3GPP TSG SA WG3 Security **S3-020654**

November 19-22, 2002

Oxford, UK

Agenda Item: WLAN

Source: Ericsson

Title: WLAN – Pseudonym Generation for EAP-SIM/AKA

Document for: Discussion and decision

1. Introduction

Both EAP-SIM and EAP-AKA authentication mechanisms include an identity privacy support feature based on the utilisation of pseudonyms: During an authentication procedure, the Authenticator node (the AAA server) optionally provides an encrypted pseudonym to the WLAN client. The WLAN client can (optionally) de-encrypt this pseudonym and present it as user identity for subsequent authentication attempts.

The EAP-SIM/AKA specifications do not define a method for the generation of pseudonyms, and leave that issue as an implementation decision. Nevertheless, in order to make it possible in 3GPP networks that pseudonyms provided by one AAA server can be recognised by another AAA server (potentially from another vendor), some standardisation is necessary.

1.1 TSG SA WG2 Input Requirements

The following requirements regarding pseudonym generation and management have been derived from working assumptions agreed at SA2#27:

Req_SA2_1: WLAN AAA servers SHALL generate pseudonyms

Req_SA2_2: No user state SHOULD be kept in AAA servers between WLAN sessions

Req_SA2_3: Pseudonyms SHOULD not be stored in HSS/HLR

Req_SA2_4: Pseudonyms MAY be derived from the user's IMSI

In order to fullfil these requirements, it is proposed that the AAA server generates pseudonyms as some form of encrypted IMSI.

1.2 Security Requirements

The following security requirements have also been considered for this pseudonym generation proposal:

Req_Sec_1: No complete break. (MUST)

Any secret keys used in WLAN AAA servers for the generation of pseudonyms should be infeasible to recover (even for an attacker that has available a number of matching permanent identities and pseudonyms).

Req_Sec_2: No partial break. (MUST)

Given a pseudonym (or even a number of correlated pseudonyms), it should be infeasible for an attacker to recover the corresponding permanent identity.

Req_Sec_3: No correlation. (MUST)

It should be infeasible for an attacker to determine whether or not two pseudonyms correspond to the same permanent identity.

Req_Sec_4: No random forgery. (SHOULD)

It should be infeasible for an attacker to generate a valid pseudonym (irrespective of the underlying permanent identity).

Req_Sec_5: No targeted forgery. (SHOULD)

It should be infeasible for an attacker to generate a valid pseudonym corresponding to a given permanent identity.

2. Proposal

2.1 Pseudonym Generation

As it was commented in section 1.1, it is proposed to generate pseudonyms as some form of encrypted IMSI. A block cipher can be used for this purpose. More specifically, it is convenient to use Advanced Encryption Standard (AES) in Electronic Codebook (ECB) mode of operation with 128-bit keys, for the following reasons:

- With its utilisation, requirements **Req_Sec_1** and **Req_Sec_2** can be fulfilled.
- A WLAN AAA server already needs AES for the implementation of the identity privacy support feature of EAP-SIM/AKA.
- ECB mode is the simplest and fastest mode to use a block cipher.
- The vulnerabilities of ECB mode are not relevant for the utilisation proposed here:
  - Replay attacks are not a concern.
  - Each block encrypted contains random data to a great extent (half of the block, see below), which significantly hardens cryptanalysis.

In order to encrypt with AES in ECB mode, it is necessary that the length of the clear text is a multiple of 16 octets. This clear text is formed as follows:

1. A *Compressed IMSI* is created utilising 4 bits to represent each digit of the IMSI. According to [TS23.003], the length of the IMSI is not more than 15 digits (numerical characters, 0 through 9). The length of the *Compressed IMSI* shall be 64 bits (8 octets), and the most significant bits will be padded by setting all the bits to 1.

   E.g.: IMSI = 214070123456789 (MCC = 214 ; MNC = 07 ; MSIN = 0123456789)

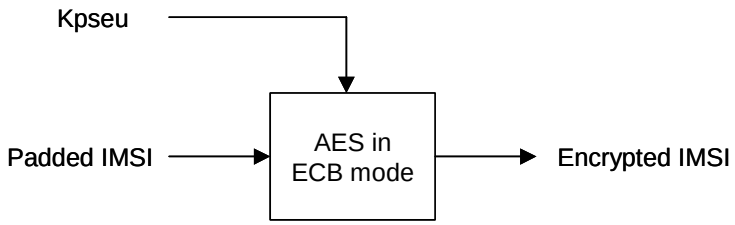
   Compressed IMSI = 0xF2 0x14 0x07 0x01 0x23 0x45 0x67 0x89

   Observe that, at reception of a pseudonym, it is easy to remove the padding of the *Compressed IMSI* as none of the IMSI digits will be represented with 4 bits set to 1. Moreover, a sanity check should be done at reception of a pseudonym, by checking that the padding, the MCC and the MNC are correct.

