3GPP TSG SA WG3 Security#31 **S3-030747**
18-21 November, 2003
Munich, Germany

Agenda Item: **6.10 (WLAN)**

Source: **Siemens**

Title: **Pseudo-CR to TS 33.234 on Requirements on UE split**

Document for: **Discussion and decision**

Abstract

TS 33.234 v070 (S3-030xxx) contains an editor's note regarding the termination point of EAP-AKA and EAP-SIM respectively in a WLAN_UE functional split scenario. This contribution proposes to include a related requirement into TS 33.234 (WLAN security). A threat scenario is given to motivate the proposal.

1. Security aspects of termination points of EAP-AKA and EAP-SIM

The following familiar figure depicts a WLAN_UE functional split scenario:

The mobile phone (the "card holding device") on the left holds the UICC or SIM (the "card") and the laptop holds the functions for WLAN access (the "WLAN access device"). The network is not aware of the UE functional split. Typically the card holding device also has a network interface (although not necessarily WLAN interface) , e.g. a GSM or UTRAN interface.

The specifications of EAP-AKA [eapaka] and EAP-SIM [eapsim] only know an EAP "peer" whose functions have to be performed by the UE, i.e. card holding device, WLAN access device and card combined. It is discussed in this contribution how the functionality of the EAP peer should be distributed over the physical devices which make up the UE.

Alternative 1: all functions of an EAP peer are executed on the WLAN access device, with the exception of the functions executed by the SIM or USIM, which are defined in GSM 03.20 and 3G TS 33.102 (i.e. basically the cryptographic algorithms A3/A8 and f1-f5 respectively). The card holding device only transfers data between the WLAN access device and the card transparently. This implies in particular that the WLAN access device receives the GSM or UMTS session keys Kc or CK, IK.

Evaluation: Alternative 1 seems the straightforward approach. However, it has a serious security drawback, which is already mentioned in draft TR " on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces" (S3-030666). Section 5.2.1 of S3-030666 states:

> "Now when (U)SIM is being used directly or re-used to authenticate open mobile platforms like Laptop PCs and PDAs, the protection of these parameters *[i.e. authentication parameters and session keys]* become even more

necessary as the likelihood of threats are much higher. This especially true when 3GPP is considering the SIM and USIM based authentication for WLAN terminals."

This means: if an attacker mounts a successful attack on the WLAN access device he can get hold of the GSM or UMTS session keys. With these keys, he can perform attacks not only on the WLAN access, but also on other domains in GSM or UMTS, e.g. the CS or PS domain. The attacks, which become possible when the attacker is in possession of the session keys, are well-known. They include false base station attacks, eavesdropping and user impersonation.

This leads to the following **security requirement**:
The UE functional split shall be such that attacking the CS or PS domain by compromising the WLAN access device is at least as difficult as attacking the CS or PS domain by compromising the card holding device.

Remark: the requirement is stated in this way because it is acknowledged that there may be situations where the risk of compromise of the WLAN access device is similar to that of the card holding device. In such a situation it would make no difference whether the WLAN access device knows the GSM or UMTS session keys. In the general situation, however, it may make sense to prevent that the WLAN access device knows the GSM or UMTS session keys. The security requirement is satisfied if, in particular, the WLAN access device is not able to infer the GSM or UMTS session keys from the information it receives.

Alternative 2: all functions of an EAP peer are executed on the card holding device, with the exception of the functions executed by the SIM or USIM as specified in GSM 03.20 and 3G TS 33.102. The WLAN access device only transfers data between the card holding device and the network transparently.

Evaluation: in alternative 2, the WLAN access device cannot get hold of the GSM or UMTS session keys, and the above security requirement is fulfilled. But there may be performance disadvantages. Often, the card holding device is much less powerful than the WLAN access device, and therefore it would be better from a performance point of view that as many functions of an EAP peer as still compatible with the above security requirement are executed on the WLAN access device.

Alternative 3: the card holding device computes the master key for EAP-SIM and EAP-AKA from the GSM and UMTS session keys, the remaining functions of an EAP peer outside the card are executed in the WLAN access device.

I.e. the card holding device computes

MK = SHA1(Identity|IK|CK) for EAP-AKA , cf. [eapaka, section 4.5] and

*MK = SHA1(Identity|n*Kc| NONCE_MT| Version List| Selected Version*) for EAP-SIM, cf. [eapsim, section 4.6].

The card holding device then forwards the *MK* to the WLAN access device.

Evaluation: the security requirement is fulfilled, and the card holding device performs only the minimum of functions required so that the WLAN access device is not able to infer the GSM or UMTS session keys from the information it receives.

Further alternatives: of course, any alternative where the function split between card holding device and the WLAN access device is in between alternatives 2 and 3, also fulfils the above security requirement. Depending on the relative capabilities of the two devices, the precise split between the two devices may or may not be of particular relevance.

Enhanced role of the card: more functions could be performed on the card. But there seems to be no obvious security advantage compared with performing the functions on the card holding device, if the latter obtains the GSM and UMTS session keys for access to GSM and UMTS anyhow.

2. Proposal

Based on the evaluation in section 1, it is proposed to make the following change to section 4.2.4.1 of TS 33.234 v070. The changes can be seen from the revision marks.

*********BEGIN OF CHANGE*********

4.2.4 WLAN-UE Functional Split

4.2.4.1 General

In the case when the WLAN-UE, equipped with a UICC (or SIM card), for accessing the WLAN interworking service, is functionally split over several physical devices, one device holding the card, and one device providing the WLAN access, that communicate over local interfaces e.g. Bluetooth, IR or serial cable interface, then is shall be:

- Possible to re-use existing UICC and GSM SIM cards; and
- The UE functional split shall be such that attacking the CS or PS domain of GSM or UMTS by compromising the device providing the WLAN access is at least as difficult as attacking the CS or PS domain by compromising the card holding device.

Note: The requirement is fulfilled if the master keys for EAP-AKA and EAP-SIM, as specified in [4] and [5], are computed either on the card or in the card holding device.

[Editor's note: The termination point of EAP is for further study e.g. if EAP-AKA and EAP-SIM shall terminate in the TE e.g. laptop computer. The decision on the termination point shall take into account the requirements in this subsection.}.

*********END OF CHANGE*********

References

[eapaka] J. Arkko, H. Haverinen, „EAP AKA Authentication", Internet Draft, draft-arkko-pppext-eap-aka-11, October 2003. http://www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-11.txt

[eapsim] H. Haverinen, J. Salowey „EAP SIM Authentication", Internet Draft, draft-haverinen-pppext-eap-sim-12, October 2003. http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-12.txt