-R BTS [15].

3 GSM Network with UMTS Authentication

In this section, we describe how GSM and UMTS networks are glued together. First, we review GSM and UMTS authentication procedures over radio network and then provide an overview of interactions with SIM and USIM during authentication between the mobile phone and the network.

3.1 Authentication

The GSM and UMTS authentication procedures are described in [17] in great detail. Due to the gradual transition by telecom operators between generations of mobile networks, it might happen that the core 3G network is connected to both 2G and 3G base stations. The same applies to 4G.

In case of hybrid network where GSM acts as a radio frontend for the UMTS core, the AUTN (UMTS authentication token) is transmitted as an extension data in the Authentication Request message [5, Sect. 9.2.2] alongside with the RAND challenge.[2] This data is supplied to the USIM, which has the secret key (K) needed to produce an Authentication Response [5, Sect. 9.2.3] and corresponding ciphering (CK) and integrity (IK) keys.

Unlike in GSM authentication, AUTN contains MAC and protected sequence number ($SQN \oplus AK$, where AK is derived according to Fig. 1), which must be

[2] Older phones, which do not support UMTS authentication will ignore it.

used to verify the authenticity and the freshness of the request. The presence of the MAC is supposed to prevent man-in-the-middle attack: phone computes the MAC using secret key K and compare it to the MAC received as a part of the AUTN to verify that authentication is requested by a legitimate network. Replay attack protection is ensured by the fact that the actual value of the SQN is unknown, the only way to unmask it is by xoring data received from the network with AK, which requires the same secret key K used in the MAC computation. The value of the SQN is updated with every authentication attempt by both network and phone and if the SQN expected by the phone does not match the one provided by the network, it might trigger a resynchronization procedure instead of an authentication.

3.2 (U)SIM

What is commonly known as USIM is actually a smartcard conforming to the UICC standard [3] which might have SIM and USIM applications running inside.

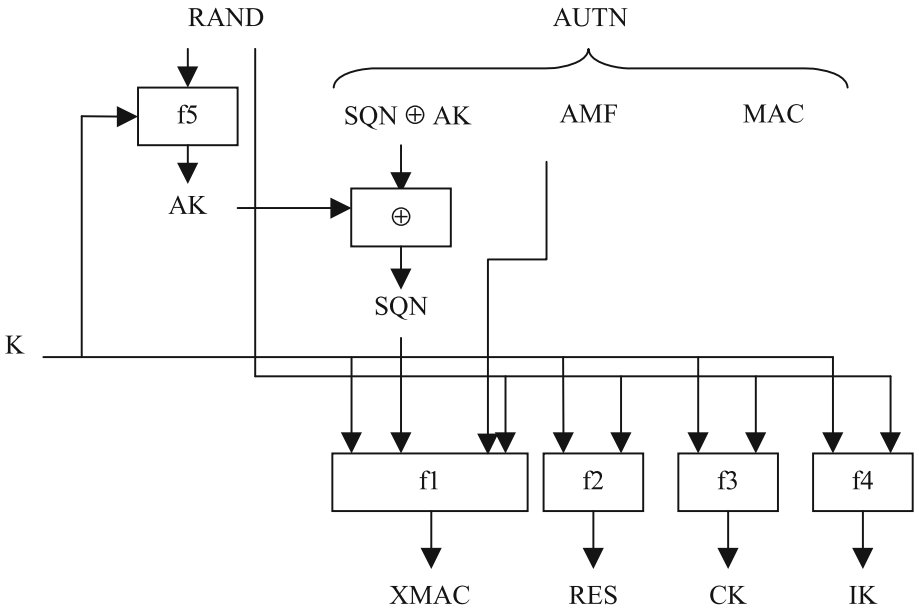

Fig. 1. Key generation [6, Sect. 6.3.2].

The interaction of key generation functions is shown in Fig. 1. This function is run by the operator's authentication center and inside the USIM application on the smartcard: it uses a secret key K, which is stored inside the USIM and is not supposed to be directly accessible from outside. Note that during the attack we have access to RAND and AUTN parameters but not to K (which is never transmitted over the air), so we are unable to know the exact value of the sequence number SQN, since it is masked with AK.

The USIM compares the XMAC (value from the f1 function) with the MAC (the value received from the radio interface) to verify request authenticity. Then RES is sent back to the base station for verification (this is how the network verifies the authenticity of the phone). IK and CK are used to derive the GSM ciphering key $K_c = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2$, where xK_n is 64 bit long part of the corresponding key [6, Sect. 6.8.1.2]. RES, ciphering and integrity keys are only generated by the USIM if the sequence number matches its expectation, otherwise, re-synchronization message AUTS, which consists of expected SQN masked with AK and corresponding MAC, is computed [6, Sect. 6.3.3].

