3GPP TSG SA WG3 Security — S3#26 **S3-020602**
19 - 23 November 2002
Oxford, UK

Source: T-Mobile

Title: Security considerations regarding IMS access with SIM authentication

Document for: Discussion and approval

Date: 2002-11-07

1 Introduction

An LS from SA1 (S3-020601) introduces the new requirement that IMS access shall also be possible using GSM SIMs. UMTS AKA provides enhancements over the GSM AKA, so this requirement probably reduces the IMS security level. This paper analyses possible new threats due to allowing SIM authentication and proposes a way forward to address the new requirement.

2 Threat analysis

Improvements of UMTS AKA to GSM AKA are:

- network authentication
- ensured challenge freshness
- stronger session keys
- (possibly) stronger algorithms

The impact on the IMS environment due to absence of these features in GSM AKA is assessed below.

2.1 Network authentication

UMTS AKA network authentication is twofold: the HN proves its identity by knowing the shared secret and the VN proves that it is trusted by the HN by possessing fresh authentication vectors.

GSM AKA provides sort of weak network authentication when ciphering is active and the VN possesses a valid Kc.

In the IMS, an attacker could try to impersonate different parts of the network:

2.1.1 A1: Impersonating P-CSCF (MITM attack)

For A1, an attacker has to deceive both user and HN. Impersonating a P-CSCF to the HN is not related to the SIM/USIM question. This attack must be countered by NDS in the inter-operator network. Any attacker that receives fresh authentication data from the HN can of course launch a MITM attack. This is not related to using GSM or UMTS AKA.

2.1.2 A2: Impersonating S-CSCF

For A2, an attacker has to deceive both user and VN. The inter-operator network must be compromised, to launch this attack. This should also be countered by NDS.

If there is no NDS, and the attacker does not possess valid authentication data:

With UMTS AKA, the UE will detect a bad HN authentication already in the Auth_Challenge (SM6) message and won't respond with RES (see TS 33.203). Using GSM AKA, P-CSCF will detect an integrity check failure of SM7, and the UE will detect an integrity check failure of SM12 (assuming a suitable conversion function as proposed below). It is possible to elicit a RES out of the UE, however.

Therefore, **even without network authentication AUTN, an attacker can not impersonate the HN** towards the user and the P-CSCF. The mandatory IMS integrity protection prevents this.

If there is no NDS, and the attacker possesses valid authentication data:

An attack is possible (see also section 2.2).

2.1.3 A3: Impersonating P-CSCF, S-CSCF and possibly additional HN servers

In this case, only the user has to be deceived, because there is no connection to the HN. Furthermore, the attacker must also launch a "false RAN" or be able to reach the target UE with IP traffic while utilising a legitimate serving network on PS layer (see also section 4).

If the attacker does not possess valid authentication data:

With UMTS AKA, the UE will detect a bad HN authentication already in the Auth_Challenge (SM6) message and won't respond with RES. Using GSM AKA, the UE will detect an integrity check failure of SM12 (assuming a suitable conversion function as proposed below). It is possible to elicit a RES out of the UE, however.

Therefore, **even without network authentication AUTN, an attacker can not impersonate the HN** towards the user. The mandatory IMS integrity protection prevents this.

If the attacker possess valid authentication data:

An attack is possible (see also section 2.2).

2.2 Challenge freshness

If an attacker gets hold of SIM authentication triplets or AKA authentication vectors, he can impersonate the HN. With AKA, however, the usability of the AVs is limited due to the sequence number checking. SIM triplets remain usable for an unlimited time. As pointed out in [1], an attacker can get valid triplets with access to the SIM or to the inter-operator network. To minimise this threat, NDS should be applied to both MAP and IP infrastructure.

2.3 Session keys

GSM AKA provides only a 64 bit key (possibly fewer effective bits), whereas UMTS AKA provides two 128 bit keys, which are needed in IMS. If GSM AKA is used, a key expansion function is required. Similar to EAP-SIM [1], the IMS keys could be generated from multiple GSM AKA runs to provide adequate strength against key searches.

2.4 Algorithms

Some GSM authentication algorithms have known weaknesses, which can be used to find the secret Ki. Together with a lack of network authentication, this could be used for remote Ki breaking attacks. However, known attacks are not possible because they require both RES and Kc knowledge. Some SIMs have an internal limit of total AKA runs allowed, which could be driven to the limit resulting in a SIM DoS.

The decision which algorithms are still acceptable for IMS and which are not should be up to the HN operator.

2.5 Old threats revisited

The false BTS attack analyses in SMG10 [2], [3] pointed out the following threats due to the missing network authentication in GSM:

1. denial of service
2. eavesdropping by bidding-down or forced usage of old keys
3. fraudulent call setup under the target's subscription
4. spoofed call setup to the target
5. spoofed call answering

The identity catching attack also mentioned in the analyses is not discussed here. It is not related to the SIM or UMTS AKA question because a P-CSCF must always be able to request a UE's IMPI to find its home domain.

