3GPP TSG SA WG3 Security — SA3#37 **S3-050101**
February 22-25, 2005
Sophia Antipolis, France

Source: **Vodafone, Siemens**

Title: **Review of recently published papers on GSM and UMTS security**

Agenda item: **6.5**

Document for: **Discussion and decision**

---

1 Introduction

This contribution reviews the follow papers by Ulrike Meyer (Darmstadt University of Technology, Germany) and Susanne Wetzel (Stevens Institute of Technology, New Jersey, USA):

- Meyer, U, Wetzel, S.: 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), September 2004, IEEE, 2004. [1]

- Meyer, U., Wetzel, S.: A Man-in-the-Middle Attack on UMTS. Proceedings of ACM Workshop on Wireless Security (WiSe 2004), October 2004, ACM, 2004. [2]

The main purpose of this contribution is to assess the impact of the papers on the 3GPP specifications and identify any changes that are needed. Our comments and analysis of the Meyer and Wetzel papers is provided in sections 2 and 3. A summary of our conclusions and proposals are provided in section 4.

This document has been sent to the authors of the papers for feedback. Unfortunately it was not possible to receive feedback from the authors before the SA3 document deadline.

The PIMRC 2004 paper is available to download from Ulrike Meyer's web site. The WiSE 2004 paper is not published freely on the Internet, although it is available to purchase from the ACM web site.

2 PIMRC 2004 paper

2.1 Comments on paper

<u>Section IV GSM Attacks</u>

<u>Section IV.B Man-in-the-Middle Attack</u>

In this section the authors describe man-in-the-middle attacks in GSM whereby an attacker impersonates a false base station towards a victim mobile and can then impersonate that victim towards the real network. The authors correctly describe that the attacker could relay the authentication messages between the real network and the victim. The authors also describe how a man-in-the-middle could modify the encryption capabilities sent by the victim to force the network to disable encryption. However, the authors fail to recognise that A5/1 support in mobiles is mandatory and that GSM networks that use A5/1 should enforce its use and not accept calls from mobiles that cannot support A5/1 encryption. This means that the attacker cannot disable A5/1 encryption by modifying the mobile's encryption capabilities. Therefore, the channel hijack attack described by Meyer and Wetzel is not possible if the network enforces the use of A5/1.

Although the channel hijack attack described in this section would fail in GSM A5/1 networks which enforce encryption, the following variant of the attack, not mentioned in Meyer/Wetzel's paper, should also be considered. The variant applies when multiple encryption algorithms are allowed by the network, as would be the case during the introduction of A5/3. The attack would be to modify the encryption capabilities of the victim to force the victim and the real network to use a weaker encryption algorithm when both sides support a stronger one. This could lead to the possibility of channel hijacking attacks in case an efficient attack on A5/1 was found, and mobiles not supporting A5/3 would still have to be allowed in GSM networks for some time. A possible enhancement to GSM security would be to provide protection against this type of "bidding down" attack.

Section V Impact of GSM Attacks on Interoperating GSM/UMTS networks

Section V.A Impact of Encryption Attacks

In this section the authors discuss how an attack that recovers the GSM encryption key influences security in networks where both GSM and UMTS are available. Several cases are described:

Case 1: GSM subscriber authenticated in GSM and handed over to UMTS:
The authors correctly explain that discovery of the GSM encryption key leads to discover of the keys used to protect UMTS communications. However, it is clear that GSM subscribers which, at some point during a call, roamed into GSM, get only GSM grade security even if they roam into UMTS during the same call. This is no surprise and cannot be countered by the UMTS security architecture.

Case 2: GSM subscriber authenticated in UMTS and handed over to GSM:
Same comments as for case 1.

Case 3: UMTS subscriber authenticated in UMTS and handed over to GSM BSS that is connected to 3G MSC:
The authors explain that discovery of the GSM encryption key leads to discover of information about the UMTS keys from which it was derived using the 3GPP standard derivation function, c3[1]. However, this information does not reduce the entropy of the base authentication key Ki, nor does it reduce the entropy of the individual cipher and integrity keys, CK and IK. Furthermore, it does not reduce the complexity of an exhaustive search on a 128 bit Ki to less that 2^128, nor does it reduce the complexity of an exhaustive search on the 128 bit CK or IK to less that 2^128. So, in practice there is no threat to UMTS communications. In GSM, UMTS subscribers suffer the same attacks as GSM subscribers, which is no surprise.

Case 4: UMTS subscriber authenticated in UMTS and handed over to GSM BSS that is connected to a 2G MSC:
Same comments as for case 3.

Case 5: UMTS subscriber authenticated via a GSM BSS connected to a 2G MSC and then handed over to UMTS:
The authors correctly explain that discovery of the GSM encryption key due to a GSM weakness leads to discovery of the UMTS keys. Here, the UMTS subscriber is affected by GSM attacks even while communicating in a UMTS network. This is the most serious of the cases in section V.A. The authors argue that re-authentication after handover would remedy the problem. This case is discussed in more detail in section 2.2.

Case 6: UMTS subscriber authenticated via a GSM BSS connected to a 3G MSC and then handed over to UMTS:
Same comment as for case 3.

In the summary in the last paragraph of section V.A there is a mistake. In particular, the last sentence states that “a single handover to a GSM base station, that is connected to a 2G MSC breaks the encryption and integrity protection of all pre-handover and post-handover UMTS communication”. This is incorrect since only post-handover UMTS communications are compromised (case 5). In the case of pre-handover UMTS communications (case 4), there is no threat to UMTS communications.

Section V.B Impact of the Man-in-the-Middle attack

The attack scenarios described in this section are unclear. However, we make the following observations based on our interpretation:

- In this section the authors seem to suggest that the man-in-the-middle impersonation attack described in section IV.B, and described above, is applicable in GSM regardless of whether GSM authentication or UMTS authentication is run. However, as mentioned earlier, the attack in section IV.B is not valid because GSM networks should reject mobiles that cannot support encryption.
- If we discount impersonation attacks against a GSM network, then the attack scenarios in this section could still be applied to eavesdrop mobile-originated calls. While this attack is a well-known vulnerability of GSM, the authors seem to claim that the attack can be carried into UMTS. In particular, they suggest that the man-in-the-middle could hand the victim into UMTS. The description of how to do this is unclear in the paper. We do not believe that the attack would be successful because the attacker would be unable to generate the correct integrity protection codes for the signalling messages that need to be sent to the mobile during, and after, the handover to UMTS.
- It should be considered whether the subscriber masquerade attack described in section IV.B could be successfully applied in a network that has GSM and UMTS encryption switched off. Certainly, it would be possible for the attacker to masquerade in the GSM part of the network by relaying the authentication messages to the target

---

[1] c3: $Kc_{[GSM]} = CK_1$ xor CK_2 xor IK_1 xor IK_2, where CK_i and IK_i are both 64 bits long and $CK = CK_1 \| CK_2$ and $IK = IK_1 \| IK_2$

mobile camped on his false base station, while he masquerades as the target mobile using a separate connection towards the real network. However, it should be considered whether the techniques described in section IV.B could be used to allow the masquerade work against the UMTS part of the network. Two attack scenarios are conceivable:

- The first attack scenario would be to attempt to initiate the fraudulent connection in the UMTS part of the network. This would require the attacker to circumvent the mandatory UTRAN integrity protection mechanism. Meyer and Wetzel seem to suggest that this could be done by relaying integrity-protected commands from the network to the target mobile in order to obtain the correct integrity protected response. Further study is needed to determine whether this would be feasible in practice. Even if it were feasible, then no solution is presented for how the attacker would be able to spoof signalling messages that originate from the mobile station itself. In particular, it seems impossible for the attacker to be able to spoof the initial layer 3 signalling messages that would be needed by the attacker to set-up the fraudulent connection.
- The second attack scenario would be to start the connection in GSM and then initiate a handover into UMTS. Again, Meyer and Wetzel seem to suggest that this could be done by relaying the Handover Command to the target mobile in order to obtain the correct integrity-protected Handover Complete message to send to the network. Further study is needed to determine whether this would be feasible in practice. Even if it were feasible, then the attacker would have to repeat this attack for subsequent signalling messages which would increase the complexity of the attack. A further complication is that no solution is presented for how the attacker would be able to spoof signalling messages that originate from the mobile station itself. For these reasons, it would seem very unlikely that this attack would be feasible to mount in practice.

Section VI Countermeasures

The authors' solution to case 5 (and to other cases) in section V.A is to require authentication to be performed at intersystem handover. However, we believe that this may be difficult and we identify other more effective means – see section 2.2.

2.2 Discussion

Several attacks are presented in the paper. However, we consider the attack described in case 5 of section V.A to be the only attack that needs further consideration. Countermeasures to this attack are described in the following sub-sections.

Our comments on section IV.B did lead us to mention that GSM enhancements to protect against "bidding down" should be considered. However, this has already been discussed as a possible enhancement within 3GPP (e.g. one possible solution is described in section 5.1 of Vodafone contribution S3-040262 "Analysis of the authenticated GSM cipher command mechanism" [3]). It is expected that enhancement to protect against "bidding down" will be considered within the scope of the recently approved work item on Access Security Enhancements, SP-040865 (= S3-041077) [4].

2.2.1 Difficulties with Meyer/Wetzel countermeasures

While it is true that the 3GPP standards allow for re-authentication and key change in mid-call, it seems that this feature is currently not implemented everywhere, and it seems unclear whether it has been tested.

Cf. S3-040207 (= N1-040501, LS from CN1 to SA3 [5]), which discusses a "key set change after re-authentication of an ongoing, already ciphering and/or integrity protected RR/RRC connection or PS signaling connection." Cf. also S3-040708 (= N1-041519, LS from CN1 to SA3 [6]): "Currently, CN1 is not aware of any scenario where re-authentication on the already ciphering- and/or integrity-protected CS connection would be required for security reasons. Accordingly, there seems to be no MSC implementation that would perform such a re-authentication."

Furthermore, when a UE is handed over from a 2G-MSC, incapable of UMTS AKA, to UTRAN then the 2G-MSC remains the anchor MSC, and will continue to perform the authentications, i.e. it will perform GSM authentications. But a UE attached to a UTRAN shall not accept GSM authentications; hence a re-authentication while the UE is in UTRAN would fail.

2.2.2 Alternatives

For a 2G-MSC/VLR (R98-), no handover to UTRAN is supported, so the attack in case 5 of section V.A does not occur for these MSCs. It is true that the 3GPP specifications allow for 2G-MSC/VLR (R99) to support handover to UTRAN, but not UMTS AKA. But it seems that at least some, if not all 2G-MSC/VLR (R99) in the field do support UMTS AKA. From Rel5 onwards, the support of UMTS AKA is mandatory in GSM only handsets – this may encourage support of UMTS AKA in 2G-MSC/VLR that support handover to UTRAN. If the 2G-MSC/VLR (R99) supports UMTS AKA then the attack in V.A Case 5 does not occur, rather we have V.A Case 6, which has no serious consequences.

2.2.3 Idle mode situation

The considerations in Meyer/Wetzel's paper concern handover situations only, but one should also look at MSC changes in idle mode, where the old security context is transferred according to the 3GPP specifications. In order to prevent a GSM security context to be used after a change to a 3G-MSC, it should be ensured through configuration of the 3G-MSC that re-authentication takes place at location area update when moving from 2G to 3G. In idle mode, re-authentication should not pose any technical difficulties.

2.2.4 PS domain

Although not mentioned in Meyer/Wetzel's paper, similar security issues exist for the PS domain, where the old security context is transferred between SGSNs at routing area update. In order to prevent a GSM security context to be used after a change to a 3G-SGSN, it should be ensured through configuration of the 3G-SGSN that re-authentication takes place at routing area update when moving from 2G to 3G. PS handover is currently being developed in 3GPP - see TS 43.129 [8].

If inter-system RAT handover (GERAN A/Gb → UTRAN) is supported, then networks should additionally be configured to ensure that all 2G-SGSN, which support handover to UTRAN, also support and use UMTS AKA. An alternative solution for PS handover, which avoids 2G SGSNs having to support UMTS AKA, takes into account the fact that a routing area update towards the new SGSN happens as part of the PS handover procedure. The new 3G SGSN can run a mid-session UMTS AKA in order to update the keys. Mid-session PS authentication may not have the same difficulties as mid-call CS authentication. A disadvantage of this approach is that a small amount of data communicated over UMTS may be protected using the derived key rather than the full UMTS key. It is therefore preferred, from a security point of view, to require the 2G SGSN to support and use UMTS AKA.

2.2.5 Conclusion

Rather than trying to examine whether all involved components support re-authentication and key set change for an ongoing call, one possibility is to ensure that all 2G-MSC/VLRs, which support handover to UTRAN, also support and use UMTS AKA, as this seems to be the far smaller effort. Then the attack in V.A Case 5 never occurs. In addition, it should be ensured that there is a UMTS re-authentication after a change to a 3G MSC in idle mode, or to a 3G SGSN, when a GSM security context was transferred. If these conclusions were agreed by SA3 they could be forwarded to GSMA who could turn them into recommendations for the operators. We do not see that changes to the 3GPP specifications would be needed.

3 WiSE 2004 paper

3.1 Comments on paper

<u>Section 2, paragraph 2</u>

It is claimed that a mechanism to prevent false base station attacks for UMTS subscribers roaming onto GSM was considered by 3GPP but not adopted. This claim refers to a proposal from Vodafone presented in S3-990206 presented at 3GPP SA3#5 in July 1999 [7]. The Vodafone proposal was to terminate UMTS integrity protection in the MSC rather than in the RNC and extend integrity protection to GSM access. It should be pointed out that the proposal in [7] has the limitation that integrity protection would need to be implemented in all GSM MSCs globally, otherwise an attacker could masquerade as an “old” GSM network in order to mount a false base station attack. This limitation was considered alongside factors during the evaluation of the Vodafone proposal. As a result of the evaluation, 3GPP decided to terminate integrity protection in the RNC, which meant that integrity protection could not be extended to GSM access in the way described in the Vodafone paper. However, this decision does not rule out the deployment of alternative integrity protection solutions for GSM in the future.