3.3 IMSI Catcher

To avoid detection by systems like [15], IMSI catcher should mimic the work of a real network as closely as possible.

There are 3 types of IMSI catcher possible:[3]

- GSM IMSI catcher.
- Hybrid IMSI catcher.
- UMTS IMSI catcher.

GSM IMSI catcher rely on by-design insecurity of GSM, where the network never authenticates itself to the phone. UMTS IMSI catcher is possible if an attacker could gain access to the operator's internal network by, for example, by breaking into femtocell [10]. This grants indirect access to operator's authentication center, which allows attacker to request authentication credentials at any time. The hybrid IMSI catcher described in this paper uses a corner-case when the GSM radio interface is used to communicate with the UMTS core to circumvent mutual authentication without direct access to operator's network.

To build IMSI catcher and avoid detection one must understand cell selection procedures used in GSM. When phone is looking for GSM cell to connect to, it chooses the one with highest C_1 value (path loss criterion). It is calculated as follows [1, Sect. 6.4]:

$$C_1 = RLA_C - RX_{MIN} - \max(MS_{TX} + P_{OFF} - P, 0) \tag{1}$$

where RLA_C is a running average of received signal level, RX_{MIN} is the minimum received signal level at the mobile station (MS) required for access to the network, MS_{TX} is the maximum transmission power level an MS may use when accessing the network and P is the maximum RF output power of the MS. More details on power offset P_{OFF} and other parameters can be found in [23]. It is important to notice that the cell with the highest radio transmission power (RLA_C) as observed by a phone is not necessarily the one with highest C_1 value calculated according to Eq. 1. The RLA_C is measured by the GSM radio modem, while RX_{MIN}, MS_{TX} are part of BTS configuration and broadcasted alongside with other information. P is a characteristic of MS radio transmitter capabilities.

[3] The case of LTE is not considered in this paper and left out for future work.

The cell reselection procedure is only relevant to the continuation of traffic interception. In our case cell selection procedure is employed for the attack by both target and attacking phones. Baseband of the attacking phone is not powered before the attack and jammer forces target phone to switch from UMTS to GSM — in both cases phones have to use cell selection procedure. The neighbor list consists of the base stations[4] regularly broadcasted by each cell. The phone is expected to monitor cells from this list to check whether it is worth switching over to one of them.

To prevent the phone from triggering cell reselection away from the IMSI catcher, it should have a higher C_2 value than any of the neighbor cells monitored by the phone [1, Sect. 6.6.2]. It is calculated as follows:

$$C_2 = \begin{cases} C_1 + C_R - T_{off} * \mathcal{H}[T_{pen} - T] & \text{if } T_{pen} \neq 11111, \\ C_1 - C_R & \text{if } T_{pen} = 11111. \end{cases} \tag{2}$$

where C_R is cell reselection offset, T_{off} is temporary offset, T_{pen} is penalty time, T is a timer implemented for each cell in the list of strongest carriers [1, Sect. 6.6.1] and $\mathcal{H}[x]$ is a discrete form of Heaviside step function. The idea behind timer T is to prevent fast moving mobile from performing unnecessary location updates in small-coverage cells: this timer is started when a new cell is added to the list for monitoring and if the cell coverage is small and MS is moving fast enough it will pass by before T_{pen} is reached without triggering cell reselections.

The correspondence between parameters used in [1], the variables in Eq. 2 and BTS configuration options used in actual experiments is summarized in Table 3.

Broadcasting non-existent neighbor cell list will effectively lock down target phone to the IMSI catcher but it will also make IMSI catcher's detection much easier, hence the preferred method for avoiding cell reselection is to broadcast authentic neighbor cell list but give IMSI catcher high C_2 value by setting high C_R and setting $T_{off} = 0$.

4 Attack

We have implemented the attack first described in [16]. The messages exchange between involved parties during the attack is shown in Fig. 2.

There are two distinct stages of the attack clearly visible in Fig. 2: before and after the credentials extraction step. The first stage is when XGoldmon-compatible (see Sect. 6 for details) phone with USIM card programmed with the target's IMSI and a random secret key K is attempting to camp on the operator's network. The attacking phone could be configured to use UMTS-only networks to avoid interference from our own IMSI catcher.[5] When fresh credentials are

[4] Up to 6 cells in GSM and up to 15 in UMTS.

