3GPP TSG SA WG3 Security — S3#16 S3-000711

28-30 November, 2000

Sophia Antipolis, France

SOURCE: LUCENT TECHNOLOGIES

TITLE: ROGUES MS-SHELL THREAT ANALYSIS (ANSI-41)

DOCUMENT FOR: INFORMATION

AGENDA ITEM: TBD

TITLE:

Rogues MS-Shell Threat Analysis

ABSTRACT:

TR45 committee indicated that protection against rogue MS-shell attack is a high priority issue. As directed by TR45, the TR45.2 and the TR45-AHAG subcommittees discussed different potential solutions. TR45.2 agreed, in principle, with the method of protection presented in contribution TR-45.2.2/00.08.15.06 (see ANNEX1). The method requires that, to access the network, the USIM has to successfully perform a "local authentication" cryptographic procedure. The procedure is based on a unique "Local Authentication Key" (LAK) generated by the Home Entity (HE/AuC), the USIM and also transferred to the Serving Node (but not known by the MS-shell). This contribution describes, in more details, some potential "rogue MS-shell" threats that can be prevented by the above method. The threat analysis presented by this contribution should also clarify why the development of this protection method against a rogue MS-shell is highly desirable and economically justifiable for an ANSI-41 operator.

1. INTRODUCTION

During deliberations in TR45.2 subcommittee, the "rogue MS-shell" threat has been identified as a serious fraud problem. In turn, TR45 indicated that protection against this type of attack is a high priority issues, and directed TR45-AHAG and TR45.2 subcommittees to identify methods by which this problem may be minimized.

During the joint meeting between S3 and AHAG in Stockholm (document S3-000233 - Stockholm), TR-45 AHAG also recommend that S3 and the AHAG explore how the vulnerability to a rogue "MS-shell" may be minimized.

Contribution TR-45.2.2/00.08.15.06, attached, describes such a method, and TR45.2 agreed, in principle, with the proposal and is currently developing potential implementation procedures.

2. WHAT IS A ROGUE MS-SHELL?

2.1 AKA Security Association establishment

In GSM/UMTS networks, the mobile equipment is comprised of the User Identity Module (UIM/USIM) and the user equipments (UE). The USIM contains the subscriber information, while the UE can be a cellular phone, a PC, a PDA or any other cellular capable equipment that is capable of communicating with a cellular Base Station over the air interface. In this document, we are referring to the UE as a "MS-shell". ANS-41 is also implementing a very similar architecture, and planning to use an UIM (R-UIM) in association with the "MS-shell".

The AKA authentication procedures establish the security association (SA) between the USIM and the Serving Network. The Home Entity (HE), upon receiving an authentication data request from the VLR, establishes a SA that includes the mutual authentication parameters (RES,RAND,AUTN), as well as the Integrity Key (IK) and Ciphering Key (CK) that are used until the AuC establishes a new SA.

The actual Message Authentication Code (MAC) and traffic channel encryption is done by the "MS-shell", and is based on the IK and CK calculated by the USIM, and transferred to the MS-Shell during the authentication procedure.

A new SA, including a new IK and CK, can be established with each network access, e.g., origination, termination or registration. Since this method uses significant network bandwidth, and it may introduce unacceptable delays in establishing a call session, the IK, established between the user and serving network during the previous execution of the authentication and key establishment procedure, is used as a '"local authentication" mechanism[1].

[1] The USIM shall contain a mechanism to limit the amount of data that is protected by an access link key set. Each time an RRC connection is released the values STARTCS and STARTPS of the bearers that were protected in that RRC connection are stored in the USIM. When the next RRC connection is established that values are read from the USIM. The ME shall trigger the generation of a new access link key set (a cipher key and an integrity key) if STARTCS or STARTPS reach a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out or during an RRC connection. When this maximum value is reached the cipher key and integrity key stored on USIM shall be deleted

The key set identifier (KSI) is a number, which is associated with the cipher and integrity keys derived during authentication, to make it possible for the network to identify the CK and the IK, which are stored in the mobile station without invoking the authentication procedure. This is used to allow re-use of the cipher key CK and integrity key IK during subsequent connection set-ups.

Note that to protect against the unauthorized use of the IK, *the 3G-security architecture requires that the IK shall be deleted from the UE when the UE is powered down, or when the USIM is removed.*

2.2 What is a Rogue MS-Shell and should the carrier wary about this threat?

The above-mentioned requirement does work well for a well-behaved MS-shell. The serving network may also implement proprietary mechanisms by which to limit the period of IK reuse in local authentication procedure. The problem is that the mechanisms used to limit the exposure to a compromised IK are based on a well behaved MS-Shell.

