Questioning the Feasibility of UMTS-GSM Interworking Attacks

Christoforos Ntantogian[1], Christos Xenakis[2]

[1]Department of Informatics and Telecommunications, University of Athens, Greece

[2]Department of Digital Systems, University of Piraeus, Greece

e-mail: ntantogian@di.uoa.gr, xenakis@unipi.gr

Abstract

Recently, Ahmadian and Salimi [1] presented and analyzed three different attacks that can be performed in UMTS-GSM interworking networks: (i) a real-time eavesdropping attack, (ii) an offline eavesdropping attack, and (iii) an impersonation attack. In this letter we question the feasibility of these attacks. In particular, we pinpoint and analyze that these attacks are based on some erroneous and misleading assumptions that the authors have made regarding the security functionality of the UMTS-GSM interworking networks. Based on this analysis, we deduce that these three attacks cannot be performed.

Keywords: UMTS-GSM interworking attacks, Security architecture of UMTS-GSM interworking networks

Attacks in UMTS-GSM Interworking Networks

Overall, three different attacks, which exploit new identified security weaknesses are presented in [1] targeting UMTS-GSM interworking networks. All attacks are performed in two steps. For the better understanding of the presented notions in this letter, we briefly outline these attacks highlighting the specific erroneous and misleading assumptions.

ATTACK 1: Real time eavesdropping (see Figure 1)

In step 1 of this attack, the adversary performs a man in the middle attack in the GSM-AKA procedure to obtain the session key Kc of GSM-AKA. In step 2, MS executes a UMTS-AKA with a valid 3G VLR/SGSN via a BTS of GSM.

More specifically,

STEP 1: The adversary mounts a man in the middle attack in GSM-AKA

PHASE 1: IMSI catching (the adversary impersonates a BTS of GMS)

1. *The victim MS connects and sends its security capabilities to a false BTS of GSM (ASSUMPTION 3).* The false BTS is under the adversary's control.

2. The adversary sends a user identity request message to the victim MS.

3. MS responses with its permanent identity (IMSI) and the adversary disconnects from MS.

PHASE 2: Obtaining RAND and AUTN (in this phase the adversary impersonates the victim MS)

4. The adversary conveys to 3G VLR/SGSN the security capabilities of the victim MS.

5. The adversary sends the IMSI identity of the victim MS to 3G VLR/SGSN.

6. 3G VLR/SGSN requests from HN/HLR authentication vectors.

7. 3G VLR/SGSN selects the first authentication vector and sends the related RAND and AUTN to the adversary. Upon receiving them, the adversary disconnects from the network.

PHASE 3: Key recovery (in this phase the adversary impersonates a valid BTS)

8. Assume that the victim MS tries to connect with the false BTS, and thus, it sends to the adversary its security capabilities.

9. MS sends its temporary TMSI or permanent IMSI to the adversary.

10. The adversary conveys to MS the same RAND that it received in step 7 of phase 2.

11. The victim MS replies with SRES for its authentication.

12. *The adversary sends to MS a cipher mode command, indicating the use of the weak encryption algorithm A5/2 (ASSUMPTION 1).*

13. MS generates a 64-bit cipher key Kc. The adversary breaks the A5/2 security algorithm and derives the key Kc.

14. The false BTS disconnects.

STEP 2: In this step MS is authenticated using UMTS-AKA via BTS of GSM

PHASE 4: Authentication of MS using UMTS-AKA and passive listening.

15. MS and 3G VLR/SGSN initiate a network connection.

16. MS sends its permanent identity (i.e., IMSI) to 3G VLR/SGSN.

17. 3G VLR/SGSN conveys to MS the same RAND and AUTN with step 7 of phase 2.

18. MS verifies AUTN and conveys to 3G VLR/SGSN its response RES.

19. 3G VLR/SGSN verifies RES.

20. MS is successfully authenticated and 3G VLR/SGSN conveys a cipher mode command to MS indicating the use of a strong encryption algorithm like A5/3.

At the end of step 2, *MS and 3G VLR/SGSN share the same encryption key Kc with the one that the adversary obtained in step 1*, *since the same RAND was used in the two steps (ASSUMPTION 2)*. Thus, the adversary can eavesdrop on the exchanged data between MS and 3G VLR/SGSN, regardless of the employed encryption algorithm (i.e., A5/1 or A5/3).

ATTACK 2: Offline eavesdropping

In step 1 of this attack MS, first, executes a UMTS-AKA via a BTS of GSM, while the adversary records the exchanged encrypted data between the victim MS and the network. In step 2, the adversary recovers the encryption key Kc and decrypts the recorded data.