2. A *Padded IMSI* is created by concatenating an 8-octet random number to the *Compressed IMSI*. This random number provides the following:
   - The necessary length to complete the block size that must be fed into the AES cipher (i.e. 16 octets).
   - It serves to fulfil **Req_Sec_3**.
   - It hardens cryptanalysis of the cipher text, and thence it helps providing **Req_Sec_1** and **Req_Sec_2**.

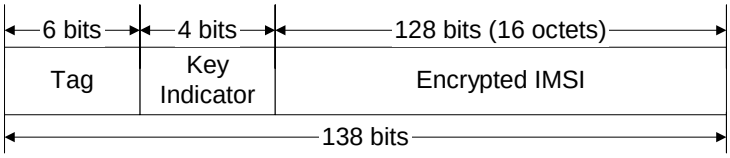
As it was mentioned above, a 128-bit secret key, *Kpseu*, is used for the encryption. The same secret key must be configured at all the WLAN AAA servers in the operator network so that any WLAN AAA server can obtain the permanent identity from a pseudonym generated at any other WLAN AAA server (see section 2.2).

The figure below summarises how the *Encrypted IMSI* is obtained.



Once the *Encrypted IMSI* has been generated, the following fields are concatenated:

- *Encrypted IMSI*, so that a AAA server can later obtain the IMSI from the pseudonym.
- *Key Indicator*, so that the AAA server that receives the pseudonym can locate the appropriate key to de-encrypt the *Encrypted IMSI*. (See section 2.2.)
- *Pseudonym Tag*, used to mark the identity as a pseudonym. The tag should be different for pseudonyms generated for EAP-SIM and for EAP-AKA.



The *Pseudonym Tag* is necessary so that when a WLAN AAA receives a user identity it can determine whether to process it as a permanent or a temporary user identity. Moreover, according to EAP-SIM/AKA specifications, when the Authenticator node (i.e. the AAA server) receives a temporary user identity from which a permanent user identity cannot be successfully obtained, then the permanent user identity must be requested from the WLAN client. As the procedure to request the permanent user identity is different in EAP-SIM and EAP-AKA, the *Pseudonym Tag* must be different for EAP-SIM pseudonyms and for EAP-AKA pseudonyms, so that the AAA can determine which procedure to follow.

The last step in the generation of the pseudonym consists on converting the concatenation above to a printable string using the BASE64 method described in section 4.3.2.4 of [RFC1421]. With this mechanism, each 6-bit group is used as an index into an array of 64 printable characters. As the length of the concatenation is 138 bits, the length of the resulting pseudonym is 23 characters, and no padding is necessary. Observe that the length of the *Pseudonym Tag* has been chosen to be 6 bits, so that it directly translates into one printable character after applying the transformation. Therefore, at reception of a user identity, the AAA server can recognise that it is a pseudonym for EAP-SIM or a pseudonym for EAP-AKA without performing any reverse transformation (i.e. without translating any printable character into the corresponding 6 bits).

2.2 Key Management

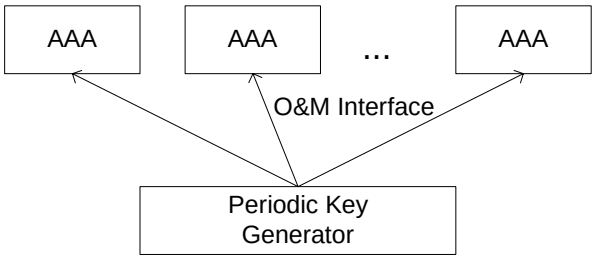
A 128-bit encryption key shall be used for the generation of pseudonyms for a given period of time determined by the operator. Once that time has expired, a new key shall be configured at all the WLAN AAA servers. The old key shall not be used any longer for the generation of pseudonyms, but the AAA servers must keep a number of suspended (old) keys for the interpretation of received pseudonyms that were generated with those old keys. The number of suspended keys kept in the AAA servers (up to 16) should be set by the operator, but it must be at least one, in order to avoid that a just-generated pseudonym becomes invalid immediately due to the expiration of the key.

Each key must have associated a *Key Indicator* value. This value is included in the pseudonym (see *Key Indicator* field in section 2.1), so that when a WLAN AAA receives the pseudonym, it can use the corresponding key for obtaining the *Paddedname* (and thence the *Username*).

