3GPP TSG SA WG3 Security – S3#26 **S3-020650**

19 - 22 November 2002

Oxford, UK

Source: **GEMPLUS Card International**

Title: **Need for a WLAN specific UICC application**

Document for: **Discussion and approval**

Agenda Item: **T.B.D**

Abstract

This input papers aims at requiring the use of a WLAN specific UICC application for 3G-WLAN interworking.

1. Introduction

At SA3#25 Munich meeting, Gemplus submitted a contribution proposing the definition of a WLAN specific UICC application in the scope of the 3G-WLAN interworking. The aim of this new input paper is to present additional security reasons explaining the need of a WLAN specific UICC application.

This discussion is based on EAP/AKA procedure described in Internet Draft-arkko-pppext-eap-aka-05 “EAP AKA Authentication”.

2. EAP/AKA with the use of USIM

In the USIM-based authentication with EAP/AKA procedure, the USIM is used in the following way:

- The terminal runs the UMTS AKA algorithm on the USIM
- The USIM
    - Verifies that AUTN is correct and hereby authenticates the network.
    - If AUTN is incorrect, the terminal rejects the authentication. If the sequence number is out of synchronization, terminal initiates a synchronization procedure.
    - If AUTN is correct, the USIM computes RES, IK, CK and provides those values to the terminal
- The terminal
    - Derives new required keying material from CK and IK
    - Decrypts the new temporary identifier and saves it to be used on next authentication
    - Sends EAP Response/AKA-challenge containing RES to WLAN

2.1. Description of keying material derivation

The required keying material derivation is based on a FIPS 186-2 pseudo-random number generator used with a secret seed-key XKEY computed from CK and IK.

XKEY = SHA-1 (Identity | **CK | IK**)

The number of pseudo-random number generator iterations depends on the required keying material. The random numbers are concatenated and partitioned as follows:

- K_encr (128 bits): the encryption key to be used with AT_ENCR_DATA
- K_aut (128 bits): the message authentication key to be used with AT_MAC

Then, in the context of EAP with 802.1X

- The Pairwise Master Key (PMK) (256 bits) to be used to derive session keys for encryption and integrity protection of the WLAN exchanged data.

As the AP authentication may be performed frequently, an optional re-authentication mechanism is proposed.

Re-authentication:
In re-authentication, new specific keys are generated. Their computation is based on the same pseudo-random generator and a new seed-key XKEY' depending on XKEY.

XKEY' = SHA-1 (Identity | counter | NONCE_S | original **XKEY**)

2.2. Risk analysis due to the exposure of (CK, IK)

With the key material derivation performed in the terminal, there is a risk of exposure of (CK, IK) since an attacker could easily gain access to the terminal by the means of a Trojan horse or a malicious program.

The two following scenarios identify some threats due to this exposure.

Scenario 1: **Only full EAP/AKA authentication procedures** (without re-authentications)

In the context that the EAP/AKA method is used with 802.1X, the keying material derivation shall provide the 256-bit Pairwise Master Key, used by the terminal to derive a Temporary key. The session keys for encryption and integrity protection of the WLAN exchanged data are derived from this Temporary key.

Threat due to the exposure of (CK,IK):
Due to the exposure of (CK, IK) in the terminal, an attacker can obtain the Pairwise Master key (either by re-computation of the Master Key from CK and IK or by directly access to this Master Key). This Pairwise Master key is valid until the next full EAP/AKA authentication procedure.
The knowledge of the Pairwise Master key allows the attacker to retrieve all the derived Temporary keys that are used to derive the session keys for encryption and integrity protection of WLAN data. The WLAN exchanged data are no longer protected.

Countermeasure:
The keying material derivations are performed in the UICC, which only provides:

- K_encr (128 bits): the encryption key to be used with AT_ENCR_DATA
- K_aut (128 bits): the message authentication key to be used with AT_MAC

And

- The Temporary keys derived from the Pairwise Master Key. The period of validity of a Temporary key is shorter than the Pairwise Master key one.

With this countermeasure, there is no longer exposure of (CK, IK) and of the Pairwise Master Key.

Scenario 2: **There are re-authentications**

For each re-authentication, the new specific keys are derived.

Threats due to the exposure of (CK, IK):
The exposure of (CK, IK) in the terminal allows an attacker to retrieve the new keying material since the seed-key XKEY' is derived from XKEY that is derived from CK and IK! Until the next full EAP authentication procedure, all the new specific keys, depending on CK and IK values, can be retrieved.

Moreover, the threat identified in the scenario 1 still exists in this scenario.

Countermeasure:
Keying material derivations are performed in the UICC, which only provides:

- K_encr (128 bits): the encryption key to be used with AT_ENCR_DATA
- K_aut (128 bits): the message authentication key to be used with AT_MAC

And

- The Temporary keys derived from the Pairwise Master Key. The period of validity of a Temporary key is shorter than the Pairwise Master key one.
-

There is no longer exposure of (CK, IK) and of the Pairwise Master Key.

3. Conclusion

In EAP/AKA procedure with the USIM, there are some identified threats due to the exposure of (CK, IK) in the terminal. The threats are avoided if the keying material derivations are performed in a WLAN specific UICC application in charge of the UMTS AKA authentication and the computation of required specific keys.