STEP 1: Traffic Recording

MS performs a successful UMTS-AKA with a 3G VLR/SGSN (via a BTS of GSM). The adversary obtains the RAND value exchanged during UMTS-AKA. Then, it passively records all the encrypted traffic exchanged between MS and the network.

STEP 2: The adversary mounts a man in the middle attack in GSM-AKA

In this step, the adversary impersonates a BTS of GSM and performs step 1 of attack 1, as described previously *(note that the same erroneous assumptions with step 1 of attack 1 are also encountered here, i.e., ASSUMPTION 1 and 3)*. At the end of this step, the adversary obtains the session key Kc which was used in step 1 to encrypt the exchanged data between MS and 3G VLR/SGSN. This happens because *in both steps the same RAND is used, and, therefore, the session key Kc of steps 1 and 2 is the same (ASSUMPTION 2)*. Thus, the adversary can decrypt all the encrypted data recorded.

ATTACK 3: Impersonation attack (see Figure 2)

In step 1 of this attack, the adversary performs a man in the middle attack in the UMTS-AKA procedure to obtain the session key Kc. In step 2, the adversary using the obtained key Kc impersonates a genuine MS to 3G VLR/SGSN, aiming at overcharging the victim MS.

STEP 1: Man in the middle attack and UMTS-AKA execution

PHASE 1: IMSI catching

In this phase, the adversary impersonates a BTS and MS connects to the false BTS (ASSUMPTION 3). Thus, the adversary obtains the IMSI identity of MS as in phase 1 of attack 1.

PHASE 2: Obtaining RAND and AUTN

The adversary impersonates the victim MS and obtains the exchanged RAND and AUTN values. The adversary remains connected with 3G VLR/SGSN.

PHASE 3: Key recovery (the adversary impersonates a BTS)

8. The false BTS forwards the obtained RAND and AUTN to the victim MS.

9. MS verifies AUTN and conveys to the false BTS its response RES.

10. *The adversary obtains RES and sends a cipher mode command to MS indicating the use of the weak A5/2 encryption algorithm (ASSUMPTION 1).*

11. MS generates the cipher key Kc. The adversary breaks the A5/2 algorithm to derive Kc.

12. The adversary completes the connection setup procedure simulating a real network to the victim MS.

STEP 2: Impersonation of MS

PHASE 4: Counterfeit authentication and service theft (the adversary impersonates the victim MS)

13. The adversary forwards to 3G VLR/SGSN the previously obtained RES value (i.e., step 10 of phase 3).

14. The adversary is successfully authenticated to 3G VLR/SGSN, since RES was generated by the legitimate MS. Finally, 3G VLR/SGSN sends a cipher mode command to the adversary indicating the use of a strong encryption algorithm, such as A5/3.

At the end of this phase, the adversary has derived the same cipher key Kc with the victim MS. Thus, the adversary can impersonate the victim MS to overcharge it.

Apart from the analysis of the above attacks, the authors in [1] *propose and analyze some security measures in order to address the identified security weaknesses on which the three attacks are based (ASSUMPTION 4).* The proposed measures do not require extended modifications in the UMTS-GSM network infrastructure.