[5] Not all the phones supported by XGoldmon provide such option.

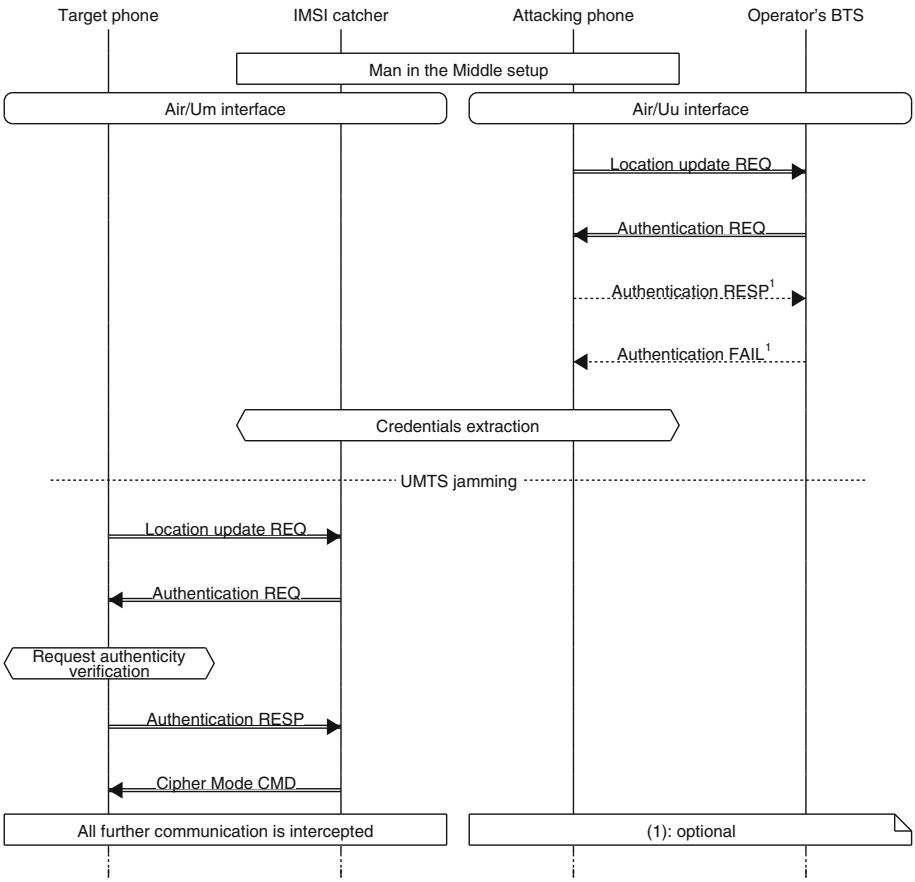

Fig. 2. Attack outline.

received from the operator The second stage begins. The credentials are re-used by the IMSI catcher, which supplies them to the target mobile phone.

The response messages from the attacking phone (the last two messages of the first attack stage, which are marked as optional in Fig. 2) will fail authentication and might lead to the operator banning mobile phone (by IMEI) from accessing the network if an authentication is attempted too frequently. However, we can stop the bogus authentication messages from reaching the operator's network by interrupting the communication between SIM card and the attacking phone using a specially crafted firmware for simtrace — see Sect. 6 for details. This helps to prevent the operator from banning attacking phone due to multiple failed authentication attempts.

The timing requirements between those two attack stages are rather flexible: the freshness of the necessary credentials is determined not by the time elapsed since last authentication attempt but by whether target phone performed authentication with the operator's network between the attack stages or not. See the explanation on SQN usage in Sect. 3.2.

Each stage begins with the phone sending a Location Update Request message to the BTS, followed by an Authentication Request message from the BTS, to which the phone replies with an Authentication Response. The Location Update Request is used by the mobile phone to update the BTS on its status. The Authentication requests sent during the first and second stage of the attack are identical — the whole purpose of the first attack stage is to obtain correct credentials, so that verifiable Authentication Request could be constructed during the second attack stage. Target phone response is received by the attacking BTS and the Cipher Mode Command issued without attempting any verification (that would require access to secret key K which we do not have). This gives the IMSI catcher full control over the encryption used by the target phone.

The attack is possible because there is no integrity protection for the Cipher Mode Command in GSM and RAND and AUTN parameters are available in clear text. In UMTS the corresponding Security Mode Command is both integrity protected and includes security capabilities transmitted by the phone. This allows the phone to easily detect an attempt to use weak or no encryption by an attacker [16].

