TR45 AHAG TR45.AHAG/01.05.22.__
Phoenix, AZ

TITLE:

UIM Authentication Method

SOURCE:

Lucent Technologies, Inc.

Semyon Mizikovsky
(973) 386-6348
smizikovsky@lucent.com

ABSTRACT:

This contribution describes a method for authenticating presence of the removable UIM in the mobile station in order to address the “rogue shell” attack.

RECOMMENDATIONS:

Review and adopt as preferred recommended method.

TR45 AHAG TR45.AHAG/01.05.22.__
Phoenix, AZ

1 Statement of Problem

TR-45 has recognized that the use of AKA in conjunction with Removable UIM (R-UIM) creates vulnerability in a form of "rogue shell" attack.

The "rogue shell" attack works like this: once an R-UIM in the shell performs AKA procedure, a "rogue shell" is used to collect the Ciphering Key CK and Integrity Key IK created as the result of AKA. The CK and IK are delivered by the R-UIM to the mobile shell because intensive computations, such as information ciphering and message authentications, can not be reasonably performed by the R-UIM due to its limitations, and so have to be performed by the mobile shell itself.

Once the CK and IK, along with other information, are collected from the R-UIM (e.g., IMSI), the shell can then be used to create a temporary clone, which would not report the removal of R-UIM, can initiate parallel communication sessions, or keep existing properly authenticated session active even after the R-UIM is removed.

Such activity will not be noticeable by the network, hence traditional methods of defense would not succeed.

The TR-45 AHAG and TR45.2 have agreed in principle to support optional local authentication procedures hereafter called "UIM authentication", that prove the presence of a valid UIM in the Mobile Station (MS).

2 Proposed Solution

2.1 UIM Authentication Key (UAK)

The UIM authentication process will be based on a new 128-bit UIM Authentication Key (UAK) that is created as an extension of the AKA process. The UAK will remain inside the UIM and will not be shared with the mobile shell, so that any authentication procedures that use UAK must be performed in the UIM.

The UAK shall be created by the HLR/AC and the UIM. The procedure for creating the UAK is specific for the Home Service Provider issuing the R-UIM. It resides in the AC and the UIM, and does not have to be standardized. However, the recommended procedure using SHA-1 algorithm **(function f_{11})** will be specified in the Enhanced Cryptographic Algorithms (ECA) document published by the AHAG.

If the UIM authentication is supported by the HLR/AC and the R-UIM, the UAK shall be delivered from the HLR/AC to the VLR in the serving system in addition to the Authentication Vector.

The serving system that does not support optional UIM authentication accepts the risk of the "rogue shell" attack and may choose to disregard the received UAK and instruct respective mobile to omit the UIM authentication too. Such serving system should also indicate its lack of support for UIM authentication to the HLR, so the UAK will not be delivered to it by the HLR in the first place.

Respectively, when the HLR and UIM do not support this feature, the UAK is not received by the serving system from the HLR, and the AKA process in the UIM associated with the Authentication vector will not result in generation of a new UAK.

2.2 Message Authentication Code (MAC)

Contrary to the 2G authentication, which validated a "signature" (AUTHR) of subscription parameters (namely ESN, IMSI, SSD-A) in the authenticated mobile, the Enhanced Subscriber Authentication (ESA) is based on authenticating the contents of messages sent by the authenticated entity. To accomplish this, a Keyed Message Authentication Code (MAC) is generated on a critical content of selected messages. The code is then attached to these messages for validation of message integrity.

On both mobile and base station sides the MAC is computed on the message content using secure hash function f_{12} specified in the ECA document.

We recommend the following inputs into this function:

- critical Message Fields,
- 128-bit IK as the secret key,
- 64-bit Random Challenge RAND,
- Additional message specific values (FRESH), like 7-bit Message Counter, 1-bit Direction Indicator, 8-bit Message Type identifier, etc. Content of FRESH can be defined by the air interface standard.

$$\mathbf{MAC = f_{12}(MessageFields, IK, RAND, FRESH)}$$

When operating on Common Control Channels, the 64-bit RAND will be the Global Challenge value currently broadcasted by the base station. Note, that to preserve access security to the greatest extend, the fast changing Global Challenge is highly recommended.

When operating on Dedicated Traffic Channels, the 64-bit RAND will be the Global Challenge value in effect at the time of setting up the current session.

The FRESH value can be defined by specific air interface requirements. For example, 7-bit Message Counter is incremented with each authenticated message, and can be reset for each new value of the Random Challenge. The 1-bit Direction Indicator is set to '0' for all Reverse direction messages, and to '1' for all messages in Forward direction.

The output of the process is the value of MAC (truncated to acceptable size, for example, 24-32 bits).

2.3. MAC Post-process by the UIM.

The technique described in this section is proposed by Qualcomm, Inc.

In order to verify presence of the R-UIM in the mobile, the MAC computed on the critical message is passed to the UIM for post-processing with the secure function f_{14}, defined in the ECA document. Both MAC and UAK are input into the function, and resulting value, called UMAC, is returned to the mobile shell.

$$\mathbf{UMAC = f_{14}(UAK, MAC)}$$

The returned value of UMAC replaces MAC and is attached to the transmitted message.

Note, that if serving system indicates the lack of support for this feature, or if UIM is not equipped to support it, this step in the procedure is skipped and original MAC is attached to the message. Note also, that messages transmitted by the base station on the Forward link contain just MAC, and the post-processing of it with f_{14} is not necessary.

2.4. Periodic Unique Challenge

In special cases it may be necessary to verify that not only active communication session is maintained with legitimate mobile, but also that legitimate UIM is still present in the mobile while the call is on. In such cases the Unique Authentication Challenge is executed.

The 64-bit Unique Random Challenge RANDU is used in place of a Global Challenge in a RAND input to the f_{12} function. The RANDU is also looped back (returned) to the base station as a critical Message Field of the *Unique Challenge Response Message*. In this example, computation will proceed as follows:

$$\mathbf{MAC = f_{12}(MessageFields, IK, RANDU, FRESH)}$$

$$\mathbf{UMAC = f_{14}(UAK, MAC)}$$

The mobile station transmits the *Unique Challenge Response message* containing the RANDU in the critical message field, with the UMAC attached to it, to the base station.

TR45 AHAG TR45.AHAG/01.05.22.__
Phoenix, AZ

3 Conclusion

Described method in conjunction with the fast changing Global Challenge provides adequate protection from the “rogue shell” attack, and can be economically implemented on a removable UIM.