<u>Section 4.1, last two sentences</u>

This is the same misunderstanding as in the previous paper (see comments on section IV.B) about support of GSM encryption algorithms not being mandatory. But it is unclear why the authors write these sentences, as they do not enter their argument later. The man-in-the-middle attack described in the paper works without this assumption.

3.2 Discussion

The new contribution in this paper, which adds to known publications about man-in-the-middle attacks in GSM, is to show that using UMTS AKA between a UE and a 3G MSC does not help if the RAN is GSM. UMTS solves false base station attacks through a combination of UMTS AKA and mandatory integrity protection. Since GSM does not support integrity protection, dual mode GSM/UMTS handsets are still vulnerable to false base station attacks even if UMTS AKA is applied for GSM access. This is a limitation of the 3GPP security architecture which was known by 3GPP during the design, but which was not, as far as we are aware, described in detail in any previous publications. To help protect against false base station attacks in GSM, the authors propose that integrity protection is added to GSM. This has recently been considered in 3GPP as a possible enhancement to GSM (cf. S3-040262, Analysis of the authenticated GSM cipher command mechanism [3]). It is expected that solutions to protect GSM systems against false base station attacks will be considered within the scope of the recently approved work item on Access Security Enhancements, SP-040865 (= S3-041077) [4].

4 Conclusions and proposals

The limitations of GSM security described in the papers were well known to 3GPP. They are already within scope of the recently approved work item on Access Security Enhancements, SP-040865 (= S3-041077) [3]. These limitations include:

- Protection against bidding down of GSM encryption algorithms by a man-in-the-middle.
- Protection against GSM false base station attacks.

Changes to the GSM security specifications may result from this work item.

We do not believe that the papers require 3GPP to make any changes to the UMTS security specifications. The most significant contribution of the papers in this area is to highlight the case when a UMTS subscriber is authenticated via a GSM BSS connected to a 2G MSC and then handed over to UMTS (case 5 in section V.A of the PIMRC paper). The authors correctly explain that discovery of the GSM encryption key due to a GSM weakness would lead to discovery of the UMTS keys. Here, the UMTS subscriber is affected by GSM attacks even while communicating in a UMTS network. We believe that this is an undesirable situation and that solutions should be made available to operators to remedy this situation. The solution proposed by Meyer/Wetzel is to run re-authentication during inter-system handover. While the UMTS specifications are compatible with this solution, in this contribution we identified a number of problems with this approach and proposed the following countermeasures, which do not require any changes to 3GPP specifications:

- Networks should be configured to ensure that there is a UMTS re-authentication after a change from a 2G MSC to a 3G MSC in idle mode when a GSM security context was transferred.
- Networks should be configured to ensure that all 2G-MSC/VLRs, which support handover to UTRAN, also support and use UMTS AKA.

A similar problem exists in the PS domain, so the following countermeasures are proposed:

- Networks should be configured to ensure that there is a UMTS re-authentication after a change from a 2G SGSN to a 3G SGSN in idle mode when a GSM security context was transferred.
- PS handover is currently being developed in 3GPP - see TS 43.129 [8]. If inter-system RAT handover (GERAN A/Gb → UTRAN) is supported, then networks should be configured to ensure that all 2G-SGSN, which support handover to UTRAN, also support and use UMTS AKA.

We believe that re-authentication at 2G → 3G MSC/SGSN change in idle mode can be implemented by suitable configuration of authentication policy settings on existing MSCs and SGSNs. The extent to which existing 2G MSCs (and future 2G SGSNs that support inter-RAT PS handover) support and use UMTS AKA is less clear. However, it is important to highlight that the 3GPP specifications do not preclude the implementation of UMTS AKA on 2G MSCs and 2G SGSNs. Even if an upgrade of existing 2G MSCs to support UMTS AKA was required, such an upgrade seems to be the far smaller effort, compared to ensuring re-authentication in mid-call.

If these countermeasures are agreed by SA3 then they should be forwarded to the GSM Association who could turn them into recommendations for operators.

5 References

[1] Meyer, U, Wetzel, S.: 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), September 2004, IEEE, 2004. http://www.cdc.informatik.tu-darmstadt.de/~umeyer/UliPIMRC04.pdf

[2] Meyer, U., Wetzel, S.: A Man-in-the-Middle Attack on UMTS. Proceedings of ACM Workshop on Wireless Security (WiSe 2004), October 2004, ACM, 2004.
(Available to purchase from ACM)

[3] Vodafone contribution to 3GPP: S3-040262, Analysis of the authenticated GSM cipher command mechanism. 3GPP SA3 meeting #33, 10-14 May 2004, Beijing, China.

[4] WID proposal to 3GPP SA: SP-040865 (=S3-041077), WID for Access Security Enhancements. 3GPP SA meeting #26, December 2004, Athens, Greece.

[5] LS from 3GPP CN1 to 3GPP SA3: S3-040207 (= N1-040501), LS on Re-authentication and key set change during inter-system handover. 3GPP SA3 meeting #33, 10-14 May 2004, Beijing, China.

[6] LS from 3GPP CN1 to 3GPP SA3: S3-040708 (=N1-041519), LS on Re-authentication and key set change during inter-system handover. 3GPP SA3 meeting #35, 5-8 October 2004, Malta.

[7] Vodafone contribution to 3GPP: S3-990206, Response to “CR to TS 25.301 - Integrity control mechanism”. 3GPP SA3 meeting #5, 5-9 July 1999, Sophia Antipolis, France.

[8] 3GPP TS 43.129, Packet-switched handover for GERAN A/Gb mode; Stage 2 (Release 6).

ON THE IMPACT OF GSM ENCRYPTION AND MAN-IN-THE-MIDDLE ATTACKS ON THE SECURITY OF INTEROPERATING GSM/UMTS NETWORKS

Ulrike Meyer[1], Susanne Wetzel[2]

[1] Darmstadt University of Technology, Department of Computer Science, Hochschulstrasse 10, 64283 Darmstadt, Germany, umeyer@cdc.informatik.tu-darmstadt.de
[2] Stevens Institute of Technology, Department of Computer Science, Castle Point on Hudson, Hoboken, NJ 07030, USA, swetzel@cs.stevens-tech.edu

Abstract - GSM suffers from various security weaknesses: Just recently, Barkan, Biham and Keller presented a ciphertext-only attack on the GSM encryption algorithm A5/2 which recovers the encryption key from a few dozen milliseconds of encrypted traffic within less than a second. Furthermore, it is well-known that it is possible to mount a man-in-the-middle attack in GSM during authentication which allows an attacker to make a victim mobile station authenticate itself to a fake base station which in turn forwards the authentication traffic to the real network, thus impersonating the victim mobile station to a real network and vice versa.