Although the attack is called man-in-the-middle in [16], in practice it is impossible to impersonate the mobile phone to the operator's network while performing successful impersonation of the GSM BSS to the target phone. There are four potential scenarios for the phone impersonation depending on the combination of UICC profile and phone baseband capabilities, which we are trying to exploit:

Table 1. Phone impersonation requirements

Type	SIM	USIM
GSM	SRES, K_c	XRES, K_c
UMTS	SRES, K_c	XRES, CK, IK

Due to lack of access to the secret key K_i stored in the (U)SIM used by the target phone, we have to obtain the information presented in Table 1 to successfully impersonate the target phone to the original network and perform a complete man-in-the-middle attack. The problem is that we cannot reuse XRES, which we have obtained during the attack described in Sect. 4 because it is derived from RAND chosen by the network and is explicitly protected from reuse by the sequence number SQN synchronization mechanism [4, Sect. 6.3.2]. Moreover, even if we force same RAND and derive SRES from XRES according to Eq. 3, we still would not be able to perform impersonation with the K_c, which we could have after breaking A5/1 for example. The K_c used in pure GSM is computed as $K_c = COMP128(RAND, K_i)$, while in our case it is derived from UMTS keys CK and IK as $K_c = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2$. An additional challenge is imposed by the fact that security capabilities (available encryption algorithms) sent by the mobile phone to the network will be mirrored back to the phone by UMTS network with the Security Mode Command, protected with IK.

This limits the scope of the implemented attack. There are, however, few use cases where such an attack is still feasible. For example, when performing a targeted attack, a social engineer might be interested in placing call from particular number towards the target (for example, a call from the head of department phone number for added credibility). In this case the lack of the target phone impersonation is irrelevant since the IMSI catcher is capable of supplying any desired phone number as a call origin. Another use case is the detection of planted GSM bugs (wiretapping devices) in the office building. Here we do not want to provide connectivity to the original command and control servers hence there is no need for GSM bug impersonation.

Without a proper target phone impersonation, we can implement man-in-the-middle attack by forwarding target phone calls and SMSes using VoIP service. The downside is that the call recipient will see incoming call from the VoIP operator number instead of expected target phone number, which will reveal the man-in-the-middle attack. In case of long-distance calls, however, it is often the case even without IMSI catcher: telecom operators sometimes rely on cheaper intermediary VoIP operators to decrease traffic cost, which leads to essentially the same effect. In the set of test calls from a mobile phone in Germany to mobile phones in Russia, some calls were indicated as originating from short numbers, Russia-based numbers or no number information was given to the call counterpart at all.[6]

Using VoIP operator might be advantageous to attacker in other way as well: it is possible to arrange the use of custom sender-ID to make sure that intercepted calls and SMS will arrive from the expected number. However, this option obviously exposes the attacker to the VoIP operator and, potentially, law enforcement agencies having legitimate access to the operator's infrastructure. Also, this feature is unavailable in some countries due to local laws and it hardly could be considered an inexpensive solution.

4.1 Experimental Setup

The experimental setup consisted of a Samsung Galaxy phone[7] acting as an attacking phone, connected to a laptop running modified OpenBTS software, which acted as an IMSI catcher using UmTRX radio frontend. More details on software and hardware used for the attack implementation and verification can be found in Appendix.

4.2 Success Verification

There are plenty of cases where authentication and key agreement between different mobile network standards performed [24]. That is why it is essential to understand what is happening within the target phone exposed to our IMSI catcher.

[6] Another explanation would be the pervasive use of IMSI catchers in Germany of course.

[7] Both SII and SIII models.

For that we will analyze over-the-air messages between the target phone and an IMSI catcher and the messages exchanged between the target phone modem and its USIM card. In particular we will have a look at SRES (GSM response) and XRES (UMTS response) parts of the Authentication Response. According to [6, Sect. 6.8.1.2] the conversion performed using following formula:

$$SRES = XRES_1^* \oplus XRES_2^* \oplus XRES_3^* \oplus XRES_4^* \tag{3}$$

where

$$XRES^* = \begin{cases} XRES & if \parallel XRES \parallel == 128, \\ XRES \parallel 0 \ldots 0 & if \parallel XRES \parallel < 128. \end{cases} \tag{4}$$

and $XRES_i^*$ are 4 byte chunks of $XRES^*$. Note: in Eq. 4 length is given in bits.

