3GPP TSG SA WG3 Security — S3#28 **S3-030198**
6 - 9 May 2003
Berlin, Germany

Title: **EAP support in smartcards and security requirements in WLAN authentication**

Source: **SchlumbergerSema**

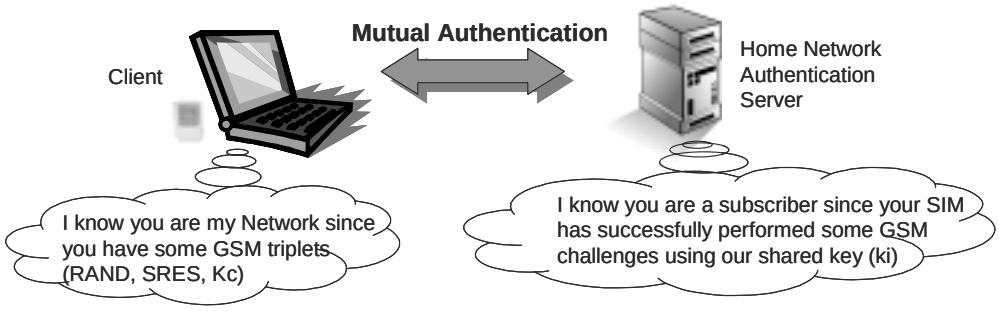
Agenda item: **6.11 (WLAN)**

Document for: **[Discussion, Approval]**

1 Introduction

Mutual authentication has been identified as a requirement in WLAN Interworking security.

Existing SIM-based WLAN authentication mechanisms (e.g. EAP-SIM) re-use part of the existing GSM infrastructure to additionally provide mechanisms for network authentication. However, some weakness has been detected in the security of the proposed network authentication procedures. This weakness derives from the usage of GSM triplets as the network authentication material. It means that a network is recognized as the subscriber's one, if it has proven the knowledge of some subscriber's GSM triplets.



An attacker that knows some subscriber's GSM triplets can simulate a fake network and mount a man-in-the-middle attack extremely compromising the user security.

The relatively low cost of base station in WLAN, positions man-in-the-middle attacks as one of the most important risks in WLAN deployment.

Deeper considerations are being undertaken related to the protection against this kind of attacks in WLAN environment. Some main issues are considered:

- USIM based solutions (e.g. EAP-AKA) are not troubled by this kind of concerns since mutual authentication is already provided by the inherent UMTS security mechanisms: secure end-to-end mutual authentication is already provided (between USIM and Home Network)

- GSM triplets, when they are the source of network authentication (e.g. EAP-SIM), shall be considered as security-relevant information in WLAN interworking and some security requirements are needed about the way this information is carried and handled.

Let us analyse some excerpts explaining in detail this known issue.

Extract from latest EAP SIM draft v9:

[…]

19.2. Mutual Authentication and Triplet Exposure

EAP/SIM provides mutual authentication. The client believes that the network is authentic because the network can calculate a correct AT_MAC value in the EAP-Request/SIM/Challenge packet. To calculate AT_MAC, it is sufficient to know the complete GSM triplets (RAND, SRES, Kc) used in the authentication. Because the network selects the RAND challenges and hereby the triplets, an attacker that knows n (1, 2 or 3) GSM triplets for the subscriber is able to impersonate a valid network to the client. Given physical access to the SIM card, it is easy to obtain any number of GSM triplets.

[…]

Yet another way to obtain triplets is to mount an attack on the client platform via a virus or other malicious piece of software.
[...]

***The client SHOULD be protected against triplet querying attacks by malicious software**. Since the security of EAP/SIM is based on the secrecy of Kc and SRES care should be taken not to expose these values to attackers when there are transmitted between entities, stored or handled. Steps should be taken to limit the transport, storage and handling of these values **outside a protected environment**. These considerations are important at both the client and authenticator implementations.*
[...]

Extract from TS 33.234 v0.3.0:

[...]