What is a “rogue” MS-Shell? A Rogue MS-Shell is the user equipment manufactured for the specific purpose of reusing a legitimate user’s IK to make fraudulent calls.

How can a legit UE design be modified for this purpose and how difficult is to manufacture such a device? Some hope that it is very difficult; in fact it is so difficult, that the cellular bandits will not bother to design and manufacture such a device (i.e., there is no economical incentive).

This is a valid question that has to be seriously evaluated. After all, the goal of a good cryptographic algorithm is to make “the cost of breaking the cipher exceed the value of the encrypted information”. An analogy can be easily made with the rogue MS-shell. Why bother to protect against this type of threat, if the cost of the equipment will exceed the value of the “free” services obtained? We will evaluate this question in the following sections.

2.3 Threat analysis

How can a rogue MS-shell obtain “free” access to the network? It may be relatively simple: the UE does not delete the IK when the USIM is removed from the MS-Shell (as required by the standards specifications). Since the serving network relies on the IK for local authentication, the rogue MS-shell can continue accessing the network until the SA association is updated. Note that if the SA is refreshed for each network access, than MS-rogue shell threat is eliminated, since the rogue MS-shell will not be allowed to re-use an invalid IK. On the other hand, if the SA is kept valid for a number of calls or hours, or even days (as indicated by some ANSI-41 operators), then significant revenues may be lost.

It may be beneficial to analyze a few scenarios, based on US based operator planned services, to understand the potential financial damage that a rogue MS-Shell can cause:

- A user decides to take advantage of the airport “internet kiosk”. She inserts her USIM into the public PC and, after the user is authenticated by the home system, a PS connection is established. When finished, she removes the USIM and boards the plane for a 16-hour flight. Since the PC terminal has been modified to retain the IK after the USIM is removed, the cellular bandit can now masquerade as a legitimate user. He can even sell airtime to an unsuspected customer. Due to the large number of daily passenger passing through an airport, one can surmise that the supply of IK ‘s will probably meet the demand for ‘free” services.

- An international traveler rents a phone for use while traveling to a foreign country (e.g., a CDMA or a TDMA cellular user traveling to Europe and requiring a UMTS phone). He does have an universal USIM, but needs a phone capable of supporting a different air-interface. Unfortunately, he is provided with a rogue MS-shell for the duration of his stay. After the UE is returned, the rogue phone can then be used to provide “free” cellular services to the next “customer.

- A user decides to use it’s USIM is a taxi-phone. The SA association is then established, and the user accesses the network. The rogue taxi-phone continues to be successfully authenticated by the serving network, even after the USIM is removed. Needless to say, when a new victim uses the same taxi-phone, a new IK is used. In a taxi-phone environment, one can assume that the supply of IK’s will meet or even exceed the demand.

- A rouge MS-Shell can be used to make 3WC. Using this method, fraudulent “call booth” can be created anywhere in the world. A very profitable call distribution center can be established.

Note that the above scenarios can be extended to convention centers, hotels, “Cyber Café”, etc.

- A fraudulent subscriber can share, for a fee, his “temporary” identity with many rogue phones. Of course, this threat will require a cooperative subscriber. The Local Authentication Key will not protect the carrier against a fraudulent subscription, but it will limit the network access to only one such “subscriber,” since the user will have to use the USIM when accessing the network, i.e., he will not be able to share his subscription with 100+ other accomplices. Therefore the service provider exposure to fraud is significantly limited.

The problem is more severe when one considers future PS scenarios, with long duration and costly connections. There are current mechanisms put in place to minimize the exposure to this type of threat, but unfortunately those protection techniques rely on a well-behaved UE, on the information calculated by the UE or on the information stored in the UE, as well as the security policies established by a serving system that may or may not implement an effective security policy.