However, when the phone supports UMTS authentication, there is no need to make such conversion. According to [5, Sect. 10.5.3.2.1], the most significant bytes of XRES are transmitted in place of SRES (5161ca9b in Fig. 3) while the rest is transmitted as an extension to Authentication Response message. It can be observed in Fig. 3 which shows the example attack in wireshark[8] traced from points of view of both attacker (BTS and attacking phone) and victim (phone and SIM card) via GSMTAP with the help of XGoldmon and simtrace tools.

If the target phone is an old phone without UMTS authentication support than the first bytes of XRES are interpreted as SRES and the UMTS extension is ignored. In this case, the attack is an example of the classical GSM IMSI catcher described in [23].

Note that both Authentication Request (downlink) and Response (uplink) are shown twice because they appear first in the BTS GSMTAP flow than in XGoldmon GSMTAP flow.

We can verify that the phone indeed performed UMTS authentication procedure and responded with unconverted XRES value. For that we take RAND value (left side of Fig. 3) and use it to request authentication data from the SIM card using the osmo-sim-auth tool. The result is compared with the SRES value calculated by substituting XRES data from Fig. 3 into the formula from [6, Sect. 6.8.1.2]:

```
./osmo-sim-auth.py -s -r c313af9c5f3496c7f2b8acd448b7cb68

GSM Authentication
SRES:    38255549
Kc:      e10d4807f0b94ffd
```

Substituting values from the traffic dump into Eq. 3 we can show that indeed:

$$\texttt{0x38255549} == \texttt{0x5161CA9B} \oplus \texttt{0x69449FD2}$$

Hence, the phone sent the unconverted result of the UMTS authentication procedure.

[8] The results may vary depending on the dissectors available to Wireshark tool.

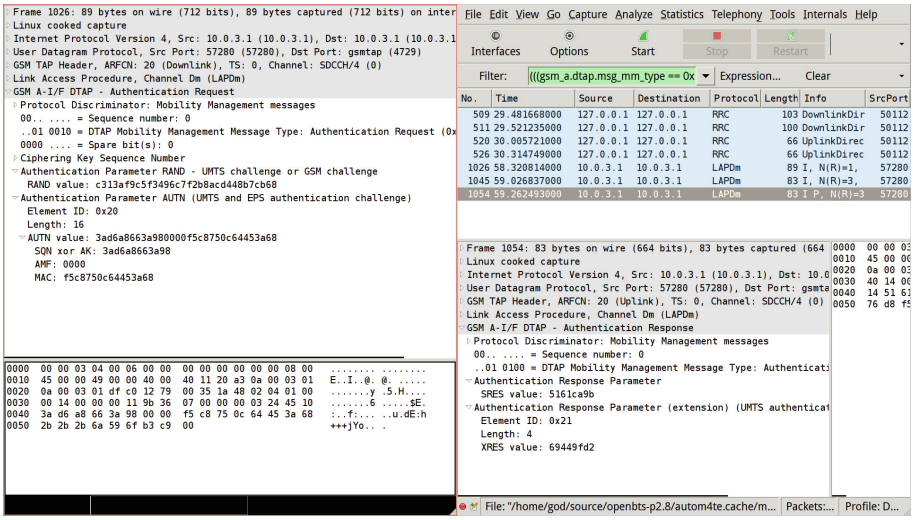

Fig. 3. Attack traffic dump.

Another verification of the attack success (besides the fact that victim phone responded with "Authentication response" instead of "MAC failure" or "Sync failure") can be obtained by carefully studying the interaction between phone and the SIM card. Figure 4 shows the phone requesting SIM card to perform authentication. Unparsed data in GSM SIM 11.11 begins with 00 88 00 81 which, according to [4, Sect. 7.1.2], means that USIM AUTHENTICATE function (88 00) was called in 3G security context (81).

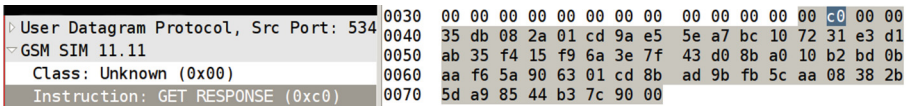

Fig. 4. Victim SIM request and response.

The SIM card response is shown to the right in Fig. 4. The GSM 11.11 field begins with 00 C0 00 00 35 DB, which according to [4, Sect. 7.1.2.1], means that the authentication function succeeded (DB). Following bytes are RES length, RES itself, length of CK, CK itself and the remaining output of the authentication procedure.