In this paper we discuss the impact of GSM encryption attacks, that recover the encryption key, and the man-in-the-middle attack on the security of networks, which employ UMTS and GSM base stations simultaneously.

We suggest to protect UMTS connections from GSM attacks by integrating an additional authentication and key agreement on intersystem handovers between GSM and UMTS.

Keywords - UMTS, GSM, security, handover, attack

I. Introduction

Mobile telephony in general and in Europe in particular is on the move from 2G to 3G, i.e., GSM to UMTS networks. As long as UMTS is not in operation on a large scale, both GSM and UMTS technologies will coexist and have to interoperate. I.e., during the transition phase there will be areas with GSM coverage only, areas with UMTS coverage only and areas with both UMTS and GSM coverage. In order to facilitate the transition from GSM to UMTS, the UMTS standard allows subscribers to roam between UMTS and GSM base stations depending on what is available at their current location. Thus, subscribers can access network services such as, for example, initiating phone calls independently of their location. Furthermore, the standard allows for session handovers from GSM to UMTS base stations and vice versa. This even tighter form of interoperation between UMTS and GSM enables a subscriber to stay connected while moving.

In order to allow for interoperation between the two technologies, the UMTS standard implements mechanism to accommodate key management and authentication based on the different security methods defined in GSM and UMTS [1]. In particular, during session handovers between GSM and UMTS it is defined that no new authentication between the mobile station of the subscriber and the network takes place. As a consequence, no new encryption and integrity protection keys are established. Instead, the keys used prior to the handover are simply converted into the format mandated by the new base station taking over the session. The respective keys are sent to the new base station [1].

In this paper we show, that this conversion and transfer of keys exposes the UMTS connection to well-known vulnerabilities of GSM, namely attacks on the GSM encryption and a man-in-the-middle attack.

Recently, a very efficient attack on GSM encryption was published by Barkan, Biham and Keller [2]. Their attack on the encryption algorithm A5/2 allows an attacker to recover the encryption key after catching only a few milliseconds of encrypted traffic. It is furthermore well-known, that GSM is vulnerable to a man-in-the-middle attack by means of which an attacker can impersonate a valid base station to the user and the user to the network at the same time [3], [2].

In this paper we describe the impact of GSM encryption attacks on UMTS connections before and after handovers between GSM and UMTS and show how a GSM man-in-the-middle attack can be carried over to UMTS because of handover procedures. We furthermore propose countermeasures which allow to protect UMTS connections from GSM attacks by integrating an additional authentication and key agreement on intersystem handovers between GSM and UMTS.

The rest of the paper is organized as follows: First, we describe the authentication and key management mechanisms defined in GSM and UMTS including key generation and usage during handover. Then, we briefly summarize the known results on GSM encryption attacks and the well-known GSM man-in-the-middle attack. The main focus of the paper is Section V which discusses the impact of both attack types on the security of interoperating GSM/UMTS networks. In Section VI we propose countermeasures to thwart the vulnerabilities. We conclude the paper with a brief summary.

II. Authentication and Key Management in GSM and UMTS

In general, subscribers to a network can not only access the network they originally subscribed to – the so-called *home network* – but can also visit foreign networks, for example, in areas or other countries where their home network has no coverage. In the following we refer to the home network as the network the subscriber originally subscribed to and to a visited network as a network the subscriber currently is connected to. The visited network can either be a foreign network or the home network itself.

A. Authentication and Key Management in GSM

In GSM, every subscriber shares a long term secret key K_i with its home network. This key is used to authenticate the mobile station to the visited network and to generate session keys used to encrypt the mobile communication.

The Authentication Center (AuC) in the home network generates authentication vectors consisting of a challenge response pair $(RAND_G, RES_G)$ and an encryption key Kc. On request, the home network sends an authentication vector to the mobile switching center (MSC) in the visited network. In order to authenticate the mobile station, the mobile switching center (MSC) in the visited network sends the challenge $RAND_G$ to the mobile station. The mobile station uses the challenge $RAND_G$ and the long term secret key K_i to generate the authentication response RES^*_G and the encryption key Kc and sends RES^*_G back to the MSC. The MSC compares the response of the mobile station with the expected response RES_G. After a successful authentication the MSC sends the encryption key Kc to the base station serving the mobile station. Subsequently, the base station and the mobile station use Kc to encrypt their communication. The GSM authentication procedure is illustrated in Fig. 1. For a detailed description of the GSM authentication please refer to [4].

The encryption key Kc is 64 bits long and is used as long as no new authentication takes place. How often a new authentication takes place is left to the network operator. The GSM standard only defines situations in which the operator may demand a new authentication, e.g., before mobile originated calls or during location updates [4]. Thus, the same encryption key may stay in use for a very long time, e.g., subsequent calls.

The encryption algorithm used in GSM is a stream cipher of the algorithm family A5. Currently A5/0 (no encryption), A5/1 (standard encryption), A5/2 (weaker version of A5/1) and A5/3 (similar to the KASUMI algorithm used in UMTS) are defined [4]. During security setup (which directly follows authentication), the mobile station and the network agree upon the algorithm to be used. First, the mobile station sends its security capabilities to the network. Then, the base station selects one of the encryption algorithms the mobile station is capable of and informs the mobile station of its choice.

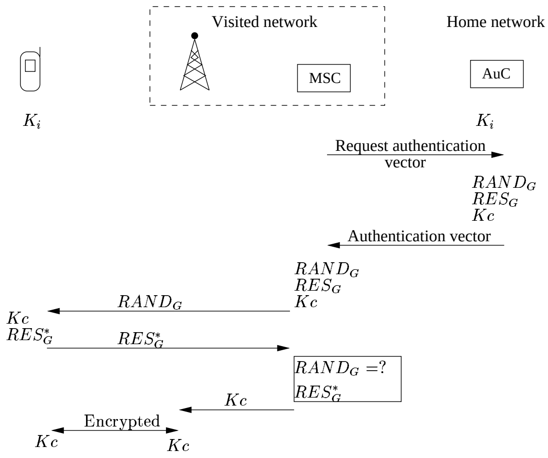

Fig. 1
Authentication and Key Agreement in GSM

The encryption key Kc is independent of the choice of the encryption algorithm.

B. Authentication and Key Management in UMTS

The authentication and key management in UMTS is based on the same principles as in GSM. Every subscriber shares a long term secret key with its home network which is used to authenticate the mobile station to the network and to generate the secret session keys. As in GSM, the home network generates authentication vectors. A visited network can request an authentication vector for a mobile station from its home network in order to authenticate the mobile station.

Unlike in GSM, UMTS networks also provide a mechanisms, the so-called authentication token $AUTN$, to protect the mobile station against attackers trying to impersonate a valid network to the mobile station. During authentication, the MSC of the visited network sends the authentication challenge together with the authentication token to the mobile station. The token contains a sequence number. Upon receipt of the token, the mobile station checks whether the sequence number is in the right range. This protection is often referred to as network authentication. If the authentication token is in the right range, the mobile station computes the authentication response RES_U and the encryption and integrity protection keys CK and IK. The mobile station sends RES_U back to the MSC. The MSC checks the correctness of RES_U.

