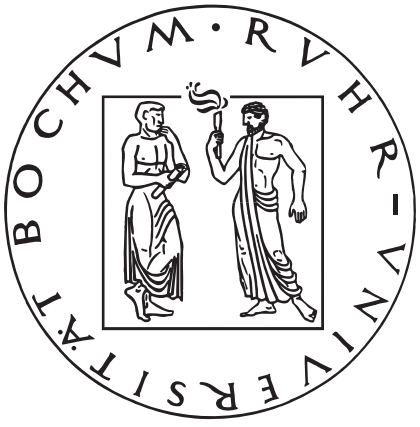
IMSI Catcher

Daehyun Strobel

13.Juli 2007

Seminararbeit
Ruhr-Universität Bochum



Chair for Communication Security
Prof. Dr.-Ing. Christof Paar

Contents

1 Introduction **1**

2 GSM (Global System for Mobile Communications) **3**
2.1 Mobile Station 4
2.2 Base Station and Base Station Controller 4
2.3 Mobile Switching Center 5
2.4 Authentication 5
2.5 GSM Encryption 6
2.6 Weaknesses 7

3 UMTS (Universal Mobile Telecommunications System) **9**
3.1 Authentication 9
3.2 Inter-operation with GSM 11

4 IMSI Catcher **13**
4.1 GSM 13
4.1.1 Modes of Operation 13
4.2 UMTS 15
4.3 Drawbacks 16
4.4 Legal Foundation 17

5 Conclusion **19**

1 Introduction

On July 29, 2005, Osman Hussain was arrested in an apartment in Rome, suspected of having placed a bomb on July 21 in a London tube station. The British Police had provided the Italian counterparts with two mobile numbers linked to him. Within 48 hours, his location was found by tracking and tapping his mobile phone ([BBC05]).

A statistic of the German Federal Network Agency shows, that this example is not an individual case (see Figure 1.1). While the landline phone monitoring stays nearly constant, there is a strong upward trend concerning the mobile phone monitoring. Alone in 2006, there have been over 35.000 orders imposed by law.

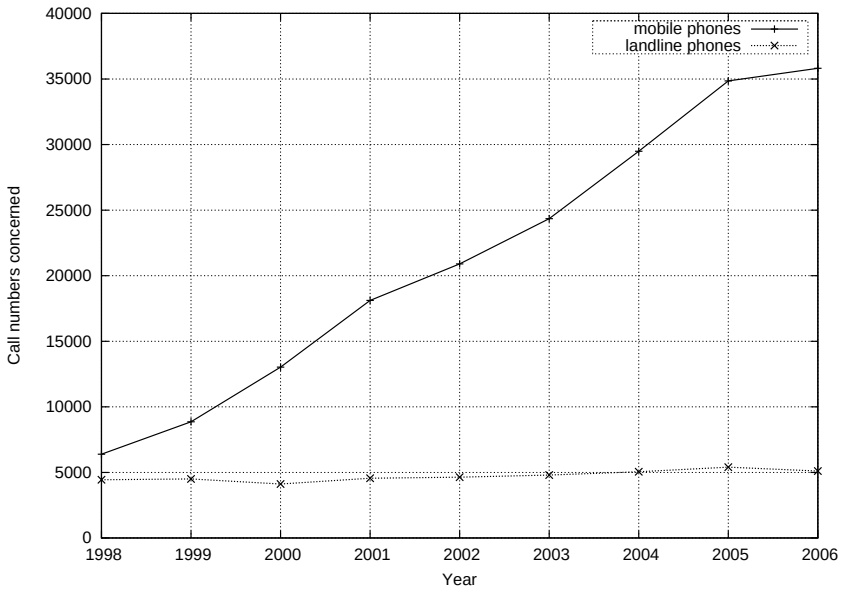


Figure 1.1: Statistics of the judicial monitoring measures of telecommunications in Germany ([BUN07])

The fact is, that tracking and tapping a mobile phone in the GSM network is not a difficult task. The operators of the telecommunication networks are obligated to permit a monitoring for the entitled authorities. Another method, and actually the more interesting one, is the assignment of an IMSI Catcher. The IMSI Catcher is an expensive device to identify, track and tap a mobile phone user in such a way, that even the network operator cannot notice anything.

In this paper, we will discuss the proceeding of this device and the necessary conditions in detail (see Chapter 4). Chapters 2 and 3 will obtain the background knowledge of the network standards GSM and UMTS, which we will need for comprehension. The conclusion is given in Chapter 5.

2 GSM (Global System for Mobile Communications)

GSM is the most common standard for mobile communication. It is used in more than 200 countries and territories all over the world. The architecture can be illustrated as a hierarchic system of mainly 4 different network components (see Figure 2.1), which are

- Mobile Stations (**MS**),
- Base Stations (**BS**),
- Base Station Controllers (**BSC**) and
- Mobile Switching Centers (**MSC**).

