3GPP TSG SA WG3 Security — SA3#37 **S3-050043**
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

Section IV GSM Attacks

Section IV.B Man-in-the-Middle Attack

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.

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

Section 2, paragraph 2

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.

Section 4.1, last two sentences

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).