3GPP TSG SA WG3 Security — S3#32 **S3-040110**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item: **6.10 (WLAN)**

Source: **Siemens**

Title: **Comments on S3-040009 and S3-040100 on measures for separation of domains**

Document for: **Discussion and decision**

Comparison of measures in S3-040009 and S3-040100 to separate domains

S3-040009 discusses various countermeasures which prevent that a security breach in one domain (e.g. GSM/GPRS) spills over into another domain (e.g. WLAN).

Countermeasure 3: section 3.3 of S3-040009 proposes to use separate ranges of RAND for each access network type (which is an extension of the "special RAND" proposal). Please note that the special RAND proposal has so far only been formulated for GSM, but could be easily extended to UMTS for the purposes of domain separation. S3-040100 elaborates on this proposal (and the earlier proposal in S3-030733).

Countermeasure 4: section 3.4 of S3-040009 proposes to use an appropriate functionality split of EAP-AKA and EAP-SIM over UE devices, using one of the alternatives discussed in S3-030747.

We show here that these two countermeasures are not equivalent. It is not possible to substitute one for the other, and, in order to achieve full protection, both have to be implemented.

Case EAP-SIM: the use of separate ranges of RAND does prevent that a security breach in GSM affects WLAN access. However, in the opposite direction, it provides lower security than an appropriate functionality split of EAP-SIM, as is shown in the following.

Assume first that countermeasure 4 is not implemented and therefore the functionality split is according to the weak alternative 1 in S3-030747, i.e. the MT returns SRES and Kc to the WLAN-TE. Assume furthermore that countermeasure 3 is implemented, i.e. the HSS issues special RANDs, which may be used only for WLAN access, and the Rel6 compliant MT gives SRES and Kc only to a WLAN-TE if the RAND is special for WLAN access.

Then a TE (laptop) may obtain (RAND, SRES, Kc) from the MT, where the RAND is special for WLAN access. When the TE (laptop) is compromised at a certain point in time an attacker may get hold of a certain number of these triplets. The attacker may then use these triplets later at any point in time during the lifetime of the SIM to perform one of the following two attacks:

1) the attacker may impersonate a 3G-AAA server terminating EAP-SIM, and hence, in particular, a WLAN access network towards the user;

2) assume that the user, at one point in time, inserts the SIM in a pre-Rel6 MT which does not implement the special RAND mechanism. E.g. the pre-Rel6 MT could be a user's regular phone, and the Rel6 MT with special RAND implemented could have been a rental phone. There will be plenty of pre-Rel6 MTs, especially for GSM and GPRS access, for a long time to come. Then the attacker can perform a false base station attack against this MT, even when encryption is switched on (so that the ciphering indicator does not provide protection), as the pre-Rel6 MT accepts the special RAND originally issued for WLAN access only.

Assume now that countermeasure 4 is also implemented and that the MT returns only the MK or the MSK to a WLAN-TE. Then none of the two above attacks is possible any more.

Re 1): the possession of MK or MSK is not enough for an attacker to impersonate a 3G-AAA server because, for each new run of an EAP-SIM full authentication, a new MK, and hence a new MSK, is derived from several keys Kc and a nonce generated by the WLAN-TE.

Re 2): an MK or an MSK is not useful for GSM or GPRS access.

Case EAP-AKA: assume that countermeasure 3 is implemented, but not countermeasure 4, i.e. the MT returns RES, CK and IK to the WLAN-TE if the RAND was issued for WLAN access. It appears that the special RAND mechanism ensures indeed the separation of domains in UMTS, i.e. a compromise of the TE does not affect non-WLAN domains in UMTS, and that an EAP-AKA server cannot be impersonated. This is due to the fact that the USIM prevents a re-use of quintuplets. **However**, any UMTS quintuplet (even if used already) may be converted into a valid GSM triplet (cf. TS 33.102, section 6.8), and the USIM may be inserted into a pre-Rel6 MT, which does not implement the special RAND mechanism, for GSM access. Then attack 2) above is possible. Therefore countermeasure 4 is also needed for EAP-AKA. Attack 1) above does not seem to be relevant, as there is no reason why EAP-SIM should be run for a UMTS user.

Conclusion

This contribution has shown the following:

- The special RAND mechanism is required to prevent a GSM security breach (e.g. through an attack on A5/2) to affect the 3G-WLAN access.
- When a split UE is used and the WLAN-TE is considered more vulnerable than the MT, then an appropriate functionality split of EAP-SIM and EAP-AKA shall be used such that MK or MSK, but not the GSM and UMTS session keys Kc, CK, IK are given to the WLAN-TE. This is to prevent false base station attacks on pre-Rel6 mobiles and impersonation of EAP-SIM servers.

References

[S3-040009] BT, " Protecting GSM/GPRS networks from attacks from compromised WLAN networks when interworking"

[S3-040100] Nokia, "Using Special RANDs to separate WLAN and GSM/GPRS"