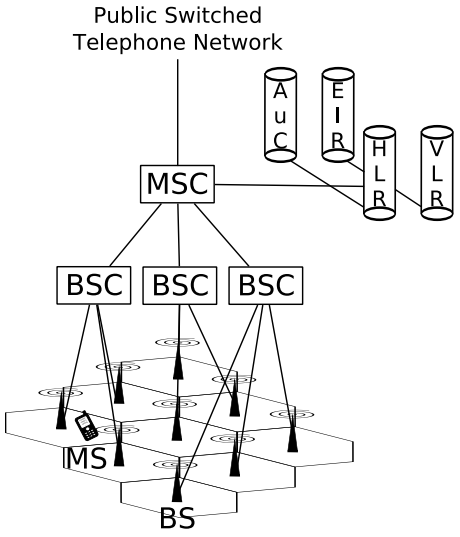


Figure 2.1: Simplified architecture of a GSM network

In the following we will discuss the functions of these components and the communication between them, to figure out the points of weaknesses in GSM.

2.1 Mobile Station

A Mobile Station can be seen as a mobile phone with a Subscriber Identification Module (**SIM**), a removable smart card. Every mobile phone has a unique 15-digit serial number, called International Mobile Equipment Identity (**IMEI**). In practice, this can be used to prevent stolen phones from accessing a network.

The identification of the subscriber is effected with the help of the SIM. It contains the International Mobile Subscriber Identity (**IMSI**), which is also a 15-digit number, concatenated of

1. the mobile country code (**MCC**): 3 digits,
2. the mobile network code (**MNC**): 2 or 3 digits and
3. the mobile subscriber identification number (**MSIN**): maximum 10 digits.

Furthermore, two algorithms are implemented on the SIM:

- The authentication algorithm A3 and
- the key generation algorithm A8.

For both algorithms, a 128 bit secret key K_i is needed that is also stored on the SIM.

2.2 Base Station and Base Station Controller

The wireless connection of a Mobile Station and a Mobile Switching Center is realized by a Base Station[1]. Therefore, the area is divided into several cellular networks with one Base Station for each cell. The size of the cell depends basically on the geographic features of the area and consequently on the range of the stations. But also the number of possible calls, that have to be handled simultaneously, has to be considered, since it is limited by the number of available channels. Hence, in densely populated areas, the cells often have a diameter of only a few hundred meters, whereas in sparsely populated areas several kilometers are usual.

In subway stations or large buildings *Relais Stations* are installed to ensure high connectivity. These Relais Stations act like a Repeater in wired networks. They simply amplify and relay incoming signals to the nearest Base Station.

However, Base Stations are not only responsible for the connectivity. They are also needed for encryption and decryption of communication data.

As the name implies, on the next higher level the Base Station Controller manages the collaboration of the Base Stations and induces power controlling if

[1] A Base Station is also referred to as Base Transceiver Station, Radio Base Station or Node B.

necessary. If a Mobile Station moves from one cell to another during a call, the Base Station Controller accomplishes a *handoff*[2]. The connection is transferred to the second Base Station to avoid a termination of the call. The assumption is, that both Base Stations are linked with the same Base Station Controller. Otherwise the handoff has to be managed by the Mobile Switching Center.

2.3 Mobile Switching Center

The Mobile Switching Center has the role of a mobility management. It is responsible for the authentication, routing, handoffs over different Base Station Controllers, connection to the landline, etc.. For this purpose, there are 4 data bases available ([SCH06]):

- Home Location Register (**HLR**): There is only one HLR in one GSM network, which stores personal informations of the subscriber, e.g. the IMSI, the phone number[3] or the GSM services.
- Visitor Location Register (**VLR**): Every MSC has its own VLR. It holds dynamic informations of the subscribers that are under the jurisdiction of the respective MSC. The informations are mostly copies of the personal informations, stored in the HLR.
- Authentication Center (**AuC**): The AuC holds the access data of every subscriber, particularly the secret key K_i of the SIM.
- Equipment Identity Register (**EIR**): As already mentioned, it is possible to prevent mobile phones from accessing the network. To realize this, the IMEI numbers of banned or stolen phones are kept in the EIR.

2.4 Authentication

If a Mobile Station wants to access a network, a challenge-response protocol is used to authenticate the subscriber (see Figure 2.2). After sending the security capabilities (see also Section 2.5), the Mobile Station is induced to transmit its IMSI to the VLR. The VLR forwards the IMSI to the HLR and receives a 128 bit random number $RAND$, a 32 bit signed response $SRES$ and a session key K_c. Only $RAND$ is passed to the mobile station. Together with the secret key K_i, these are the two inputs of the authentication algorithm A3. As output, the signed response $SRES'$ is generated, which is returned to the VLR. If $SRES$ and $SRES'$ match, the authentication request will be accepted, otherwise it will be discarded.

[2] In Britain, the term *handover* is more common.
[3] Also called Mobile Subscriber ISDN number (MSISDN).