4.2.2 WLAN-UE Functional Split

The security functionality required on the terminal side for WLAN-3G interworking may be split over several physical devices that communicate over local interfaces. If this is the case, then the following requirements shall be satisfied:

- *Any local interface carrying security-relevant information must be adequately protected against eavesdropping and undetected modification. This protection may be provided by physical or cryptographic means.*

- *The endpoints of a local interface must be authenticated and authorized. The authorisation may be implicit in the security set-up.*

- ***The involved devices must be adequately protected against attacks on stored security-relevant information***

[...]

2 CONCLUSIONS and SOLUTION

As explained in these extracts, the security relevant-information (e.g. GSM triplets in EAP-SIM) should not be exposed to any kind of attacks as this may compromise both user and network security. This implies that a security risk is being assumed when this kind of WLAN security-relevant information is handled in clear by non-secured terminals (laptops,...) where all kind of virus attacks are possible.

Fortunately, there are already some solutions that handle this risk and that can be optionally provided by operators wishing to offer to their subscribers a more secure WLAN authentication.

The Internet draft “EAP support in smartcards” describes a framework defining an EAP client split between a smartcard and a WiFi client device (laptop, PDA...).

This draft does not represent a new EAP type, but it impacts the client architecture and security. The goal of this definition is to enable a client framework wherein, for any type of EAP used, all security calculations and data is managed inside a smartcard.

Particularly, EAP support in smartcards, may be applied to SIM-based WLAN authentication mechanisms (e.g. EAP-SIM). In that case, many of the issues regarding network authentication security requirements are solved.

The following figures show an example of network authentication in EAP-SIM. The first one shows a standard ME-SIM interface and the second one, a SIM enhanced with EAP support in smartcards.

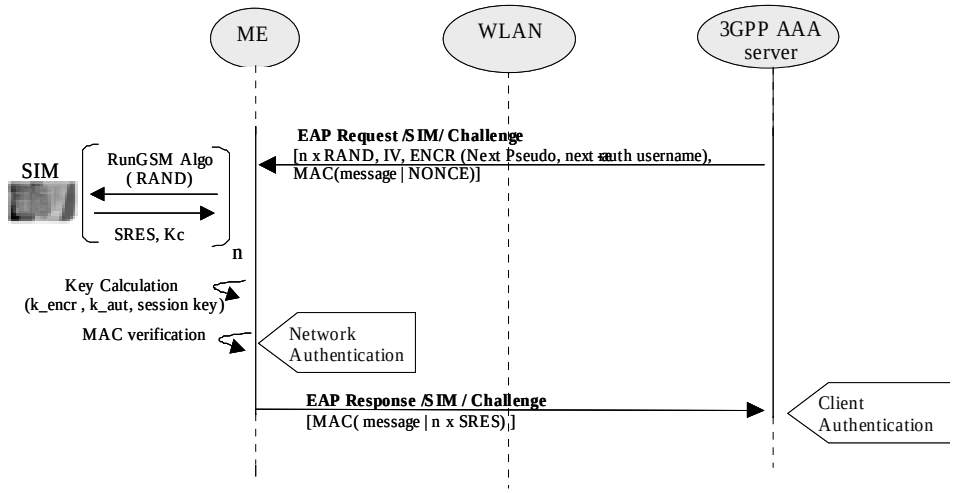


Fig 2: Network authentication example in EAP-SIM

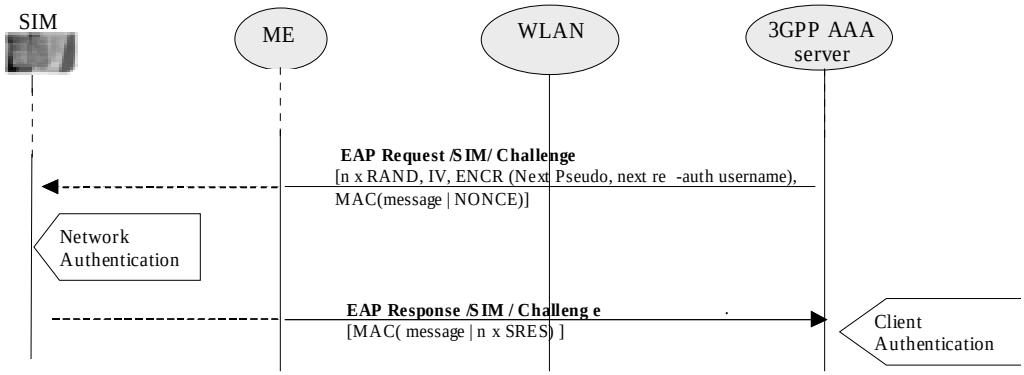


Fig 3: Network authentication example in EAP-SIM with EAP support for smartcards

Main enhancements to be underlined:

- EAP packets are tunneled to the SIM via the corresponding APDUs
- EAP traffic is not affected. There are no network impacts; it is just a client architecture matter.
- During the authentication process, all security calculations are performed inside the SIM.
- GSM triplets are not expose in clear in the insecure ME (e.g. laptop)
- Whether there are other devices between the supplicant ME and the SIM, (e.g. connected by local links) GSM triplets are not transferred in clear.

This split architecture produces a big number of advantages:

- Disable the risk of rogue base attacks. (GSM triplets are not exposed)
- Does not require changes to the network (this is just a client split)
- Would remove complexity from the WLAN client
- Facilitate operators to have their own security mechanisms for WLAN authentication:
    - Keeping it an intra-operator decision,
    - Keeping it protected in the SIM and in the Home network authentication server. (Inheritance of the same feature than GSM/UMTS networks with the authentication algorithms)
- May be also applied for USIM when using the GSM-security context.
- Additionally, as the Run-GSM-Algorithm command is not accessible by these insecure devices, the known brute force attack against the GSM authentication algorithm (especially COMP 128 v1) is not possible. A main consequence is that the risk of SIM cloning is strongly minimized.

3 Proposal

1. This document was considered in last SA2 meeting to be a security related issue that needed further SA3 considerations (see the following extract form the SA2 #29 WLAN meeting report)

[...]
S2-030256:
Identifies a security risk in utilising EAP/SIM in certain terminal environments and provides a solution for that. It was commented that SA3 should be considering this issue rather than SA2. It was commented that since it may have architectural impacts it is important that SA2 has a perspective. No impacts on network architecture have been identified.
[..]

Consequently, a liaison statement is proposed to be sent to SA2 to inform that SA3 has found that relevant authentication security improvements are provided by “EAP support in smartcards”. These enhancements may be taken into account by the standardisation activities undertaken in SA2 and SA3 in order to promote any further study by other groups. Moreover, this liaison shall ask T3 to start the corresponding actions to enable these security enhancements in the ME-(U)SIM interface. SA1 should be put in copy.

2. That “EAP support in smartcards shall be referenced in TS 33.234 adding the following paragraph 6.1.3 to the TS:

6.1.3 EAP support in smartcards

“EAP support in smartcards” (draft-urien-eap-smartcard) describes a framework defining an EAP client split between a smartcard and a WLAN-ME. Regarding security considerations, the solution proposed in this draft adds relevant protection to GSM based WLAN authentication mechanisms (e.g. EAP SIM)

This draft does not represent a new EAP type, but it impacts the client architecture and security. The goal of this definition is to enable a client framework wherein, for any type of EAP used all security calculations and data is managed inside a smartcard. Particularly, EAP support in smartcards, may be applied to (U)SIM-based WLAN authentication mechanisms (e.g. EAP-SIM or EAP-AKA).

The following figure reproduces a generic authentication procedure including the client split based in “EAP support in smartcards”:

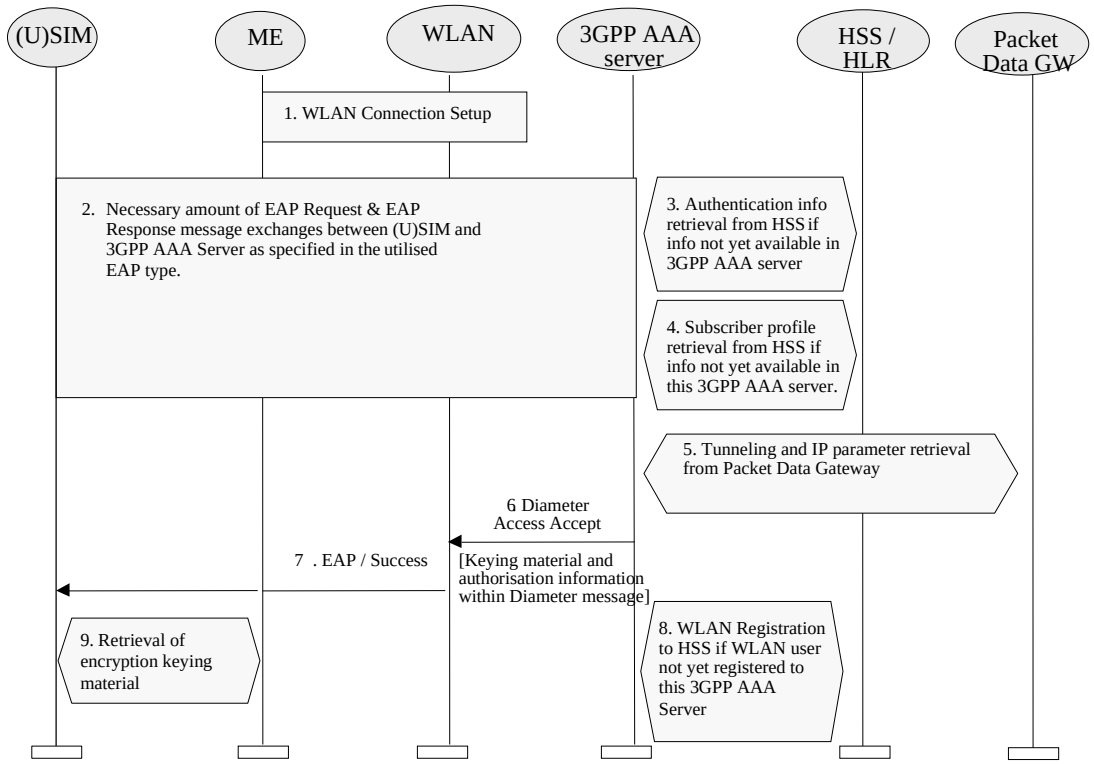


Figure: Authentication procedure based on EAP support in smartcards

1. WLAN connection is established with a Wireless LAN technology specific procedure (out of scope for 3GPP).

The EAP authentication procedure is initiated in WLAN technology specific way.
All EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

RadiusDiameter is used to encapsulate and transport all EAP packets to the 3GPP AAA Server.

In the client, EAP packets are transported within the corresponding Application Protocol Data Unit (APDU) as defined in “EAP support in smartcards”

2. A number of EAP Request EAP Response message exchanges is executed between 3GPP AAA Server and the EAP client embedded in the (U)SIM. The amount of round trips depends e.g. on the utilised EAP type. Information stored in and retrieved from HSS may be needed to execute certain EAP message exchanges.

3 Information to execute the authentication with the accessed user is retrieved from HSS. This information retrieval is needed only if necessary information to execute the EAP authentication is not already available in 3GPP AAA Server. To identify the user the *username* part of the provided NAI identity is utilised.

4 Subscribers WLAN related profile is retrieved from HSS. This profile includes e.g. the authorisation information and permanent identity of the user. Retrieval is needed only if subscriber profile information is not already available in 3GPP AAA Server.

5 Tunneling and IP parameters may be retrieved from/via Packet Data Gateway over the Wm reference point.

6 If the EAP authentication was successful, then 3GPP AAA Server sends Diameter Access Accept message to WLAN. In this message 3GPP AAA Server includes EAP Success message, keying material derived from the EAP authentication as well as connection authorisation information (e.g. NAS Filter Rule or Tunneling attributes) to the WLAN.

WLAN stores the keying material and authorisation information to be used in communication with the authenticated UE.

7 WLAN informs the UE about the successful authentication with the EAP Success message.

8 3GPP AAA server registers the WLAN users 3GPP AAA Server to the HSS. In registration messages, the subscriber is identified by his permanent identity. This registration is needed only if the subscriber is not already registered to this 3GPP AAA Server.

9 ME may receive from the (U)SIM the keying material derived from the EAP authentication performed.