3GPP TSG SA WG3 Security — S3#33 **S3-040351**
10 - 14 May 2004
Beijing, China

Source: **Gemplus**

Title: **WLAN application**

Document for: **Discussion and decision**

Agenda Item:

Abstract

This contribution proposes the use of a WLAN application to solve WLAN security issues.

1. Introduction

At SA3#31 and SA3#32 meetings some concern was expressed that the security breach in one domain could spill over into another domain. E.g. the A5/2 vulnerability can spread from the GSM network to the WLAN access network or end user devices can spread from the WLAN network to the GSM network. SA3#32 contributions discussed various countermeasures to prevent such security issues. This contribution proposes the use of a WLAN application as solution.

2. WLAN security

At SA3#32, the following contributions discussed countermeasures to prevent spreading of vulnerabilities between WLAN and GSM.

- **S3-040009** [1] proposes 4 countermeasures:
  - *Countermeasure 1*: Segregated HSS and UICC applications
  - *Countermeasure 2*: Key separation function in HSS
  - *Countermeasure 3*: the use of separate range of RAND for each access network type
    This countermeasure is associated with the assumption that "we have a device that can be trusted to interpret the information correctly i.e. a traditional GSM/GPRS 3G PS and CS mobile phone issued by the Home Network Operator".
  - *Countermeasure 4*: Appropriate functionality split of EAP-AKA and EAP-SIM over UE devices

- **S3-040100** [2] proposes to use Special RANDs to separate WLAN and GSM/GPRS domains

- **S3-040110** [3]

This contribution comments S3-040009 and S3-040100 and states that *"countermeasures 3 and 4 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"*.
The conclusion analyses EAP-SIM and EAP-AKA cases and concludes that:

- *The Special RAND mechanism is required to prevent a GSM security breach 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-Rel-6 mobiles and impersonation of EAP-SIM server.*

3. WLAN application

The use of a WLAN application was already proposed and discussed to solve the risks of using a legacy SIM card for WLAN interworking in case of EAP-SIM (Cf S3-020651 SA3#26 meeting). After that, vulnerabilities due to A5/2 attacks have been identified.

The use of an independent WLAN application allows separating GSM/GPRS and WLAN domains, the session keys Kc, CK and IK never leave the UICC. So, a WLAN application prevents all the security attacks identified in S3-030110 contribution [3], it is an alternative to the combination of countermeasures 3 and 4, which are based on Special RAND and functional split of EAP-SIM/AKA.

Special RAND

The Special RAND is a ME-based mechanism; the UICC is not involved in the decision to perform the authentication command according to the Special RAND value sent by the Home Network. The Special RAND mechanism assumes the use of a trusted device (cf assumption of countermeasure 3 [1]). So, in case of ME not implementing the Special RAND mechanism or a hacked ME then there is no separation of domains. The Home Network has no guarantee of the interpretation of the Special RAND by the ME since the HN has no information on the ME capability of the user's UE.
In case of usage of a WLAN application, the Home Network knows if a WLAN application is present on the user's UE since the HN knows the capabilities of the UICC. The Home Network controls the level of security associated to WLAN access request.

Split UE

With WLAN application the session keys Kc, CK or IK are always protected whatever the type of split UE since these session keys never leave the UICC.

Sharing security functions and data with USIM

The WLAN application may share security functions and data with the USIM, different options of sharing could be proposed. Options have already been specified for ISIM in TS 33.203 [4].
These options of sharing allow dealing with different business models. E.g. of business models [1]

- The WLAN access network operator and GPRS operator are separate companies
- 3G WLAN interworking is used to ensure that the users use their subscription (and USIM) to get access also over WLAN, in this way bind users to one operator.

So, the WLAN application offers a higher level of security to prevent attacks. An open issue could be the availability of the WLAN application. This point is developed in the following section.

4. Standardization of WLAN application

The WLAN Smart Card Consortium (WSCC) specified WLAN SIM application and ETSI SCP proposes EAP support on UICC. The WLAN-SIM application is in line with the initiative support of EAP for Smart Cards currently in progress in ETSI SCP.

WLAN-SIM

The WLAN Smart Card Consortium took on the work of specifying an interoperable solution to integrate a smart card in the EAP framework used for authentication. While their goal is to run EAP

inside the card, they felt the need to satisfy an intermediate requirement of mobile network operators currently deploying I-WLAN on GSM. Therefore they specified the WLAN-SIM.

Features of the WLAN SIM:

- Shall be compatible with EAP-SIM
- Shall protect the A3A8 algorithm by executing the EAP-SIM specific cryptographic calculations in the UICC
- Does not expose SIM specific data (IMSI, ADN, PLMN…) to malicious programs in the WLAN terminal
- Shall determine when to use Pseudonym instead of IMSI
- Shall derive and store EAP authentication key and WPA-Session key in UICC: protection of the WLAN session against hijacking.
- Shall be independent from SIM, to possibly separate the I-WLAN subscription credentials from GSM and GPRS
- Shall allow re-use of the credentials from the SIM on the same UICC
- Shall be optional
- Shall be standard
- Shall not have a big impact on terminal software

Advantages of the WLAN SIM:

- Already specified and agreed by a large number of industry players
- Can be adopted by 3GPP in Rel-6 timeframe
- Can be developed on existing UICC
- Does not need to modify the SIM (specs are frozen)
- Compatible with the EAP support in UICC initiative currently in progress in SCP, as every EAP method can be implemented as an independent application. EAP support in UICC naturally integrates the WLAN-SIM in the overall.

So, the standardization of a WLAN application is possible in Rel-6 timeframe.

5. Conclusion

The use of a WLAN application offers a higher security level to prevent attacks on vulnerability spreading between WLAN and GSM/GPRS domains. The standardization of a WLAN application is not an issue.

We kindly recommend SA3 to adopt WLAN solution and send a LS to T3 to ask them to work on WLAN application.

6. References

[1] TD S3-040009, “Protecting GSM/GPRS networks from attacks form compromised from compromised WLAN networks when interworking”, BT Group

[2] TD S3-040100, “Using special RAN to separate WLAN and GSM/GPRS”, Nokia.

[3] TD S3-040110, “Comments on S3-040009 and S3-040100 on countermeasures for separation of domains”, Siemens.

[4] TD 33.234, “Wireless Local Area Network (WLAN) interworking security” v6.0.0