As a security measure, the VLR assigns a Temporary Mobile Subscriber Identity (**TMSI**) to the Mobile Station to reduce the frequent transmission of the IMSI. This helps to avoid being identified or tracked. In further sessions, this TMSI can be used as identity response.

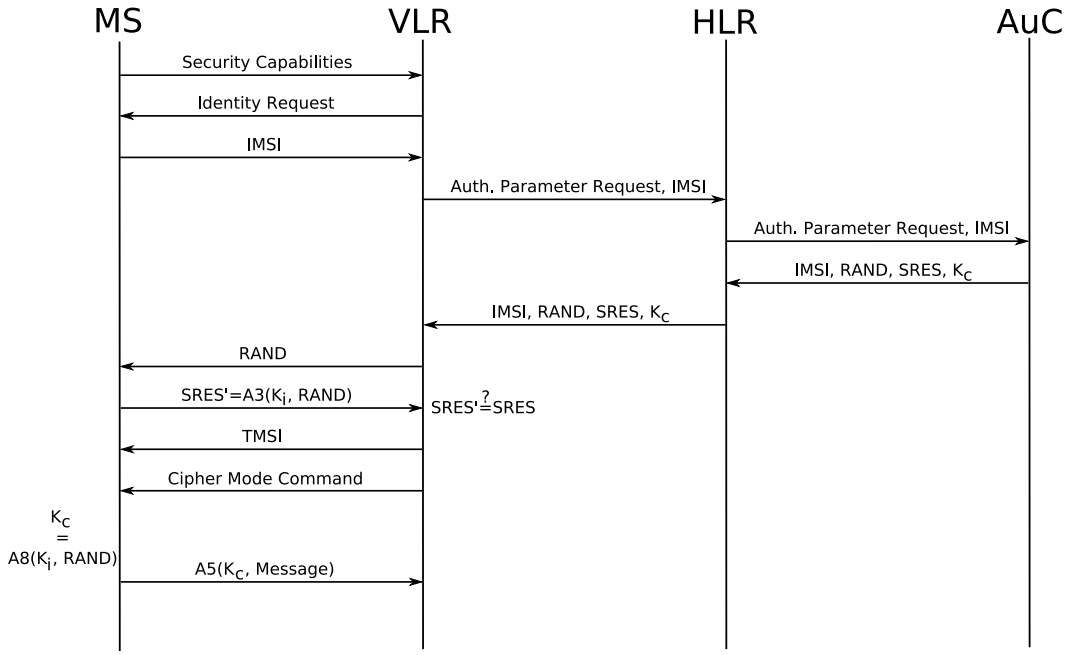


Figure 2.2: Authentication and encryption in GSM

2.5 GSM Encryption

To provide communication privacy, the stream cipher A5 is implemented on every mobile phone. It is a combination of three (A5/1) or four (A5/2) linear feedback shift registers (LFSRs) which encrypts and decrypts the communication data, if needed. The session key K_c, used in this algorithm, is generated by the algorithm A8 on the SIM with the input $RAND$. In this case, $RAND$ is the same random number as it is used in the authentication process. As an alternative, A5/0 encloses no encryption at all.[4]

In the security capabilities, the Mobile Station specifies, which encryption algorithms are supported. The Base Station chooses one of these and informs the Mobile Station with the cipher mode command.

[4] A5/1 is mostly used in Europe. An exception is France, where the encryption is disabled. This is why A5/0 is also called 'French mode' ([SPY05]).

2.6 Weaknesses

GSM has a few weaknesses, but regarding to the use of an IMSI Catcher, we will focus in Chapter 4 on point 1.

1. The authentication process considers only a one-sided authentication. The Mobile Station has to prove, that it is permitted to access the network, but there is no verification of the Base Station.

2. *Security by obscurity*: Since the beginning of GSM, the algorithms A3, A8 and A5 have not been published and always kept secret. But with the help of reverse engineering a number of serious weaknesses have been identified. In April 1998, Ian Goldberg and David Wagner released an article about cloning a GSM SIM ([ISA98]) and in April 2000, Alex Biryukov, Adi Shamir and David Wagner presented a paper about real time cryptanalysis of A5/1 on a PC ([BSW01]). The successor A5/2 is even more insecure and is not used as standard any more.

3. The encryption is only applied for the wireless transmission. That means, every communication is sent in plain text from the Base Station to the gateways.

4. For technical reasons, it is necessary for a Mobile Station to transmit the current location in short periods to the Base Station. This can be abused to track and record the movement profile of a subscriber.

3 UMTS (Universal Mobile Telecommunications System)

UMTS is a mobile phone standard of the third generation (3G) and is a successor of GSM. It is characterized by a significant faster data transfer rate and a richer range of services compared to GSM. Built on the security of GSM, the following features have been added:

- Mutual entity authentication between Mobile Station and the Home Environment, the equivalent to MSC/HLR,
- a sequence number generator to guarantee freshness in the authentication process,
- integrity, using a MAC for the authentication process,
- A5/3, also known as *Kasumi*, a block cipher with a key size of 128 bits (for further details, see also [3GP01]).