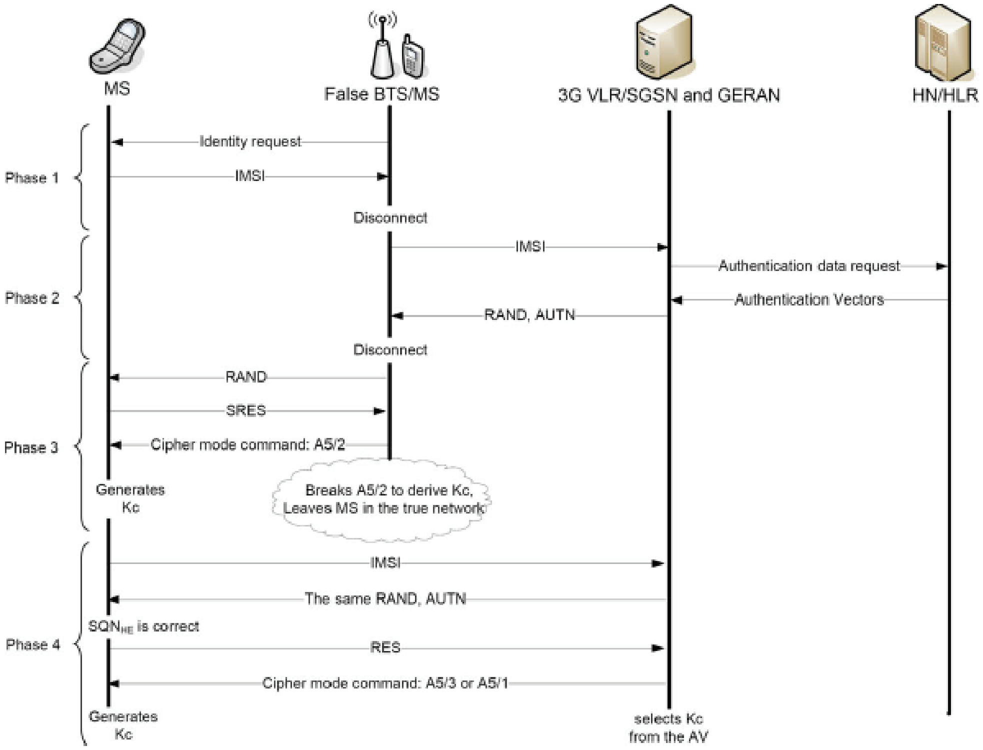

Figure 1: Attack 1-online eavesdropping

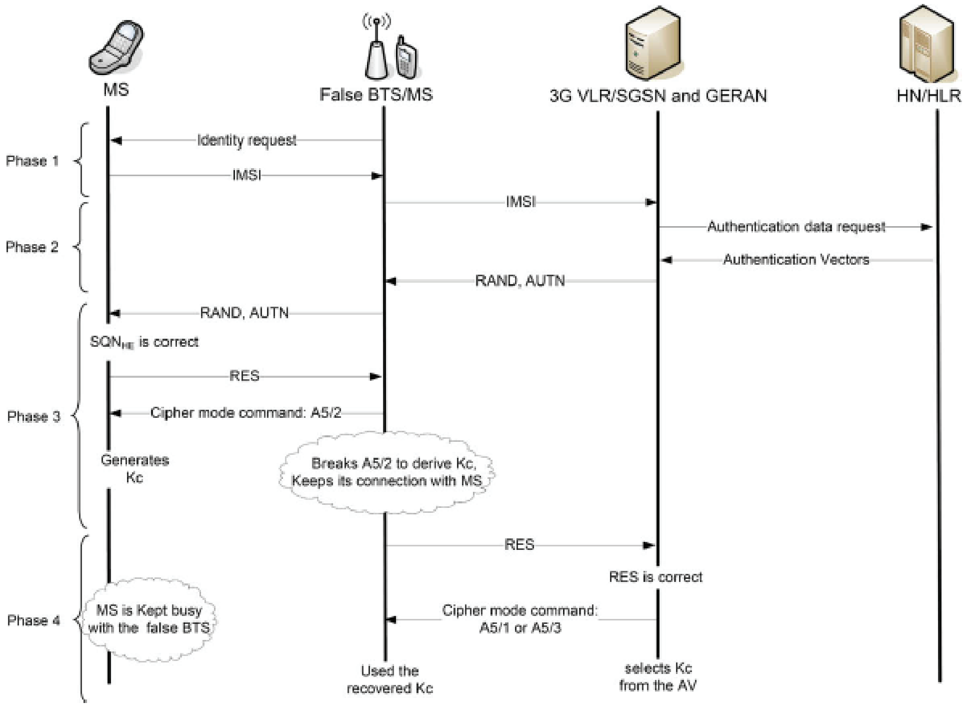

Figure 2: Attack 3-impersonation attack

Erroneous Assumptions

In this section we argue that the previously presented attacks are based on some erroneous assumptions and misconceptions that the authors have made regarding the security functionality of UMTS and GSM networks. More specifically,

ASSUMPTION 1: MS supports the A5/2 encryption algorithm

All the three presented attacks exploit the security weaknesses of the A5/2 encryption algorithm. That is, an adversary that has recorded a few frames of data which is encrypted using A5/2 can derive the session key Kc in under one second. However, a major misconception in [1] is that the mobile equipment of the victim MS supports the A5/2 encryption algorithm. This is an erroneous assumption, since in 2006 the GSM Association prohibited the implementation of the A5/2 algorithm in mobile phones and mandated the use of A5/1 or A5/3 algorithms [2]. Therefore, the three presented attacks cannot be performed, since the attacker cannot mandate MS to use the weak A5/2 security algorithm (i.e., step 1-phase 3 of attack 1, step 2 of attack 2, and step 1-phase 3 of attack 3) in order to obtain the session key Kc of GSM-AKA or UMTS-AKA and use it to perform subsequent malicious actions. Although the security of A5/1 and A5/3 encryption algorithms has been questioned, breaking their security is harder compared to A5/2 in terms of cost, time and complexity.

ASSUMPTION 2: The keys generated between the two steps of attacks 1 and 2 are the same because the same RAND is used.

