3GPP TSG SA WG3 Security — S3#25 **S3-020544**

8 - 11 October 2002

Munich, Germany

Source: **Siemens**

Title: **On the security of EAP/SIM and EAP/AKA and their use in WLAN-3G-interworking**

Document for: **Discussion**

Agenda Item: **7.9**

Abstract

The EAP/SIM and EAP/AKA protocols have been proposed for use in WLAN-3G-interworking as authentication and key agreement protocols. The basic difference in the security of these protocols is that, while both EAP/SIM and EAP/AKA provide mutual authentication, the network-to-user authentication of EAP/SIM is based on the derived key Kc which carries a comparatively higher risk of being exposed whereas the network-to-user authentication of EAP/AKA is based on the permanent key K which enjoys strong protection. The threats resulting from this property of EAP/SIM are well known and described in the EAP/SIM draft [1, section 21]. EAP/SIM security could be increased by minimising the exposure of pairs (RAND, Kc). However, some of these measures may make it more difficult to leverage the existing authentication infrastructure. It is concluded that EAP/AKA should be preferred over EAP/SIM.

---

1. Introduction

The two protocols under discussion, EAP/SIM and EAP/AKA, are specified in [1] and [2]. Section 21 of [1] on "Security considerations" provides a good summary of threats relevant for the use of EAP/SIM in 3G-WLAN interworking, cf. also S3-020511. The draft TS on WLAN-3G-interworking security [3] shows how these protocols could be used in a WLAN-3G-interworking context, cf. S3-020522.

2. Discussion

2.1 Keys used for network-to-user authentication in EAP/AKA and in EAP/SIM

This subsection summarises well-known properties of EAP/AKA and EAP/SIM for the benefit of the reader:

The cryptographic security of the EAP/AKA-protocol is basically the same as that of the AKA protocol. In particular, the network-to-user authentication is provided by the use of a signed challenge and a sequence number mechanism for replay protection. The AuC computes a MAC over the challenge RAND and the sequence number. This MAC and the sequence number are verified by the USIM. The important aspect to note here is that the computation of the MAC is based on the long-term secret K which is stored only in the USIM and in the Authentication Centre AuC, both of which are particularly well protected. The network thus proves possession of the long-term secret K to the user.

On the other hand, the EAP/SIM protocol provides considerable enhancements to the standard GSM authentication and key agreement protocol: the length of the session keys produced by EAP/SIM is no longer restricted to 64 bits, and network-to-user authentication is provided. However, the MAC used to provide network-to-user authentication is computed over the client challenge, the network challenges RAND and the cipher keys Kc correponding to the

challenges RAND (there may be several to make longer session keys possible). Thus, the network only proves possession of the short-term secrets Kc to the user.

2.2 Risk of exposure of (RAND, Kc)

Kc may be exposed in several ways:

In the WLAN-3G-interworking architecture:

- An attacker could gain access to the 3GPP AAA server: the AAA server should be very well protected, so that the risk here should be small. Also, it has been decided that the 3GPP AAA server always resides in the home network so that issues of trust between the home and the visited network do not arise.
- An attacker could gain access to the communication between the AuC and the 3GPP AAA server: also this communication should be well protected, using the mechanisms provided by NDS.
- An attacker could gain access to the terminal, e.g. by means of a Trojan horse: this seems a non-negligible risk.

In the GSM architecture:

It is perfectly feasible from a technical point of view to use the same SIM card (or SIM application on a UICC) for GSM access on the one hand and for WLAN access using EAP/SIM on the other hand. If this is the case, then the well-known threats to Kc in GSM also apply.

2.3 Threats arising from the exposure of (RAND, Kc)

The following threats have already been noted in [1, section 21]. The may reduce the security of EAP/SIM to that of GSM.

Using obtained pairs (RAND, Kc), an attacker could impersonate the network and perform a “false AP” attack. In particular, an attacker could play man-in-the-middle and eavesdrop on the user’s communication. (The attacker could not, though, impersonate a user or hijack bandwidth). If the same long-term key Ki was also used for GSM access then, if an attacker managed to obtain Kc by breaking GSM encryption, the advantage of longer keys in EAP/SIM would also go away as the attacker could combine several obtained Kcs to perform the above eavesdropping attack.

It should be noted here that pairs (RAND, Kc) once obtained by an attacker remain good for an attack as long as the permanent key Ki remains the same, and that could be for years.

2.4 Possible countermeasures

The security of EAP/SIM can be increased by minimising the exposure of Kc. In particular:

- Countermeasure: different permanent keys Ki could be used for access to GSM and for WLAN access using EAP/SIM. This would help against attacks on the GSM encryption algorithm or eavesdropping on GSM-internal interfaces, e.g. the BTS-BSC radio link.
  Drawback: this would mean that a different key database would have to be set up in the AuC for WLAN access. This would imply issuing new UICC cards with new SIM applications to the users.
- Countermeasure: the computation of AT_MAC could be performed in the SIM so that Kc does not leave the SIM card when used in EAP/SIM, cf. also [4]. This would help against attacks on or from the terminal.
  Drawback: this would mean that a new WLAN-SIM application would have to be developed. It would necessitate issuing new UICC cards to the users.

2.5 The use of EAP/AKA

There seem to be no security problems associated with the use of the same USIM with the same permanent key K for both, UTRAN access using AKA and WLAN access using EAP/AKA. However, an independent USIM for WLAN access is also possible. The dicussion of the pros and cons of these two approaches appears to be similar to the discussion relating to the ISIM when using AKA for access to the IMS.

Conclusions

1. If it is the objective to reach a security level for WLAN-3G interworking which is comparable to GSM then the use of EAP/SIM without additional precautions seems fine. This objective would, however, contradict a security requirement in [3] that " The user should have same security level for WLAN access as for 3GPP access". But note, that the security requirements section in [3] may need some revision as there seem to be contradictory requirements.

2. Measures to increase the security level of EAP/SIM over that of GSM are technically possible, but the benefits have to be carefully weighed against the drawback that they seem to make it more difficult to leverage the existing authentication infrastructure. The use of EAP/AKA seems to make it possible to use the existing infrastructure.

3. The use of EAP/AKA seems preferable over the use of EAP/SIM.

References

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

[2] J. Arkko, H. Haverinen, "EAP AKA Authentication", draft-arkko-pppext-eap-aka-05.txt, IETF, October 2002.

[3] Draft 3G TS 33.cde v0.1.0, "Wireless Local Area Network (WLAN) Interworking Security", S3-020522, October 2002.

[4] "Use of smart cards in WLAN interworking", Gemplus, 3GPP S3-020518, October 2002.