3.1 Authentication

The authentication in UMTS is more complicated than in GSM. A secret key K is shared by the Universal Subscriber Identity Module (**USIM**) and the Home Environment (**HE**). Instead of A3 and A8,

- the authentication functions $f1$, $f2$ and
- the key generating functions $f3$, $f4$, $f5$

are used as follows (see also Figure 3.1):
The Home Environment

1. generates a sequence number SQN and a 128 bit random number $RAND$,
2. computes
   a) $MAC = f1(K, (SQN||RAND||AMF))$, with the authentication management field AMF,
   b) the expected user response $XRES = f2(K, RAND)$,

c) cipher key $CK = f3(K, RAND)$,
d) integrity key $IK = f4(K, RAND)$,
e) anonymity key $AK = f5(K, RAND)$,
f) authentication token $AUTN = SQN \oplus AK||AMF||MAC$,
g) $AV = RAND||XRES||CK||IK||AUTN$ and

3. sends the authentication vector AV to the Service Network (**SN**), the equivalent to MSC/VLR.

If the Mobile Station sends its request, the Service Network responses with $RAND$ and $AUTN$.

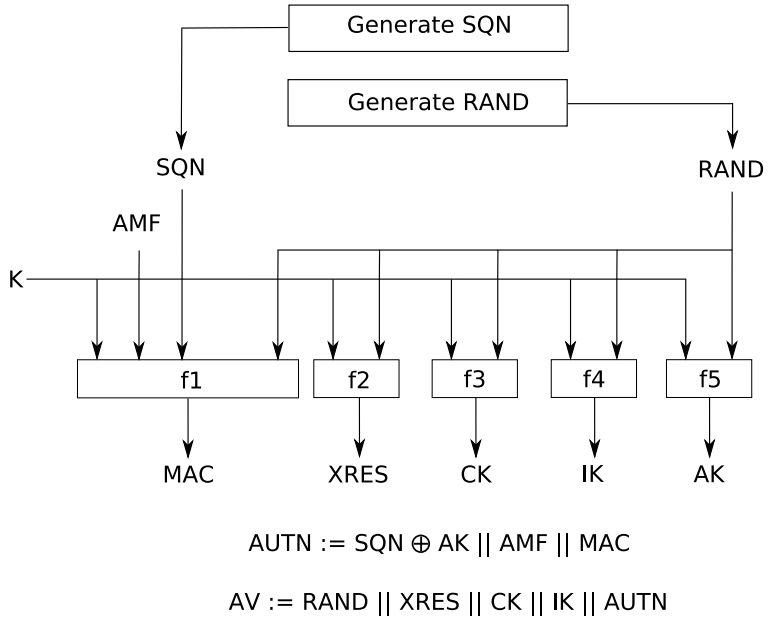


Figure 3.1: Generation of an authentication vector ([3GP99])

On the other side, the user proceeds as shown in Figure 3.2.
The USIM

1. computes

a) $AK = f5(K, RAND)$,
b) $SQN = (SQN \oplus AK) \oplus AK)$,
c) $MAC' = f1(K, (SQN||RAND||AMF))$

2. checks if

a) $MAC' = MAC$,
b) SQN is valid,

3. computes
   a) $RES = f2(K, RAND)$,
   b) $CK = f3(K, RAND)$,
   c) $IK = f4(K, RAND)$ and
4. sends RES to the Service Network.

The Service Network checks if $RES = XRES$. If one of these comparison fails, a new authentication vector is generated.

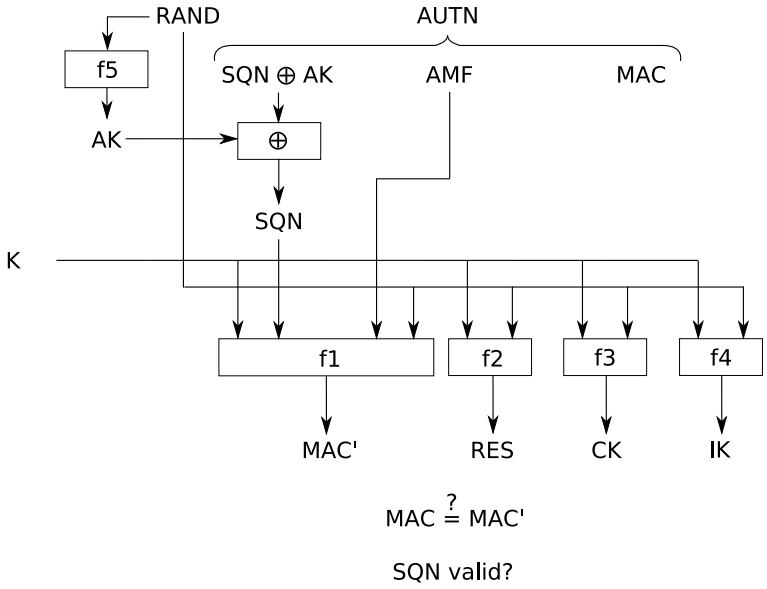


Figure 3.2: User authentication function in the USIM ([3GP99])

