3GPP TSG SA WG3 Security — SA3#25 **S3-020557**

8 - 11 October 2002

Munich, Germany

Source: Nokia, Ericsson

Title: On the use of EAP/SIM in 3G-WLAN-interworking

Document for: Discussion

Agenda Item: 7.9

1 Background

EAP-SIM is the current working assumption in 3GPP to provide authentication and key management in the 3G-WLAN interworking system for users equipped with a SIM card.

The EAP-SIM draft describes some potential threats derived from the fact that keying material is derived and checked in the EAP client, which may reside in an open SW environment (instead of in the UICC or SIM card)

Possible countermeasures identified in [S3-02Sie WLAN EAP-SIM] include modifications to existing SIM cards such as storing separate Ki for WLAN or performing the computation of AT-MAC in the SIM card.

It's worth noting that IEEE have already indicated in the 802.11i WG discussions that EAP-AKA in GSM compatible mode is not acceptable due to the lack of network authentication.

In addition, a exisiting security requirement in 3GPP states that" The user should have same security level for WLAN access as for 3GPP access", which is in contradiction with the security level provided by EAP-SIM.

2 Discussion

The USIM application and UMTS AKA have been designed for performing network authentication on the smart card and for fixing other weaknesses in GSM AKA.

EAP AKA in UMTS mode seems to provide an appropriate level of security even if the same subscription was re-used in WLAN. Having a separate USIM application for WLAN could be considered as an additional security enhancement, but this needs further discussions in SA3.

The existing and soon to be deployed USIM application should be preferred over any new improvements to GSM SIM application.

One of the requirements in current the 3G-WLAN interworking TS is that existing UICC cards should be supported and the solution should not require any new changes to the UICC. Hence we would prefer solutions that do not require any new WLAN authentication applications on the UICC but that work with the existing SIM or USIM application.

However if the USIM application is not sufficient, and a new WLAN authentication application is anyway required, then the WLAN authentication application should not be based on the GSM SIM application but rather it should be based on an authentication method that natively supports mutual authentication and strong session key generation, such as UMTS AKA.

Anyway an interim solution for existing GSM subscribers is needed.

Existing GSM functions can be re-used in a reasonably secure way, as shown in the EAP-SIM draft. The level of security on Wireless LAN with EAP SIM is better than in GSM due to the EAP SIM network authentication support and key generation improvements, but however the mechanism is not as secure as 3GPP access or UMTS AKA.

We consider EAP SIM as a good intermediate solution whose biggest benefit is that it doesn't require new smart cards. Any "enhanced" GSM SIM solution that doesn't work with existing cards isn't worthwhile because of the reasons stated above. EAP SIM can be used before the USIM based solution, which does require new smart cards, is available.

3 Proposal

We propose changing the security input requirements in TS 33.cde as follows:

***** Modified text *****

4.2 Security Requirements

[Editor's note: These requirements are copied from TS 23.xxx v0.1.0 for the first version of this TR, and shall be reviewed and updated according to the input from the preceding sections]

- Legacy WLAN terminals should be supported.
- Minimal impact on the user equipment, i.e. client software.
- The need for operators to administer and maintain end user SW should be minimized
- Existing UICC cards should be supported. The solution as such should not require any new changes to the UICC cards.
- Changes in the HSS/HLR/AuC should be minimized.
- The security data, i.e. long-term keys, which are stored on the UICCcard must not be sent from the card itself. Instead the interface to the UICC card should be of type challenge-response, i.e. a challenge is sent to the UICC card and a response is received in return.
- The user should have at least the same security level for WLAN access as for his current mobile subcription (i.e. GSM or UMTS)~~The user should have same security level for WLAN access as for 3GPP access.~~
- Mutual Authentication ~~should~~ shall be supported for GSM and UMTS subscribers
- The selected Authentication solution should also allow for Authorisation
- Methods for key distribution to the WLAN access NW shall be supported
- For UMTS subscribers, ~~S~~the selected WLAN authentication mechanisms for 3GPP interworking shall provide at least the same security as 3GPP System authentication procedure. For GSM subscribers, the selected WLAN authentication mechanisms for 3GPP interworking shall provide at least the same security as the GSM system authentication procedure
- Subsequent WLAN re-authentication shall not compromise the requirement for 3GPP/GSM System equivalent security
- Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material.
- Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks. In other words, a man in the middle shall not be able to learn the session key material.
- The WLAN technology specific connection between the WLAN UE and WLAN AN shall be able to utilise the generated keying material for protecting the integrity of an authenticated connection
- It shall be possible to store all long-term security credentials used for subscriber and network authentication in a tamper resistant memory such as the UICC card.