2.4 How to combat this problem?

There are a number of methods to deal with this problem:

2.4.1 Do nothing

It is suggested that the best approach is rely on normal AKA procedures, i.e., the a rogue MS-shell potential fraud can be analyze based on a “financial model” protection, i.e., it would costs more to design and manufacture such a device then the profits one can expects to gain from type of attack (analogues to the cryptographic concept that “the cost of breaking the cipher exceeds the value of the encrypted information”). Although this is a legitimate argument in some cases, it is not an acceptable method of combating a rogue MS-shell attack. It is not clear at all how complex, or costly is to modify an existing UE not to delete the IK’s. Some design methods that a cellular bandit may consider when designing such a rogue MS-shell may include:

- Creating an image of the memory, and restore it after the USIM is removed
- Detect the code that reports the USIM removal, and patch a command to bypass the “delete IK,CK” directive.
- Store the IK and CK in a temporary array after they are received from the USIM during the SA procedure, and restore them after the USIM is removed.
- Modify the PC modem functionality, via a new modem driver, to bypass the removal of the IK.

A clever hacker or software designer can probably invent many other ways of achieving this goal (and based on past experience, they are very ingenious and persistent when motivated by greed). The mass production of such a modified phone can be probably achieved at relatively low cost. The risks of being detected are minimal, since there is no automatic way of detecting that a rogue MS-shell accesses the network (it perfectly impersonates the legitimate user’s secrete ID).

Although the cost is most probably higher then other current methods, one has to consider that, due to the vastly improved security architecture designed into a 3G network, the cellular bandits may find that the cost of designing a rogue MS-shell is economically justifiable. The rogue MS-shell may even be one of the more attractive and reliable ways of fraudulently accessing a 3G network, since timely detection may not be easily achieved. Some “user” may consider impersonating John Doe a very attractive alternative, for which they will be willing to pay premium price.

Therefore “doing nothing”, although very attractive from a development cost, is not one of the best methods to protect against a rogue mobile attack.

2.4.2 Security Association per call

If a carrier chooses to use a new security association for each new network access (origination, termination, registration), then no new development is required. This method does not require any changes to the current AKA architecture or procedures, and effectively protects against a rogue MS-shell. Unfortunately, this solution may not be economically feasible due to the high cost of network resources, limited network bandwidth, call setup delays, etc. This view has also been expressed by some ANSI-41 operators.

Some suggest taking a “wait and seeing” attitude, i.e., monitor for a rogue MS-shell attack, and when detected, the carrier can implement the policy of a new SA per each access as the default mode of operation. Although this may theoretically work, in practice is difficult to see that such a method can be effectively implemented. There is no specific indication to a service provider that a rogue MS-shell accesses the network. Probably the first indication will come from an irate customer, complaining about his or hers bill. But even if the carrier recognizes that the losses caused by rogue MS-shells have dramatically increased, the carrier will have a very limited set of tools at his disposal to protect himself. The only option available to a carrier is to enable SA per call in all its networks, or hopefully only in some vulnerable networks (note that it will be very surprising if the problem can be localized to few serving networks). There is a very high probability that the problem will first be detected in a very high Busy Hour Call Attempts service area, making the SA per call option very costly from a network and quality of service point of view. The home carrier will have to rely on a collaborative serving network to implement SA per call, and accept the increase network traffic.

2.4.3 Velocity violation

It was also suggested that a velocity violation (e.g., detecting multiple call instances) could be used to provide protection against a rogue MS-shell attack. This method presents some severe drawbacks: the serving node does not know which call is legitimate and which is not, therefore this method is considered service effective, since the probability is that a legitimate caller will be dropped approximately 50% of the time.

Although this method has some limited success in a 2G system, it is not effective in a 3G system since a subscriber can have multiple simultaneous call instances (i.e., CS and multiple PS). Therefore one cannot rely on the old, established methods of detecting velocity violations.

In conclusion, this protection method cannot be seriously considered as effective protection against rogue MS-shell threat.

2.4.4 Local authentication mechanism (based on a Local Authentication Key[2])

The best protection against a rogue MS-shell threat is the method described in contribution TR-45.2.2/00.08.15.06 (annex 1). The method is based on a Local Authentication Key (LAK) known only to the USIM and the Serving Node (controlled by the HE/AuC). This method provides a very effective and automatic method of denying network access to a rogue cellular device.

In conclusion, the LAK method is the only method able of providing a reliable protection mechanism against a rogue MS-shell attack. This method can be implemented in an ANSI-41 network without any technical barriers to global roaming.

3. CONCLUSION

We conclude that the solution put forth that “the best solution is to do nothing”, and apply AKA per call when needed, cannot be seriously considered by TR45, if protection against a MS-rogue shell is required. One should note that if we do nothing now, it may be practically impossible to modify hundred of million of phones in the field at a latter date.