3.2 Inter-operation with GSM

To provide a high network coverage, the UMTS standard allows for inter-operation with GSM ([MEY04]). Therefore, not only UMTS, but also GSM Base Stations are connected to the Service Network. These GSM Base Stations neither support integrity protection nor the UMTS encryption algorithms. However, to guarantee mutual authentication, the authentication data generated by the Home Environment and Mobile Station are simply passed through. Only the cipher mode is chosen by the Base Station. The session key K_c that is needed for the GSM encryption, is computed from the integrity key IK and the cipher key CK as follows ([WET04]):

1. Split the 128 bit keys IK and CK into 64 bit keys, such that $IK = IK_1||IK_2$ and $CK = CK_1||CK_2$

2. Compute $K_c = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2$

Figure 3.3 shows the UMTS authentication protocol with a GSM Base Station. That this inter-operation does not only brings advantages, can be seen in Section 4.2.

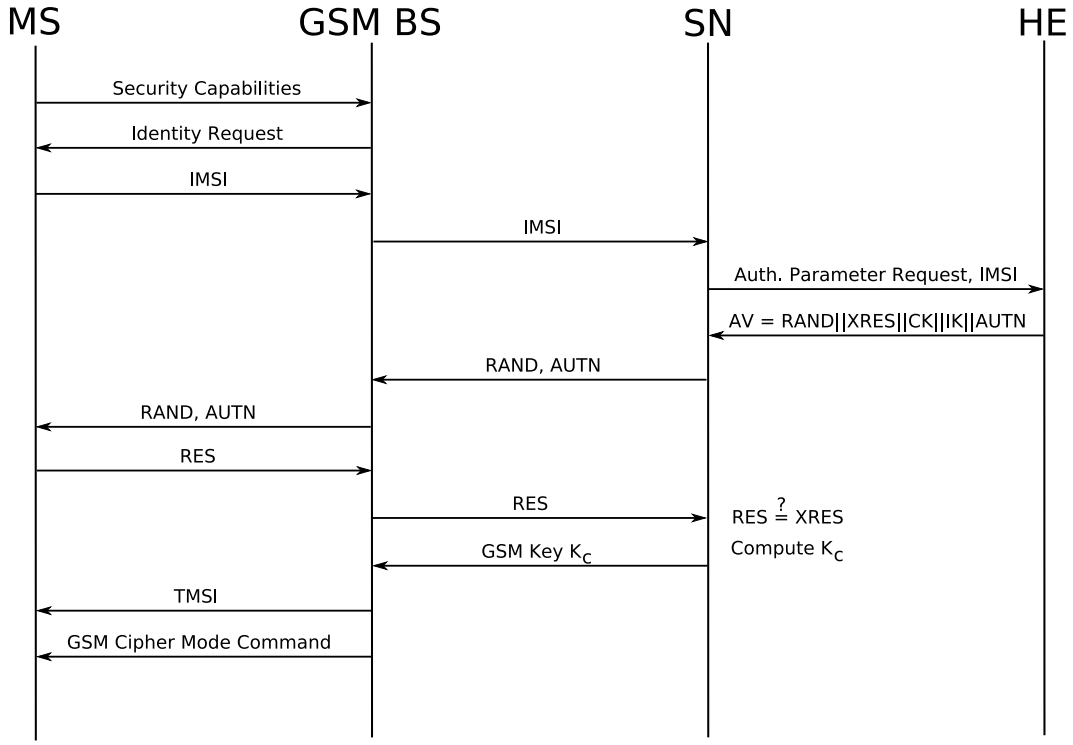


Figure 3.3: Authentication in UMTS with GSM Base Station

4 IMSI Catcher

In 1996, the German company *Rohde & Schwarz* presented the first IMSI Catcher GA 090 in Munich. The idea of an IMSI Catcher was originally to identify a subscriber by forcing to transmit the IMSI. With the help of the network operator, it is possible to determine the associated phone number. In 1997, the successor GA 900 allows the owner not only to identify, but also to tap outgoing phone calls.

4.1 GSM

4.1.1 Modes of Operation

In GSM, both devices take advantage of the one-sided authentication. As already mentioned, it is not necessary to authenticate a Base Station to a Mobile Station. An IMSI Catcher exploits this weakness and masquerades to a Mobile Station as a Base Station. With a signal strength up to 25 watt, it can theoretically supply a radius of several kilometers[1]. Additionally, the GA 900 in combination with an own SIM, has the functionality to act like a Mobile Station and to perform a man-in-the-middle attack. Figure 4.1 shows the modified GSM protocol.

Identifying an IMSI

Every mobile phone has the requirement to optimize the reception. If there are more than one Base Station of the subscribed network operator accessible, it will always choose the one, with the strongest signal. An IMSI Catcher masquerades as a Base Station and causes every mobile phone of the simulated network operator within a defined radius to log in. With the help of a special identity request, it is able to force the transmission of the IMSI, instead of a TMSI. A similar procedure can be used to identify the IMEI.