Thus, we have verified that when the target phone connects to our IMSI catcher, the UMTS authentication is indeed takes place. This, however, is just one part of the overall attack: first we have to make sure that the target phone actually connects to us and we have to handle the traffic to and from the phone to make the attack practically feasible, which is described in greater details in Sect. 5.

5 Feasibility

Theoretical attacks can be modeled for formal verification and studied using simulation. The comprehensive overview of interoperability between various generations of mobile networks is given in [24]. However, as it was shown in [18] it is easy to overlook some details due to the complexity of choosing the correct assumptions for a formal model. That is why practical implementation and field experiments with real hardware are essential and cannot be replaced with simulation only.

Table 2. Baseband behavior on MAC failure

Phone	Vendor	Version	Call in/out	SMS in/out
iPhone 5	Qualcomm	10b350 3.04.25	OK/OK	OK/OK
iPhone 4	Qualcomm	MC605IP/A 04.12.09	OK/OK	OK/OK
Galaxy S2	Infineon	I9100BOLP5	OK/OK	OK/OK
Galaxy SIII	Infineon	I9300BOLF1	OK/OK	OK/OK
Samsung corby pro	unknown	B5310AEJ1	OK/OK	OK/OK
Google nexus 1 (HTC)	Qualcomm	32.41.00.32U 5.08.00.04	OK/OK	OK/OK
Geekphone	Qualcomm	unknown	OK/OK	OK/OK
Keon	Qualcomm	unknown	OK/OK	OK/OK
Nokia N900	Nokia	20.2010.36-2	blocked	blocked

During the experiments, we have observed peculiar behavior of many phones in case of a MAC failure. According to [5, Sect. 4.3.2.6], if a MAC failure is detected, the phone should stop all further communication with the BTS in question. Moreover, [2, Sect. 3.5.5] explicitly specify that such a cell should be treated as barred for timer T3212 minus one minute (if available) or for 12 hours by default. Most of the phones, however, proceed as if authentication succeeded. The behavior of different models is summarized in Table 2. Information about the version of the phone baseband or even on the vendor of the baseband for a particular model is not always available. Note that none of the phones indicated any error to the user regardless if it allowed for calls or SMS.

This violation of the GSM standards is not just a mere testing oversight: it puts both user's privacy and its voice and SMS traffic confidentiality at risk. The widespread lack of even basic security status indication on many phones leaves affected users unaware of the very presence of this dangerous vulnerability.

Given the very limited number of baseband vendors, this means that the majority of the phones available on the market do not even attempt to use security improvements offered by UMTS. This makes IMSI catcher attack highly practical: even if correct authentication challenge was not obtained in time to execute man-in-the-middle attack, the IMSI catcher still might intercept all the voice calls and SMS from the phone.

5.1 Countermeasures

Similarly to other man-in-the-middle attack implementations, IMSI catchers can operate due to either lack of mutual authentication between communicating parties or due to some flaws discovered in authentication protocols. Sometimes, however, users consciously choose communication over insecure channel as an acceptable security risk: for example when accepting self-signed certificate in web browser to access website, which does not contain highly valuable information or request access credentials. In mobile communication such situations arise inevitably: legal requirements clearly hold safety (ability to place emergency call) higher than security.

Complete assurance from man-in-the-middle attacks is impossible as long as we would like to preserve backward compatibility with insecure communication technologies. However, it does not mean that we should make an attacker's job easier. To make IMSI catcher attacks harder to implement, baseband authors should follow security procedures described in 3GPP standards.

Broken ciphers like A5/1 should be phased out, although judging from the time required for A5/2 withdrawal, this might take very long time. It also might be difficult due to the backward compatibility issues.

Nevertheless, users should always have clear indication whether encryption is available or not. Operators could try to disable the ciphering indicator via (U)SIM option [4, Sect. 4.2.8]. However, [7, Sect. 14] explicitly states that phone could allow a configuration, which would override operator's settings. For example user could explicitly express preference to rely on operator's choice or special secure version of the phone with always-on ciphering indicator could be produced. This feature is trivial to implement because it does not require any changes to 3GPP standards. Unfortunately, the vast majority of the phones available on the market as of time of writing do not implement this feature. Even mobile phones with open OS (Operating System) like Android[9], FirefoxOS[10], Mer[11] and Ubuntu Touch[12] do not provide this obvious security improvement yet.

6 Conclusion

In this paper we have demonstrated practical feasibility of building low-cost IMSI catcher, which uses man-in-the-middle attack against hybrid GSM/UMTS networks with mutual authentication. The limitations and potential attack detection measures were studied: scenarios which makes this attack practically relevant were proposed.