While this protection works well in UMTS-only networks it is shown in [5] that it is not effective in interoperating UMTS/GSM networks.

The encryption and integrity keys are both 128 bits long and as such are twice as long as the GSM key. The UMTS authentication is illustrated in Fig. 2 and described in more detail in [1] Unlike in GSM, there are counters in UMTS on

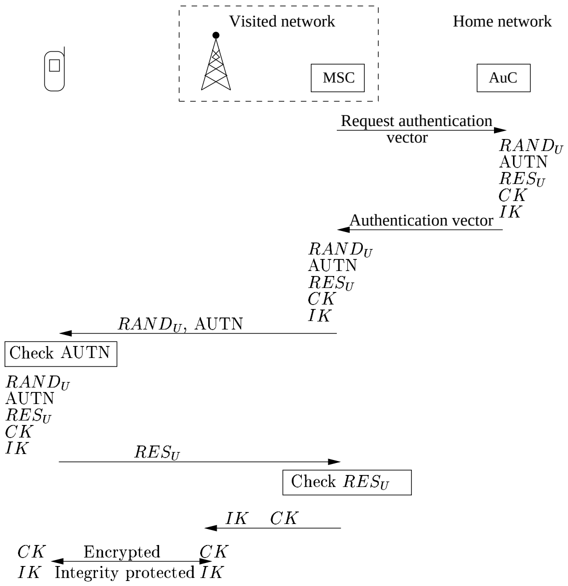

Fig. 2
Authentication and Key Agreement in UMTS

how many packets have been encrypted (integrity protected) with the same encryption (integrity) key. As soon as one of the counters exceeds an operator-set limit, a new authentication is enforced immediately before the next connection to a base station.

To date, only one encryption algorithm is defined for UMTS. It is a stream cipher based on the block cipher KASUMI. The integrity protection is based on the same cipher [6].

In both GSM and UMTS authentications are carried out between the mobile station and the MSC. In GSM the encryption is employed between a mobile station and a base station. In UMTS the encryption reaches a bit further back into the backbone network, namely the radio network controller (RNC) which is located between the base station and the MSC. In order to simplify explanations for the remainder of this paper we will nevertheless refer to the UMTS base station as the end point of the encryption.

C. Authentication and Key Management in Interoperating UMTS and GSM Networks

In interoperating GSM/UMTS networks, UMTS and GSM base stations are in operation at the same time. Some areas of either the home or visited network may have both GSM and UMTS coverage, others may have UMTS coverage or GSM coverage only. In order to be able to connect to whatever base station is available at a current location, a subscriber's mobile station must support both the GSM radio interface and the UMTS radio interface. Throughout this paper we assume that all subscribers are equipped with mobile stations of this kind.

While the smart card of a GSM subscriber is a Subscriber Identity Module (SIM) the UMTS subscriber's smart card is a User Services Identity Module (USIM).

While the UMTS encryption and integrity protection algorithms are implemented on the mobile unit itself, the longterm secret GSM (UMTS) key K_i and the algorithms for the generating the GSM (UMTS) authentication responses are part of the SIM (USIM) card. As detailed earlier, these algorithms and keys are different for the two types of smart cards. The GSM encryption algorithm is also implemented on the SIM card and can be implemented on the USIM card as well. UMTS subscribers can only connected to GSM base stations if their USIM supports the GSM encryption and authentication algorithm.

On the network side, base stations are connected to the operator's backbone network via mobile switching center (MSC). There are two types of MSCs. The old type of MSCs (2G MSCs), to which only GSM base stations can be connected to and the new type of MSCs (3G MSCs) to which UMTS base stations *and* GSM base stations can be connected to. GSM base stations only support GSM encryption and UMTS base stations only support UMTS integrity protection and encryption. 2G MSCs only support the GSM authentication algorithm while 3G MSCs support both GSM authentication *and* UMTS authentication.

Combining the different types of smart cards, types of serving base station and types of MSCs leads to a number of different authentication scenarios in order to allow for roaming of mobile stations:

Case 1: A GSM subscriber is authenticated via a GSM base station, which is connected to a a 2G or 3G MSC.
This is the standard GSM scenario as described in Fig. 1. For GSM subscribers the authentication procedure is the same for both types of MSCs.

Case 2: A GSM subscriber is authenticated via a UMTS base station, which is connected to a 3G MSC.
In this case a GSM subscriber connects to the network via a UMTS base station. The visited network requests a GSM authentication vector $(RAND_G, Kc, RES_G)$ from the home network. The MSC and the mobile station perform the GSM authentication as described in Fig. 1. The UMTS base station simply forwards the GSM authentication messages. The MSC sends $RAND_G$ to the mobile station (via the UMTS base station). The mobile station generates the authentication response $RAND_G^*$ and the encryption key Kc from $RAND_G$ and the longterm secret key K_i. Then, the mobile station sends $RAND_G^*$ back to the MSC which compares $RAND_G^*$ to $RAND_G$. The authentication is deemed successful, if the two values match.

After a successful authentication the mobile station and the MSC convert the established GSM key Kc into UMTS keys

$$CK = c_4(Kc) = Kc||Kc \quad (1)$$
$$IK = c_5(Kc) = Kc_1 \oplus Kc_2||Kc||Kc_1 \oplus Kc_2, \quad (2)$$

where $Kc = Kc_1||Kc_2$ and Kc_1 and Kc_2 are 32 bits in length. The UMTS keys CK and IK are subsequently used to encrypt and integrity protect the communication between the UMTS base station and the mobile station. The integrity protection of the signaling messages is always immediately started after handover to UMTS while encryption is only enabled after handover if it was enabled before handover.

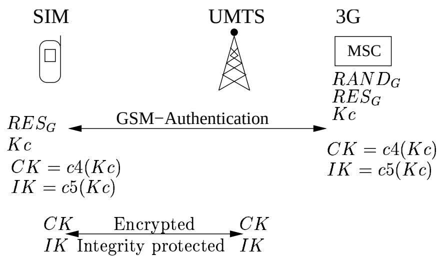

Fig. 3
Authentication in Case 2

Case 3: A UMTS subscriber is authenticated via a UMTS base station, which is connected to a 3G MSC.
This is the case described in Fig. 2, where a UMTS subscriber authenticates himself to a UMTS-only network.

Case 4: A UMTS subscriber is authenticated via a GSM base station, which is connected to a 3G MSC.
In this case a UMTS subscriber is connected to a GSM base station and this GSM base station is connected to a 3G MSC. Since the 3G MSC supports UMTS authentication, the UMTS authentication can be carried out as described in Fig. 2. The GSM base station forwards the UMTS authentication traffic transparently.

After completing authentication the mobile station and the MSC convert the generated UMTS keys IK and CK into a GSM key Kc:

$$Kc = c_3(CK, IK) = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2, \quad (3)$$

where CK and IK are each split into CK_1, CK_2 IK_1 and IK_2 with length 64 bits each, such that $CK = CK_1||CK_2$ and $IK = IK_1||IK_2$.