Tapping a Mobile Phone

Figure 4.1 shows the functionality as communications intercept station of the GA 900. In this case, the IMSI Catcher, which acts as a Base Station, behaves

[1] Compared to 50 watt of a Base Station.

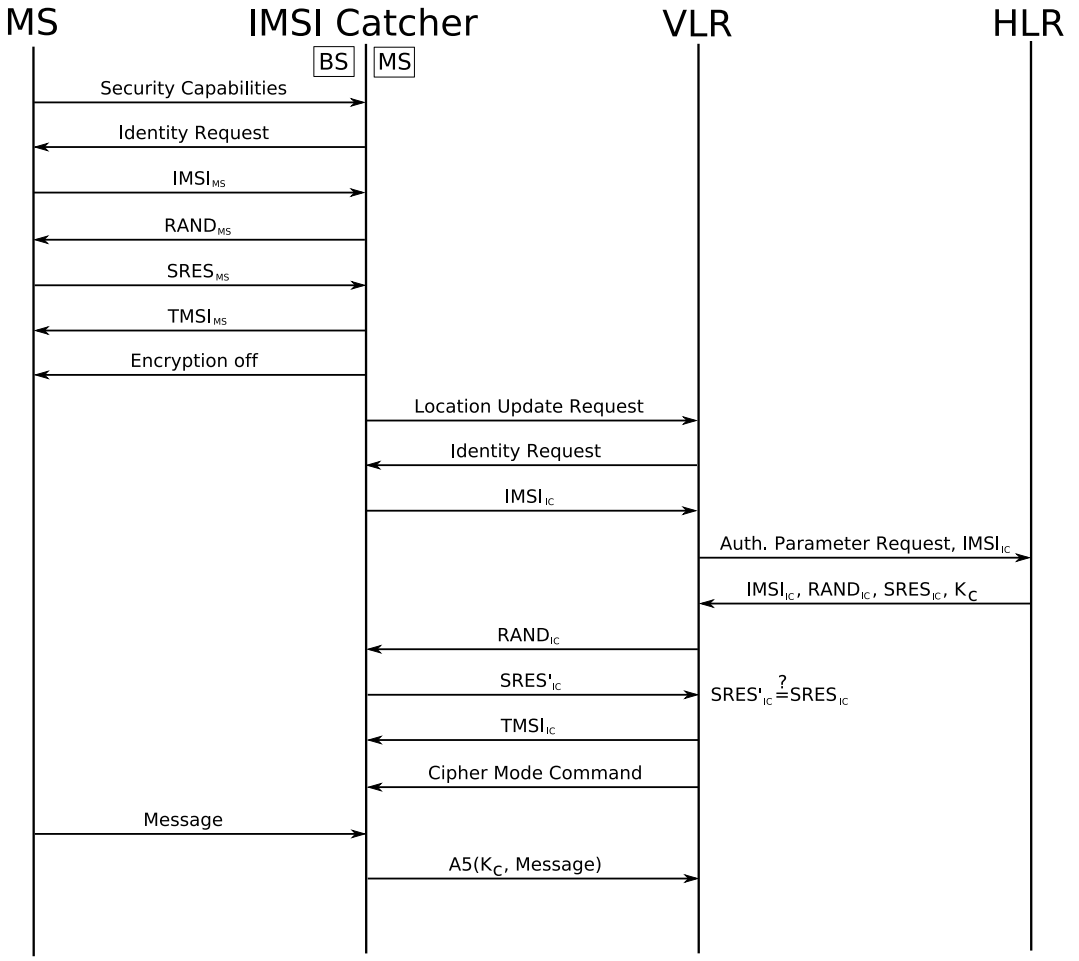


Figure 4.1: Man-in-the-middle attack with an IMSI Catcher

simultaneously like a Mobile Station to the real Base Station. After the authentication process, it uses the fact, that the encryption can simply be disabled from the Base Station. Hence, it can encrypt the plain text traffic from the Mobile Station and pass it to the Base Station.

Since the IMSI Catcher establishes a regular connection with a SIM, it is not possible to tap more than one phone call at the same time. It should be also clear, why incoming phone calls cannot be patched through. The subscriber has no direct connection to the network operator. Hence, he is not approachable for incoming calls.

A man-in-the-middle attack without a SIM may also be possible ([FOX02]). Then, in the authentication process, the IMSI Catcher simply passes the authentication data from the Mobile Station to the Base Station and the other way around. But in this scenario, the the encryption to both sides has to be disabled, since the attacker is not in the possession of the session key K_c. On the one side,

it can be realized by sending the cipher mode command A5/0 to the Mobile Station, but the problem is to induce the no-encryption mode to the Base Station. Sending only A5/0 in the security capabilities will probably not succeed, due to the security standard of GSM. Hence, to establish a regular connection with a SIM may be less complicated.