Furthermore, experiments with real phones in the presence of developed IMSI catcher revealed that security aspects are largely neglected by baseband vendors

[9] Corresponding bug #5353 dates back to 2009 with no indication of any progress or intention to fix it so far.
[10] See the recent bug #960007 for tracking developments.
[11] Bug #838.
[12] Bug #1276208.

in case of hybrid GSM/UMTS networks. The demonstrated vulnerability has not been previously published to the best of author's knowledge and potentially affects millions of users worldwide.

Countermeasures to improve security with regards to IMSI catchers were discussed. Implementable improvements were reviewed for both long-term (requires standards update) and short-term (could be deployed as an over-the-air upgrade) solutions.

Acknowledgment. The author would like to thank Marta Piekarska for her help with field experiments and Kévin Redon for his help with German papers and draft review.

Appendix: Experimental setup details

In practice the attack consists of two phases: site survey and actual man-in-the-middle. The first phase is needed to gather information on the cells visible in particular area — this step is required to properly pick ARFCN on which attacking BTS should listen. The actual attack is then performed once target phone enters the area. Note that first phase does not have to be performed right before the attack — it is possible to gather this data separately.

Software

There are numerous open source projects implementing both network and mobile side of the GSM and, to some extent, 3G stack of protocols. This allows researchers unaffiliated with mobile industry to make independent inquiry into operation and security of mobile networks deployment.

Osmocom-BB [21] is an open source GSM stack implemented around Calypso chip used in old Motorola phones. It consists of several utilities including actual GSM phone implemented in software.

The command to start 2G phone is:

```
cd osmocom-bb/src/
./host/osmocon/osmocon -p /dev/ttyUSB0    -m c123xor ./
    target/firmware/board/compal_e88/layer1.compalram.bin
./host/layer23/src/mobile/mobile -i 127.0.0.1
```

Tools like RSSI implemented on top of the Osmocom-BB stack were used to assess radio environment and monitor signal quality during the experiment. The following command will chain-load RSSI into Osmocom-compatible phone (Motorola model C123 and alike):

```
./osmocom-bb/src/host/osmocon/osmocon -p /dev/ttyUSB0 -m
    c123xor -c ./osmocom-bb/src/target/firmware/board/
    compal_e88/rssi.highram.bin ./osmocom-bb/src/target/
    firmware/board/compal_e88/chainload.compalram.bin
```

Xgoldmon [14] is the utility, which obtains debug stream from Intel/Infineon XGold baseband processor. It supports Samsung Galaxy S2/SIII, Note2 and Nexus phones. The read-only debug stream contains raw 3G messages including authentication request and response data. By writing IMSI of the target phone into programmable SIM card we can use xgoldmon-compatible attacking phone to issue authentication request and thus obtain authentication challenge made for the target phone as shown in Fig. 2.

OpenBTS [22] implements GSM base station with SIP backend. This makes experimental setup self-contained: no other components like BSC are required. During the experiment patched version of OpenBTS were used with additional functionality taken from Fairwaves version.

Due to version incompatibilities OpenBTS requires the explicit version of GNURadio[13] software stack to work properly with USRPv1. It can be supplied using following commands:[14]

```
set -x PKG_CONFIG_PATH "~/gr342/lib64/pkgconfig"
./configure --with-usrp1
make
```

OpenBTS uses "open loop" power control, which means it does not actively control the transmission power of the cellphone. To successfully execute man-in-the-middle attack we should carefully assess radio environment and choose proper transmission power and a channel to operate on to make sure that radio interference from existing cells will not prevent our IMSI catcher from taking the role of preferred cell for cell selection.

To extract authentication information from xgoldmon the utility daemon was written. It parses the GSMTAP traffic and updates OpenBTS database with recent authentication data. This helps to automate the attack and further ease timing requirements. The authentication challenge contains SQN — sequence number, which is increased with every challenge so the current authentication challenge is invalidated as long as the phone receive authentication request with more recent sequence number.

Hardware

The open source implementations of GSM protocols rely on either SDR hardware where all the signal processing details are handled in the software itself or on the chips with known or reverse-engineered specifications, which allows for fine-grained control over the data sent to the network.

UmTRX [20] is open source hardware project implementing SDR transceiver capable of GSM and LTE operations. It is a successor to quite popular USRP hardware with better clocking and multi-channel capabilities available out of

[13] 64 bit build used in this case.

[14] FISH shell syntax used: http://fishshell.com/.