Observe that, if a pseudonym is sent to a WLAN client but then the user does not initiate new authentication attempts for a long period of time, the key used for the generation of that pseudonym will eventually be removed from all the WLAN AAA servers. If the user initiates an authentication attempt after that time, using that old pseudonym, the

receiving AAA server will not be able to recognise the pseudonym as a valid one, and it will request the permanent user identity from the WLAN client. Thence, in order to achieve that permanent user identities are used as little as possible, it is recommended that the encryption key is not renewed very often.

The configuration of the keys could be done via O&M, as shown in the figure below.



Handling of these secret keys, including generation, distribution and storage, should be done in a secure way (out of the scope of this proposal).

2.3 Impact on Permanent User Identities

User identities (permanent or temporary) are sent with the form of a NAI, according to the EAP-SIM/AKA specifications, and the maximum length of a NAI that we can expect to be handled correctly by standard equipment is 72 octets (see [NAI]). Moreover, this NAI will be transported inside the User-Name attribute of a RADIUS Access-Request, with standard length up to 63 octets (see [RADIUS]). Therefore, it can be assumed that the maximum length of a WLAN user identity should be 63 octets (i.e. 63 characters).

Since the length of the pseudonym proposed in section 2.1 is 23 characters, the length of the realm part of any WLAN permanent user identity must always be 40 characters or less. This applies regardless of whether the length of the username part of the permanent user identity is less than 23 characters. (Note that a WLAN temporary user identity is formed as a NAI with the pseudonym as the username part and the same realm part as the permanent user identity.)

Moreover, the WLAN permanent user identities should not begin with the character resulting of the printable encoding transformation (see section 2.1) of the *Pseudonym Tag* used for EAP-SIM and EAP-AKA pseudonyms. This is needed so that at reception of a WLAN user identity, the AAA server can determine whether it is a permanent or a temporary user identity.

2.4 Acknowledged Limitations

The proposed mechanism for pseudonym generation fulfils requirements **Req_Sec_4** and **Req_Sec_5** in the sense that it is not feasible (without knowledge of the secret key) to forge a pseudonym that the AAA server recognises as valid:

- **Req_Sec_4**: To perform random forgery, an attacker would need to be able to generate an *Encrypted IMSI* so that the corresponding clear text passes the sanity check performed over the padding, the MCC and the MNC. That is, the attacker needs to fix at least the 3 most significant octets of the clear text by manipulating the 16 octets of the cipher text.
- **Req_Sec_5**: To perform targeted forgery, an attacker needs to fix the 8 most significant octets of the clear text by manipulating the cipher text.

Nevertheless, the proposed mechanism does not prevent forging of pseudonyms generated with keys that are no longer maintained in the AAA servers. That is, an attacker may form a pseudonym by concatenating the desired *Pseudonym Tag* and 132 bits of random information, and then applying the printable encoding transformation (see section 2.1). At reception of such pseudonym in a AAA server, the following cases are possible:

- The *Key Indicator* may not correspond to any key (active or suspended) maintained at the AAA server.
- If the *Key Indicator* corresponds to any of the keys maintained at the AAA server, then that key is used for the de-encryption of the *Encrypted IMSI*, but the sanity check over the padding, the MCC and the MNC would show that the IMSI is not correct.

In any case, the AAA server must interpret that the received pseudonym was generated with a key that is no longer available, and therefore it must request the permanent user identity to the WLAN client.

This could be exploited to perform DoS attacks by initiating a large amount of authentication attempts presenting different forged temporary identities. Nonetheless, the consequences of this attack should not be worse than the already possible attack of initiating a large amount of authentication attempts presenting different forged permanent identities.

3. Conclusions

It is suggested that SA3 adopts the mechanism described in section 2 for the generation of pseudonyms to be used for WLAN authentication with EAP-SIM and EAP-AKA.

4. References

[EAP-SIM] "EAP SIM Authentication", IETF draft-haverinen-pppext-eap-sim-07.txt, Nov. 2002

[EAP-AKA] "EAP AKA Authentication", IETF draft-arkko-pppext-eap-aka-06.txt, Nov. 2002

[NAI] "The Network Access Identifier", IETF RFC 2486, Jan. 1999

[RADIUS] "Remote Authentication Dial In User Service (RADIUS)"
IETF RFC 2865, June 2000

[AES] "Advanced Encryption Standard (AES)"
Federal Information Processing Standard (FIPS) draft standard,
http://csrc.nist.gov/publications/drafts/dfips-AES.pdf, Sep. 2001

[TS23.003] "Numbering, Addressing and Identification" (Release 5)
3GPP TS 23.003 v.5.4.0, Sep. 2002

[RFC1421] "Privacy Enhancement for Internet Electronic Mail:
Part I: Message Encryption and Authentication Procedures"
IETF RFC 1421, Feb. 1993