Position Fixing

As one can imagine, an IMSI Catcher is not able to localize a Mobile Station. There is only the functionality to verify the presence in a defined area. Localization or tracking can be realized by the network operator. Due to the permanent location update process with the Base Station, the Mobile Station reveals the GSM cell, it is currently located at. This may be, depending on the size of the cell, a radius of a few hundred meters to several kilometers. In addition, signal strength or signal propagation delay can be used to rise the accuracy. Hence, in combination with an IMSI Catcher, the localization can be improved enormously.

4.2 UMTS

Since UMTS uses mutual entity authentication, the man-in-the-middle attack as seen on GSM is not successful. The IMSI Catcher is not in the possession of the secret key K and hence, cannot generate the authentication vector AV. For the same reason, the identification of the IMSI cannot be realized in this way.

However, in 2005, Ulrike Meyer and Susanne Wetzel described an attack that exploits the inter-operation with GSM ([MEY04]). It is also a man-in-the-middle attack, but executed in three phases:

1. The IMSI or a valid TMSI of the victim has to be found out. This is easy, since it is sent in the beginning of an authentication process.

2. The impersonation as the victim to the Server Network. The attacker sends the IMSI to the Server Network and waits, until the random number $RAND$ and the authentication token $AUTN$ is returned, before he disconnects (see Figure 4.2). The combination $RAND$ and $AUTN$ is saved for the later use.

3. The IMSI Catcher masquerades as a GSM Base Station and the $RAND$ and $AUTN$ is sent to the victim. When there is not too much time elapsed since the second phase, the token is fresh and is accepted by the Mobile Station. The attacker cannot verify the response RES, which is not important, and gives the GSM cipher mode command A5/0 to the Mobile Station (Figure 4.3).

To forward the communication data, a regular connection is needed, since it is not possible to impersonate the victim to the Server Network at the same time. Hence, the attacker has to possess an own USIM to connect to the network.

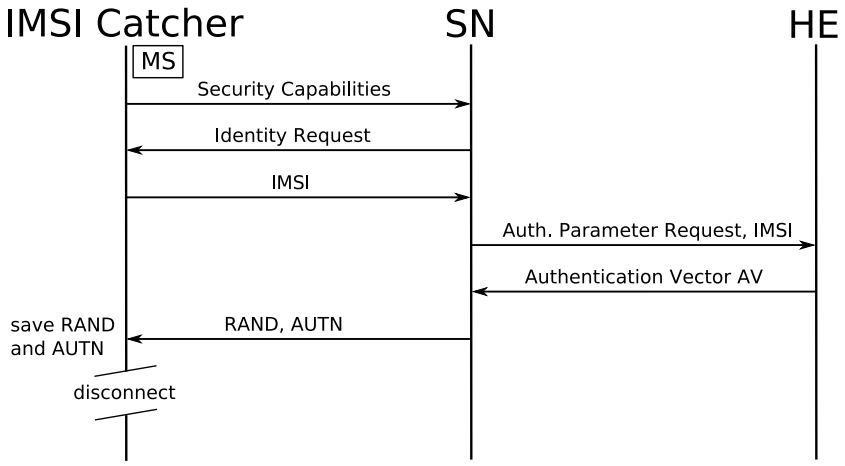


Figure 4.2: Attacker obtains currently valid authentication token ([MEY04])

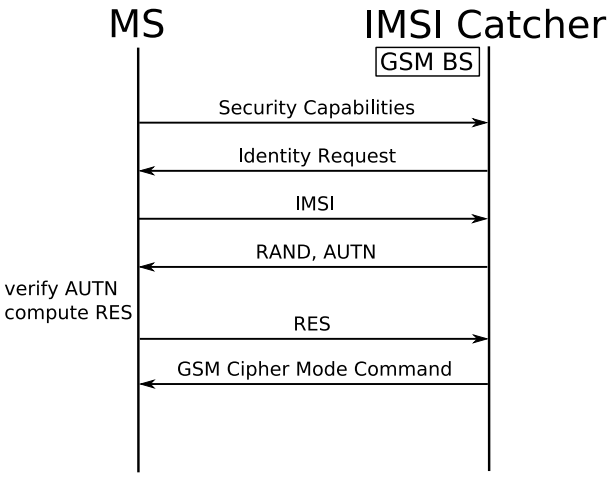


Figure 4.3: Authentication of the attacker as a GSM Base Station ([MEY04])

4.3 Drawbacks

The assignment of an IMSI Catcher has a number of drawbacks:

- It must be ensured, that the mobile phone of the observed person is in standby mode and the correct network operator is found out. Otherwise, for the Mobile Station, there is no need to log into the simulated Base Station.
- Depending on the signal strength of the IMSI Catcher, numerous IMSIs can be located. The Problem is to find out the right one.
- All mobile phones in the catchment area have no access to the network. Incoming and outgoing calls cannot be patched through for these subscribers.

Only the observed person has an indirect connection.