Table 3. OpenBTS configuration options and cell (re)selection parameters

Variable	Configuration option name	GSM Standard
C_R	GSM.SI3RO.CRO	Cell reselection offset
T_{off}	GSM.SI3RO.TEMPORARY_OFFSET	Temporary offset
T_{pen}	GSM.SI3RO.PENALTY_TIME	Penalty time
RX_{MIN}	GSM.CellSelection.RXLEV-ACCESS-MIN	Min. received signal level at MS
MS_{TX}	GSM.CellSelection.MS-TXPWR-MAX-CCH	Max. transmission power level for MS

the box. Both USRPv1 with ClockTamer clock source and UmTRX were used during the experiments.

Motorola C123 phone with Osmocom-BB firmware and Nokia with net-monitor feature enabled were used for the site survey during the attack.

References

1. 3GPP: Digital cellular telecommunications system (Phase 2+); Radio subsystem link control. Technical Specification TS 100.911 v8.23.0, 3G Partnership Project, October 2005
2. 3GPP: Digital cellular telecommunications system (Phase 2+); Functions related to Mobile Station (MS) in idle mode and group receive mode. Technical Specification TS 143.022 v11.0.0, 3G Partnership Project, October 2012
3. 3GPP: Smart Cards; UICC-Terminal interface; Physical and logical characteristics. Technical Specification TS 102.221 v11.0.0, 3G Partnership Project, June 2012
4. 3GPP: Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture. Technical Specification TS 131.102 v11.5.1, 3G Partnership Project, July 2013
5. 3GPP: Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3. Technical Specification TS 124.008 v11.8.0, 3G Partnership Project, October 2013
6. 3GPP: Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture. Technical Specification TS 33.102 v11.5.1, 3G Partnership Project, July 2013
7. 3GPP: Universal Mobile Telecommunications System (UMTS); LTE; Service aspects; Service principles. Technical Specification TS 122.101 v11.9.0, 3G Partnership Project, July 2013
8. Ball, J.: NSA monitored calls of 35 world leaders after US official handed over contacts. The Guardian, October 2013. http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls
9. Fox, Dirk: Der IMSI-Catcher. Datenschutz und Datensicherheit **26**, 212–215 (2002)
10. Golde, N., Redon, K., Borgaonkar, R.: Weaponizing femtocells: the effect of rogue devices on mobile telecommunication. In: Network & Distributed System Security Symposium 2011, February 2012

11. GSM Association: European Mobile Industry Observatory 2011 (2011)
12. Hufelschulte, J.: GroGeheimdiensten abgehört. Focus, November 2013. http://www.focus.de/politik/deutschland/_id_3428205.html
13. Kalenderi, M., Pnevmatikatos, D.N., Papaefstathiou, I., Manifavas, C.: Breaking the gsm a5/1 cryptography algorithm with rainbow tables and high-end fpgas. In: FPL, pp. 747–753 (2012)
14. Log messages convertor for phones with XGold baseband processor: XGoldmon. https://github.com/2b-as/xgoldmon
15. Mayer, T.: IMSI Catcher Detection System. Master Thesis at the Chair of Communication Systems at Freiburg University, June 2012
16. Meyer, U., Wetzel, S.: A man-in-the-middle attack on UMTS. In: Proceedings of the 3rd ACM workshop on Wireless security, WiSe 2004, pp. 90–97. ACM, New York (2004)
17. Meyer, U., Wetzel, S.: On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks. In: Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC2004), September 2004. IEEE (2004)
18. Mjølsnes, S.F., Tsay, J.K.: Computational Security Analysis of the UMTS and LTE Authentication and Key Agreement Protocols. CoRR abs/1203.3866 (2012)
19. Ntantogian, C., Xenakis, C.: Questioning the feasibility of UMTS-GSM interworking attacks. Wirel. Pers. Commun. **65**(1), 157–163 (2012)
20. Open Source Hardware Transceiver for GSM: UmTRX. http://umtrx.org/
21. Open Source MObile COMmunication: osmocom. http://osmocom.org/
22. Range Network and community: OpenBTS. http://wush.net/trac/rangepublic
23. Song, Y., Zhou, K., Chen, X.: Fake BTS Attacks of GSM system on software radio platform. J. Netw. **7**(2), 275–281 (2012)
24. Tang, C., Naumann, D.A., Wetzel, S.: Analysis of authentication and key establishment in inter-generational mobile telephony. IACR Cryptology ePrint Archive **2013**, 227 (2013)
25. Wehrle, D.: Open Source IMSI-Catcher. Master Thesis at the Chair of Communication Systems at Freiburg University, October 2009