A false BTS attack is possible without knowing valid authentication data, but a false IMS attack requires valid authentication data *for the particular target* SIM. If an attacker owns authentication data, he can succeed with attacks A2 and A3, possibly causing effects 1., 2., 4., and 5. A3 (network impersonation towards the user) seems to be the most probable attack. To achieve effects 2., 4., and 5., the attacker must combine A3 with a UE functionality towards the real network. The attacker must use his own identity to pass through MOCs, which will be detected by the B-party.

It is not possible for the attacker to impersonate the victim towards the real network, because he does not know the integrity key related to the fresh HN challenge. Thus effect 3. can not be achieved.

3 Mapping GSM AKA to Digest-AKA

Entities involved in IMS authentication are (U)SIM, UE, P-CSCF, I-CSCF, S-CSCF, HSS. Changes due to introduction of SIM authentication must be minimised. It is proposed to map GSM AKA to IMS AKA (including Digest-AKA [4]) using conversion functions within UE and S-CSCF. All other NE can remain unchanged.

Alternative 1: Conversion functions as in RAN access (TS 33.102).

CK = Kc || Kc

IK = Kc1 xor Kc2 || Kc || Kc1 xor Kc2 with Kci 32 bits long and Kc= Kc1 || Kc2

aka-version = "AKAv2"

AUTN = 0

$RAND_{IMS} = RAND_{GSM}$

Alternative 2: Conversion functions over n triplets

with Kc_i, $RANDi_{GSM}$, RESi related to GSM AKA run i:

CK = SHA1(Kc_1 || Kc_2 || .. || Kc_n), truncated to 128 bits

IK = SHA1(Kc_n || Kc_{n-1} || .. || Kc_1), truncated to 128 bits

aka-version = "AKAv2"

AUTN = 0

$RAND_{IMS} = RAND1_{GSM}$

server specific data = ($RAND2_{GSM}$ || ... || $RANDn_{GSM}$)

DigestPasswd = (RES1 || RES2 || .. || RESn)

Optional for both alternatives:

AUTN = SHA1(RAND || Kc), truncated to 128 bits

As discussed above, IMS authentication will fail if the network does not know the correct Kc related to the challenge issued. Therefore, it might not be necessary to generate an AUTN for SIM AKA use. The only benefit of doing so would be a protection of the UE against sending RES to a false network, thus countering brute force attacks.

4 Practical considerations

4.1 Network infrastructure

Above considerations focused on theoretically possible threats, not taking into account the underlying IP network structure. In many cases theoretical attacks are impractical because they can not reach their target or at least require additional attacks against the IP infrastructure. Therefore, operators should take care to tighten their configuration by strict filtering in order to close potential paths for attacks. Furthermore, above considerations only took SIP traffic into account. To launch a real MITM attack, also the session data must be intercepted.

Possible attacker locations[1] can be classified in three categories:

1. Internet
2. 3G subscriber connected via GRX
3. 3G subscriber in the same serving GPRS network

To counter SIP-based attacks, the operator must take all attacker locations into account.

Countermeasures for each location category should include:

1. Traffic filtering
2. Inter-operator NDS/IP and traffic filtering "inside the tunnels"
3. Check of link-layer forwarding, which may bypass filters

These countermeasures are also necessary when using UMTS AKA, because attacks my not only be related to the authentication.

4.2 UE implementation

Practical security requirements for UE implementations are still undefined. Some measures can be identified from above considerations.

Most probably, "open" SIP clients will be available which can optionally bypass the IMS to directly inter-operate with SIP entities outside the IMS. Therefore, it is important to indicate to the SIP client whether a message was received integrity protected (through IPSec) or unprotected (through plain IP). Furthermore, it is important to indicate whether a SIP message was received through the dedicated IMS APN or, for example, through the Internet APN. The UE should provide traffic filtering means according to these indications – independent from USIM or SIM authentication.

To counter brute-force attacks against the SIM through multiple authentication requests it may make sense to limit the response rate on authentication requests within the UE.

[1] Attacks originating within an operator's environment are out of scope here because they must be covered by NDS or by physical security.

5 Summary and Proposal

It has been shown that the mandatory integrity protection of IMS signalling provides a major difference between using GSM AKA for IMS or for RAN access. A false BTS attack can be launched without knowledge of authentication data, which is not possible in the IMS case. Even though GSM authentication triplets remain valid forever, an attacker has to get triplets for his target in the first place. So there is still at least one more step to launch successful IMS attacks when compared to false BTS attacks – which aren't common, either. Using the GMS AKA for IMS authentication does not introduce significant new security holes.

GSM AKA can be mapped onto IMS AKA with minimal changes. It is proposed to decide on one of the alternatives in section three and to adapt IMS AKA accordingly.

References

[1] H. Haverinen, J. Salowey, "EAP SIM Authentication" draft-haverinen-pppext-eap-sim-06.txt, IETF, October 2002.

[2] "Addressing the false BTS problem in UMTS", Vodafone, SMG10 tdoc, Oct. 1998

[3] "Countermeasures on the false BTS threats", Siemens, SMG10 tdoc, Nov. 1998

[4] A. Niemi, J. Arkko, V. Torvinen, "HTTP Digest Authentication Using AKA", RFC 3310, IETF, Sept. 2002