- There are some disclosing factors. In most cases, the operation cannot be recognized immediately by the subscriber. But there are a few mobile phones that show a small symbol on the display, e.g. an exclamation point, if encryption is not used. Another point is the calling number. Since the network access is handled with the SIM/USIM of the IMSI Catcher, the receiver cannot see the number of the calling party. Of course, this also implicates that the tapped calls are not listed in the itemized bill.
- The assignment near the Base Station can be difficult, due to the high signal level of the original Base Station.

4.4 Legal Foundation

Since September 11, 2001, also in Germany largest efforts to prevent terroristic attacks have been launched. One consequence is the increased non-indisputable assignment of the IMSI Catcher. In August 14, 2002, §100i was introduced, which allows the police in an urgent suspicion to identify the IMSI and the IMEI with technical devices. What has been illegally accomplished before ([HEI01]), is now legal, on the optimistic assumption of the Federal Ministry of the Interior that a restriction of the mobile phones in the catchment area takes only 10 seconds ([BUN02]).

5 Conclusion

The one-sided authentication of GSM is a serious weak point, which is emploited by the IMSI Catcher. After identifying the IMSI and IMEI with a masquerade attack, outgoing calls can be tapped with a man-in-the-middle attack.

In many articles, the authors assume, due to the launch of UMTS, that the IMSI Catcher will not play a large role in the future. But GSM had a strong development in the whole world in the last years and at the beginning of 2006 over 1.7 billion subscribers. The change-over to UMTS will last for a long time, above all, because one needs a special UMTS supporting mobile phone. In addition, the UMTS coverage is moderate. Hence, the inter-operation with GSM will probably remain, so that a man-in-the-middle attack will be still possible.

List of Figures

1.1 Statistics of the judicial monitoring measures of telecommunications in Germany ([BUN07]) 1

2.1 Simplified architecture of a GSM network 3
2.2 Authentication and encryption in GSM 6

3.1 Generation of an authentication vector ([3GP99]) 10
3.2 User authentication function in the USIM ([3GP99]) 11
3.3 Authentication in UMTS with GSM Base Station 12

4.1 Man-in-the-middle attack with an IMSI Catcher 14
4.2 Attacker obtains currently valid authentication token ([MEY04]) . 16
4.3 Authentication of the attacker as a GSM Base Station ([MEY04]) 16

Bibliography

[3GP99] 3GPP: *Authentication management field ver2*, URL: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_06_9910/docs/s3-99348,%20CR33102-017%20authentication%20managment%20field%20ver2.rtf, 1999.

[3GP01] 3GPP: *3GPP TS 35.202 V3.1.1*, URL: http://www.3gpp.org/TB/other/algorithms/35202-311.pdf, 2001.

[BBC05] BBC UK: *Tracking a suspect by mobile phone*, URL: http://news.bbc.co.uk/2/low/technology/4738219.stm, 2005.

[BSW01] Alex Biryukov, Adi Shamir and David Wagner: *Real Time Cryptanalysis of (A5/1) on a (PC)*, Lecture Notes in Computer Science, Vol. 1978, URL: http://www.isaac.cs.berkeley.edu/isaac/gsm-press.html, 2001.

[BUN07] Bundesnetzagentur: *Statistik der strafprozessualen Überwachungsmaßnahmen der Telekommunikation*, URL: http://www.bundesnetzagentur.de/media/archive/9710.pdf, 2007.

[BUN02] Bundesregierung: *Rechtliche Zulssigkeit von so genannten IMSI-Catchern*, Bundestag printed paper 14/6885, URL: http://dip.bundestag.de/btd/14/068/1406885.pdf, 09/10/2001.

[FOX02] Dirk Fox: *Der IMSI-Catcher*, Datenschutz und Datensicherheit 26, 2002.

[HEI01] Heise: *Polizei mit IMSI-Catcher auf Lauschangriff*, URL: http://www.heise.de/newsticker/meldung/20094, 08/11/2001.

[ISA98] ISAAC: *Smartcard Developer Association Clones Digital GSM Cellphones*, URL: http://www.isaac.cs.berkeley.edu/isaac/gsm-press.html, 1998.

[MEY04] Ulrike Meyer and Susanne Wetzel: *A Man-in-the-Middle Attack on UMTS*, URL: http://www.cs.stevens.edu/ swetzel/publications/mim.pdf, 2005.

[SCH06] Jörg Schwenk: *Mobilfunk: Systembersicht*, Systemsicherheit, Teil 3: Mobilfunk, URL: http://www.nds.rub.de/lehre/vorlesungen/systemsicherheit/Systemsicherheit_3_Mobilfunk_v05.pdf, 2006.

[SPY05] Spyworld: *Interception of GSM Cellphones*, URL: http://www.spyworld-actu.com/IMG/_article_PDF/article_288.pdf, 2005.

[WET04] Ulrike Meyer and Susanne Wetzel: *On the impact of GSM Encryption and Man-in-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks*, Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC2004), IEEE, 2004.