The mobile station and the GSM base station subsequently use Kc to encrypt the traffic (see Fig. 4).

Case 5: A UMTS subscriber is authenticated via a GSM base station, which is connected to a 2G MSC.
Since a 2G MSC does not support UMTS authentication, a UMTS subscriber can be authenticated by a 2G MSC if and only if the USIM supports the GSM authentication algorithm.

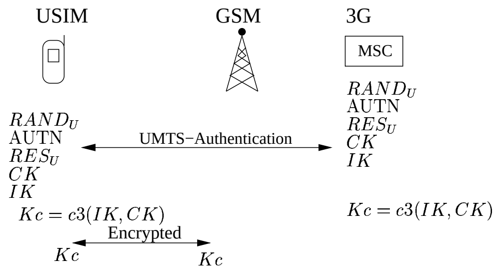

Fig. 4
Authentication in Case 4

The visited network requests a GSM authentication vector from the home network. The home network first generates a UMTS authentication vector and then converts it into a GSM authentication vector. The GSM authentication challenge and the UMTS authentication challenge are the same, i.e., $RAND_G = RAND_U$. The 32 bit GSM authentication response RES_G is generated from the 128 bit UMTS authentication response RES_U by splitting the UMTS response into four 32 bit values such that $RES_U = RES_{U_1}||RES_{U_2}||RES_{U_3}||RES_{U_4}$ and computing

$$RES_G = c_2(RES_U)$$
$$= RES_{U_1} \oplus RES_{U_2} \oplus RES_{U_3} \oplus RES_{U_4}$$

The GSM encryption key is derived as in equation 3:

$$Kc = c_3(CK, IK)$$

The home network forwards the GSM authentication vector to the visited network. The MSC in turn sends the authentication challenge to the mobile station which itself generates the GSM authentication information following the above mentioned procedure. This is followed by the remainder of the standard GSM authentication procedure. After successful completion of the authentication the GSM encryption key Kc is used to encrypt the traffic between the mobile station and the GSM base station.

III. Key Conversion during Intersystem Handovers

The focus of the last section was on roaming between GSM and UMTS networks which allows a subscriber to use services independently of his location, e.g., initiate a call. In addition to roaming the UMTS standard also supports session handovers which allow a subscriber to continuously use a service while moving, e.g., move while calling someone. In an interoperating GSM/UMTS network such session handovers can not only occur from UMTS to UMTS base stations, or GSM to GSM base stations but also from UMTS base stations to GSM base stations and vice versa. In the following we discuss how the communication between a

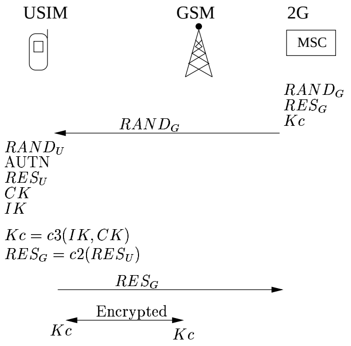

Fig. 5
Authentication in Case 5

mobile station and the new base station is protected after a handover occurred.

On handover between two UMTS base stations, the currently used encryption and integrity keys are sent to the new base station system and are reused after handover.

Similarly, upon handover between two GSM base stations, the GSM encryption key is sent to the new base station and reused for encryption after handover. However, the encryption algorithm used after handover may be different from the one used before handover, e.g., if the new base station does not support the encryption algorithm used before handover. The new algorithm to be used is indicated to the mobile station as part of the handover command message.

On intersystem handovers from a UMTS base station to a GSM base station the UMTS keys IK and CK are converted into a GSM key Kc using the conversion function c_3 (see equation 3). AS the GSM base station does not support the UMTS encryption and integrity protection after handover to GSM, Kc is used for encryption. This is independent of the subscriber type.

On intersystem handovers from a GSM base station to a UMTS base station we have to distinguish between three different cases: If a GSM subscriber is to be handed over, the GSM key is converted into UMTS keys using the conversion functions c_4 and c_5 respectively (see equations 1 and 2).

If a UMTS subscriber is to be handed over and the GSM base station is connected to a 2G MSC, the currently used GSM key Kc is converted into UMTS keys CK and IK using the conversion functions c_4 and c_5 respectively (see equations 1 and 2).

If on the other hand the GSM base station is connected to a 3G MSC, then the MSC has a copy of the UMTS keys that were generated during the last authentication. The MSC then simply forwards these original UMTS keys to the new UMTS base station during handover.

Note, that subsequent key conversions from GSM to UMTS and back to GSM retrieve the original GSM key:

$$c_3(c_4(Kc), c_5(Kc)) = Kc$$

Moreover, if encryption was disabled before handover, it will stay disabled after handover.

IV. GSM Attacks

A. Attacks on GSM Encryption

The GSM encryption algorithms A5/1 and A5/2 were originally kept secret. However, in 1994 a sketch of the design of A5/1 was leaked. In 1999 Briceno, Goldberg and Wagner [7] reverse engineered the exact design of both algorithms. Since then various attacks on the algorithms were published. The first publicly available cryptanalysis of A5/1 was published by Golic in 1997 [8]. Other attacks soon followed in [9], [10] and [11]. For A5/2 Goldberg et al. [12] first devised a known plain-text attack which requires the attacker to know the XOR of two plain-texts that are exactly 2^{11} frames apart. Subsequently, Petrovic et al. [13] proposed an attack which allows to predict the key stream produced by A5/2 from the knowledge of a few hundred known ciphertext/plaintext bit pairs. The strongest attack on A5/2 known to date was described by Biham, Barkan and Keller [2]. The cipher-text-only attack requires only a few milliseconds of encrypted voice traffic (4 frames) to be passively intercepted by the attacker in order to allow the recovery of the corresponding encryption key Kc within less than a second. The attack works because encryption is applied after error correction. This leads to known linear relationships between the plain-text bits to be encrypted. The authors also describe three active attacks that use the A5/2 attack to break the encryption if A5/1 or A5/3 are used.

In the following we concentrate on the type of encryption attacks (such as the A5/2 attack of Biham, Barkan and Keller) which recover the encryption key Kc. The impact of encryption attacks that merely predict the key stream output of a GSM encryption algorithm is not studied in this paper.

B. Man-in-the-Middle Attack

GSM is vulnerable to a man-in-the-middle attack which allows an attacker to impersonate a false base station to a victim mobile station and to impersonate the victim to a real network at the same time [3]. In order to mount this attack, the attacker forces the mobile station to connect to a fake base station by broadcasting the network number of the subscriber's home network. If the mobile station is in stand-by mode, it will always connect to the base station it receives best. Thus, the attacker can make the mobile station connect to him by drowning any present real base station. After connection set-up, the fake base station impersonates the mobile station to the network by resending the identity information it received from the mobile station. In the subsequent authentication process the attacker simply forwards the authentication traffic between the mobile station and the real network. By sending false information about its encryption capabilities to the network, the attacker can disable the encryption between himself and the network. By requesting to turn off encryption the attacker can also disable the encryption between the mobile station and the fake base station. This attack not only allows the attacker to eavesdrop on the communication between the mobile station and the network but also to insert and modify traffic.