Another major misconception in [1] lies in the erroneous assumption that the session keys Kc generated in GSM-AKA and in UMTS-AKA are identical, because the same RAND parameter was used for the generation of the session keys. The authors in [1] have overlooked the fact that the session key Kc generated in UMTS-AKA is not derived from the RAND parameter. This observation renders attacks 1 and 2 infeasible.

More specifically, let K_c^{GSM} be the session key generated in GSM-AKA, This key is derived as:

$$K_c^{GSM}\text{=A8(Ki, RAND),}$$

where RAND is an 128-bit nonce generated by the HN/HLR, Ki is the permanent 128-bit key shared between the mobile user and HN/HLR, and A8 is a keyed hash function, which generates a 128-bits output. The last 54 bits of the 128 bits output are appended with 10 zero bits to form the 64-bit session key K_c^{GSM}. On the other hand, in UMTS-AKA, where MS is authenticated via a GSM BTS, a 64-bit session key K_c^{UMTS} is derived using the 128-bit keys CK and IK (generated from HN/HLR) as:

$$K_c^{UMTS}\text{=c3(CK,IK)= CK1}\oplus\text{CK2}\oplus\text{IK1}\oplus\text{IK2,}$$

where CK and IK are each split into CK1, CK2 and IK1 and IK2, respectively, with length 64 bits each, such that CK = CK1||CK2 and IK = IK1||IK2. It is evident that the session keys K_c^{GSM} and K_c^{UMTS} generated in GSM-AKA and UMTS-AKA respectively, are generated from different network parameters, resulting in completely different session keys.

Based on this observation, it can be deduced that attacks 1 and 2 cannot be performed because even if the attacker is able to obtain the key K_c^{GSM} of GSM-AKA (i.e., step 6 of attack 1), it cannot use it to decrypt and eavesdrop on the data exchanged, since it is encrypted using the session key K_c^{UMTS}, generated from UMTS-AKA.

We also mention that the attacks 1 and 2 cannot be performed in case of handovers. In particular, when MS moves to a new network (UMTS or GSM) it has to re-execute the authentication procedure (i.e., UMTS-AKA or GSM-AKA). The re-execution of authentication entails the generation of a new encryption key Kc, which is different from the key used in the old network. Thus, attacks 1 and 2 cannot be mounted in case MS moves from one network to another.

ASSUMPTION 3: MS can always connect to a BTS of GSM regardless of the mobile device's network capabilities

An essential prerequisite to perform the attacks is that the adversary can deceive MS to connect with a false BTS of GSM. However, in case the mobile equipment of the victim MS supports only the UTRAN radio interface [2], (i.e., the mobile equipment is a 3G device and connects only to Node b radio stations of UMTS networks), then none of the above attacks cannot be applied since MS cannot connect with a BTS of GSM .

ASSUMPTION 4: The attacks exploit new security vulnerabilities of UMTS-GSM integrated networks and new security measures must be adopted

The authors erroneously mention that the presented attacks exploit new security weaknesses of UMTS-GSM integrated networks. In fact, the three attacks presented in [1] are mere variations of the well known man-in-the-middle attack in UMTS-GSM integrated networks [3], [4]. 3GPP is aware of this attack and has proposed several possible solutions (e.g., authenticated cipher set command [5], use of special RANDs [6] and key separation [7]), which counteract not only the man-in-the-middle attack of [3], but also all the presented attacks in [1].

References

[1] Z. Ahmadian, S. Salimi, "*Security enhancements against UMTS–GSM interworking attacks*", Computer Networks, Elsevier 2010, doi:10.1016/j.comnet.2010.01.005

[2] 3GPP TS 43.020 (v9.1.0), "*3rd Generation Partnership Project; Technical Specification Group Services and system Aspects; Security related network functions (Release 9)*", Dec 2009.

[3] U. Meyer, S. Wetzel, "*A Man-in-the-Middle Attack on UMTS*", Proceedings of ACM Workshop on Wireless Security (WiSe 2004), Oct. 2004.

[4] 3GPP TSG SA S3-050043, "*Review of recently published papers on GSM and UMTS security*", Sophia Antipolis, France, Feb. 2005

[5] 3GPP SA3 Tdoc S3-040262, "*Analysis of the authenticated GSM command mechanism*", Beijing, China,10–14 May 2004

[6] 3GPP SA3 Tdoc S3-030588, "*Further development of the Special RAND mechanism*", Povoade Varzim, Portugal, 7–10 October 2003

[7] 3GPP TSG SA S3-030463, "*Cipher key separation for A/Gb security enhancements*", San Francisco, USA, 15–18 July 2003

[8] 3GPP TS 35.202 V9.0.0 (2009-12), "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;3G Security Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification (Release 9)"