V. Impact of GSM Attacks on Interoperating GSM/UMTS Networks

A. Impact of Encryption Attacks

In this section we will now discuss how an attack that recovers the GSM encryption key (like the A5/2 attack described above) influences the network security in networks where both GSM and UMTS technologies are available simultaneously. As discussed earlier, these kind of networks already exist and will continue to exist until the last GSM subscriber has updated his subscription to a UMTS subscription and the last base station that is capable of GSM only has been replaced.

In the following we analyze the impact of the attack and intersystem handover procedures for the different combinations of subscriber type, handover to or from UMTS and type of MSC.

Case 1: A GSM subscriber is authenticated in a GSM network and is handed over to UMTS.

During GSM authentication, the encryption key Kc was generated on the SIM card as well as in the home network. It was used to protect the communication between the mobile station and the GSM base station. Upon handover to UMTS, the mobile station and the new MSC convert Kc into the UMTS keys IK and CK using the conversion functions c_4 and c_5. If the MSC before handover is 3G MSC, it is this MSC which converts the GSM key and sends it to the new MSC. If the old MSC is a 2G MSC, the GSM key is sent to the new MSC which then converts the GSM key into UMTS keys.

If an attacker can break the GSM encryption algorithm used before handover, then the attacker knows the encryption key Kc. She can then also convert Kc into the UMTS keys using c_4 and c_5 and thus break the UMTS encryption and integrity protection after handover. The attacker can then eavesdrop on the communication between the mobile station and the base station and can insert and manipulate traffic between them.

Case 2: A GSM subscriber is authenticated in a UMTS network and is handed over to GSM.

During authentication, the GSM encryption key Kc was generated on the SIM card and in the home network. The MSC of the visited network and the mobile station both converted Kc into the UMTS keys $IK = c_5(Kc)$ and $CK = c_4(Kc)$. The UMTS keys were used to encrypt and integrity protect the communication between the mobile station and the UMTS base station before handover. Upon handover to GSM, the original encryption key Kc is recovered in the mobile station and in the old MSC by means of $c_3(CK, IK) = c_3(c_4(Kc), c_5(Kc)) = Kc$ and sent to the GSM base station.

If an attacker can break the GSM encryption algorithm used after handover, i.e., she can recover the GSM encryption key Kc she can also compute the UMTS keys IK and CK used before handover using the conversion functions c_4 and c_5. If the attacker has recorded the communication between the UMTS base station and the mobile station before handover she can now decrypt the recorded traffic.

Case 3: A UMTS subscriber is authenticated in a UMTS network and is handed over to a GSM base station, that is connected to a 3G MSC.

During authentication, the UMTS keys IK and CK were generated on the USIM and in the home network. These keys were used before handover. Upon handover to a GSM base station, the keys are converted into a GSM key Kc by means of $c_3(IK, CK) = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2$ in both the mobile station and the old MSC. The GSM key *and* the UMTS keys are transfered from the old 3G MSC to the new 3G MSC. The 3G MSC stores the UMTS keys for subsequent handovers back to UMTS. The GSM encryption key Kc is used to encrypt the communication between the mobile station and the GSM base station after handover.

If an attacker can break the encryption algorithm used after handover, i.e., recovers the encryption key Kc then this the knowledge of Kc leaks 64 bits of information of the 256 bit UMTS keys used before handover.

Case 4: A UMTS subscriber is authenticated via a UMTS base station and is handed over to a GSM base station, that is connected to a 2G MSC.

During authentication, the UMTS keys were generated on the USIM card and in the home network. Before handover, the UMTS keys were used to secure the communication between the mobile station and the old MSC. Upon handover to GSM, the keys are converted in the mobile station and in the old MSC to a GSM key Kc using the conversion function c_3. Kc is then transfered from the old 3G MSC to the new 2G MSC. Unlike in case 3 the UMTS keys are not transfered.

Breaking the GSM encryption after handover again reveals 64 bit of the UMTS key material to the attacker.

Case 5: A UMTS subscriber is authenticated via a GSM base station that is connected to a 2G MSC and is then handed over to a UMTS base station.

Since the 2G MSC is not able to perform a UMTS authentication, the mobile station and the home network have to perform a GSM authentication. During this authentication the UMTS keys IK and CK were generated on the USIM card as well as the home network and immediately converted into the GSM key Kc using c_3. Upon handover to UMTS, the GSM key Kc is converted into UMTS keys $IK^* = c_5(Kc)$ and $CK^* = c_4(Kc)$. These keys are different from the keys IK and CK that were generated on the USIM card during authentication.

If an attacker can recover the GSM encryption key Kc before handover, she can use Kc to compute the UMTS keys IK^* and CK^*. Thus, the encryption and integrity protection after handover are broken. Moreover, handover reveals 64 bits of information of the UMTS keys IK and CK generated during authentication.

Case 6: A UMTS subscriber is authenticated via a GSM base station that is connected to a 3G MSC and is then handed over to a UMTS base station.

Since the 3G MSC can carry out a UMTS authentication, the mobile station and the home network perform such a UMTS authentication. The GSM base station transparently forwards the authentication traffic. During the authentication, the UMTS keys were generated on the USIM card and in the home network. After a successful authentication, the UMTS keys are converted into a GSM encryption key Kc using the conversion function c_3. Instead of converting the GSM key into a UMTS key upon handover to UMTS, the original UMTS keys stored in the MSC are transfered from the old MSC to the new MSC and from the new MSC to the UMTS base station.

An attacker who can recover the GSM encryption key Kc can thus only learn of 64 bits of information of the UMTS key material used after handover.

In summary this analysis shows that for GSM subscribers a single handover to GSM breaks all pre-handover and post-handover UMTS communication. For UMTS subscribers a handover to a GSM base station that is connected to a 3G MSC reveals 64 bits of information of the key material used in pre-handover or post-handover UMTS communication. In case of a handover to a 2G MSC the impact is even worse: a single handover to a GSM base station, that is connected to a 2G MSC breaks the encryption and integrity protection of all pre-handover and post-handover UMTS communication.

B. Impact of the Man-in-the-Middle Attack

A man-in-the-middle attack as described in Section IV-B can occur on any GSM authentication. As GSM subscribers as well as UMTS subscribers can connect to GSM base stations and be authenticated in GSM style, both types of subscribers are vulnerable to the attack.

Assume that a subscriber has caught a man-in-the-middle attacker and the attacker as well as the mobile station move out of range of the serving GSM base station to which the attacker originally impersonated the victim. As described earlier, the attacker has disabled the encryption between himself and the network as part of the attack. Consequently, upon handover to UMTS the encryption is not enabled because it was disabled before handover. However, in order for the man-in-the-middle attack to carry over to UMTS, the attacker has to master the integrity protection of the signaling messages between the mobile station and the UMTS base station which is started right after handover. (As discussed earlier, the integrity protection algorithm is implemented on the mobile phone of the subscriber.)

In order for the attacker to continue to impersonate the victim mobile station to the network, the attacker has to sent correctly integrity protected messages to the network. The attacker cannot generate these messages herself, but can force the mobile station to generate them instead: the attacker simulates a handover to a UMTS base station to the mobile station by impersonating the GSM base station and the UMTS base station at the same time. The attacker sends a handover command to the mobile station that tells the mobile station to connect to the fake UMTS base station. Depending on whether the last authentication was a GSM authentication or the last authentication was a UMTS authentication, the subscriber either converts the GSM key into UMTS keys or activates the stored UMTS keys for use after handover. Since the mobile station will integrity protect the messages, the attacker only needs to transparently forward these messages to the real UMTS base station.

Note that the impact of this attack differs from the impact of the encryption attacks. A man-in-the-middle attack does not depend on any type of broken encryption algorithm and thus always negatively impacts interoperating UMTS/GSM networks.

VI. COUNTERMEASURES

In order to protect from the A5/2 attack in general, the 3GPP currently discusses to disable A5/2. While this would protect from the concrete threat of the attack to GSM networks and from the impact of the attack on interoperating UMTS/GSM networks, the threat of similar attacks recovering the encryption key on interoperating UMTS/GSM networks will remain. Furthermore, disabling A5/2 does not protect from carrying over man-in-the-middle attacks from GSM to UMTS.

Instead, we propose the integrating of an additional UMTS authentication and key agreement procedure in connection with intersystem handovers in order to secure the UMTS part of the network against GSM encryption attacks. Newly generated UMTS keys have no known relation to a broken GSM key and a newly generated GSM key does not reveal any information about formerly used UMTS keys.

Furthermore, the additional UMTS authentication also prevents man-in-the-middle attacker to be carried over from GSM to UMTS since the authentication between a UMTS base station and a UMTS subscriber is secure against man-in-the-middle attacks.

Upon handover from UMTS to GSM the new authentication is to be carried out while the subscriber is still connected to a UMTS base station. I.e., a new authentication is performed, whenever a subscriber enters a UMTS cell, that is a border cell to a GSM part of the network. If the newly generated keys are UMTS keys, the mobile station and the 3G MSC convert them into a GSM key Kc using c_3. The mobile station and the serving 3G MSC store this key until the actual handover to GSM takes place. Upon handover to GSM the old MSC transfers the key to the new MSC which in turn forwards it to the base station.

In the case of a handover from GSM to UMTS where the GSM base station is connected to a 3G MSC, the new authentication can be carried out before the actual handover. In this case the MSC can initiate an authentication as soon as the mobile station enters the cell. Since the 3G MSC can do a UMTS authentication it can authenticate the mobile station using the respective procedure as described in Section II-C. Upon handover the newly established keys are sent to the UMTS base station.

In case of a handover from GSM to UMTS where the GSM base station is connected to a 2G MSC, the 2G MSC is not capable of performing a UMTS authentication. Authenticating before handover does therefore not protect form a man-in-the-middle attack. Instead the new authentication must take place right after the handover. While this implies that an attacker can eavesdrop on the first few seconds of the connection to the UMTS network, the attacker will be shut out as soon as the authentication is successfully completed.

In order to avoid unnecessary authentications, sophisticated methods can be used to determine whether a mobile station that is currently located in a GSM cell is really going to be handed over to UMTS [14].

VII. Conclusion

In this paper we have described the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating UMTS/GSM networks.

We have shown, that for GSM subscribers a single handover to GSM breaks all pre-handover and post-handover UMTS communication. For UMTS subscribers a handover to a GSM base station that is connected to a 3G MSC reveals 64 bits of information of the key material used in pre-handover or post-handover UMTS communication. The impact of a handover to a 2G MSC is even worse as a single handover to a GSM base station breaks the encryption and integrity protection of all pre-handover and post-handover UMTS communication.

Furthermore, we have discussed that handover procedures allow man-in-the-middle attacks to be transfered from GSM to UMTS.

In order to thwart the attacks we have proposed to carry out an additional authentication and key agreement in connection with intersystem handovers.

References

[1] 3GPP Technical Specification, “3GPP TS 33.102, V5.3.0, Third Generation Partnership Project; Technical Specifications Group Services and System Aspects; 3G Security; Security Architecture,” September 2003.

[2] E. Barkan, E. Biham, and N. Keller, “Instant ciphertext-only cryptanalysis of GSM encrypted communication,” in *Advances in Cryptology - CRYPTO 2003*, vol. 2729 of *LNCS*, pp. 600–616, August 2003.

[3] D. Fox, “Der IMSI-catcher,” *DuD, Datenschutz und Datensicherheit*, 2002.

[4] ETSI Technical Specification, “ETSI TS 100.929, V8.0.0, Digital Cellular Telecommunications System (phase 2+)(GSM); Security related network functions,” 2000.

[5] U. Meyer and S. Wetzel, “A man-in-the-middle attack on UMTS.” in submission.

[6] 3GPP Technical Specification, “3GPP TS 35.202 V5.0.0, Third Generation Partnership Project; Technical Specification Group; 3G Security; specification of the 3GPP confidentiality and integrity algorithms; document 2: Kasumi algorithm specification,” Juni 2002.

[7] M. G. I. Briceno and D. Wagner, “A pedagogical implementation of the gsm A5/1 and A5/2 ”voice privacy” encryption algorithms.” http://cryptome.org/gsm-a512.htm, 1999.

[8] J. Golic, “Cryptanalysis of alleged A5 stream cipher,” in *Advances in Cryptology*, vol. 1233 of *LNCS*, pp. 239–255, Springer Verlag.

[9] A. Biryukov, A. Shamir, and D. Wagner, “Real time cryptanalysis of A5/1 on a pc,” in *Advances in Cryptology, proceedings of Fast Software Encryption’00*, vol. 1978, pp. 1–18, Springer-Verlag, 2001.

[10] E. Biham and O. Dunkelman, “Cryptanalysis of the A5/1 gsm stream cipher,” in *Progress in Cyptoloty, proceedings of Indocrypt”00*, LNCS, pp. 43–51, Springer-Verlag, 2000.

[11] P. Ekdahl and T. Johansson, “Another attack on A5/1,” *Transactions on Information Theory*, vol. 49, pp. 284–289, 2003.

[12] I. Goldberg, D. Wagner, and L. Green, “The (real-time) cryptoanalysis of A5/2.” presented at the Rump Session of Crypto’99, 1999.

[13] S. Petrovic and A. Fuster-Sabater, “Cryptanalysis of the A5/2 algorithm.” Cryptology ePrint Archive, Report 200/052, http://eprint.iacr.org, 2000.

[14] U. Meyer, K. Kastell, and R. Jakoby, “Secure handover procedures,” in *Proceedings of the 8th Conference on Cellular and Intelligent Communications*, October 2003.