The other alternative to have a new SA per call, with the associated increase in traffic load caused by additional authentication directives traversing multiple networks, for millions of call per busy hour is also not very attractive. This method will most certainly have a great negative impact on the networks capacity and bandwidth utilization, the serving nodes as well as the HE/AuCs performance. This method also assumes that a roaming partner is willing to support the significant network traffic expected to support this protection mechanism.

The only possible conclusion one can reach is to concur with the TR45 and TR45.2 directive and to continue developing the best technical solution to combat the “rogue MS-shell” threat. We already have a technical solution that every one agrees that it provides protecting against this type of threat, while fully supporting global roaming, while requirering relatively minor modifications to the current AKA procedures.

[2] It should be also noted that implementing a Local Authentication Key mechanism will also make Global Challenge in ANSI-41 (as directed by TR45) more effective and minimize its reliance only on the IK.

Annex 1 - **TR-45.2.2/00.08.15.06**

TITLE:

Enhanced local authentication for a 3G mobile

SOURCES:

Lucent Technologies Inc.

Michael Marcovici	Simon Mizikovsky
(630) 979 4062	(973) 386-6348
(630) 224-9955 FAX	(973) 884-6364 FAX
marcovici@lucent.com	smizikovsky@lucent.com

ABSTRACT:

This contribution proposes a new mechanism to protect against 'rogue" mobile shell units, by providing a secondary authentication mechanism.

RECOMMENDATIONS:

For Approval.

Notice:

This contribution has been prepared by Lucent Technologies Inc. to assist the Standards Committee TIA TR45, ETSI, and 3GPP. This document is offered to the Standards Committee as a basis for discussion and should not be considered as a binding proposal on Lucent Technologies Inc. or any other company. Specifically, Lucent Technologies Inc. reserves the right to modify, amends, or withdraw the statement contained herein.

Permission is granted to TIA, ETSI, and 3GPP Committee participants to copy any portion of this document for the legitimate purposes of creating the standards. Copying this document for monetary gain or other non-standardization purpose is prohibited.

4. INTRODUCTION

The current 3GPP authentication protocol, as defined in 3GPP TSG 33.102, can be summarized as follows:

> As a result of successful Authentication and Key Agreement (AKA) procedure, the network and the mobile station (MS) establish a security association by generating a set of common keys: the Integrity Key (IK) and the Ciphering Key (CK). On the MS side, those keys are generated inside the User Subscription Identity Module (USIM), which is expected to be a removable Smart Card.
>
> Once generated on the USIM, the keys are sent to the mobile "shell", or user equipment (UE) via the Authenticate Command. The UE uses the value CK for ciphering any future communications with the network and the value IK for ensuring the integrity of the messages exchanged between the UE and the Serving Network (SN).
>
> While the security association is valid, the IK can be used for local periodic re-authentication between the VLR/SGSN (SN) and MS. This local authentication process, i.e., the use of the IK for the MS's local re-authentication, significantly minimizes the required intersystem network traffic associated with the use of a fresh vector for authentication on each call. Unfortunately, it does open a window for the potential fraudulent use of the network. The following scenario describes one such potential fraudulent use of the network. Additional scenarios can be easily envisioned.

4.1 Statement of Problem

This section briefly summarizes one potential “Rogue Mobile Shell” attack. Consider the public access mobile shell (a cellular phone in a public place, rental car, limo, leased, etc.), which is activated when the customer's USIM is inserted into the unit. The Home System, by conducting the AKA procedure, establishes the security association with the user’s MS and, as the result, the USIM generates a new set of CK and IK keys. In the classic 3GPP security architecture, the USIM is also instructed by the HLR as of how long this association can be valid and when to re-authenticate.

The USIM then sends the CK and IK to the mobile shell (UE), which in turn uses the CK to encrypt/decrypt the communication with the serving system, and the IK for generating a Message Digest, or Integrity Signature for specific critical messages sent to the Serving System.

Assuming normal operation, the same CK and IK will be used for more than one call to conserve network resources, and the Serving System will be happy to communicate with the mobile providing that Message Digests check and Decryption process works fine.

Assume at this point that the user is done with this phone, and the USIM is removed. According to the Security Requirements, the mobile shell must erase the CK and IK. Unfortunately a rogue shell cannot be controlled, and it has been modified to retain the keys! At this point it really does not need the USIM any more. In fact, it will not conform to the HLR instruction to "replace" the security association after so many calls, or so much time. Therefore the hacker can use the existing keys to keep communicating with the serving system, make new calls, etc., until a new security association is established by the AuC at the request of the SN. This is assuming that the SN has some built in proprietary functionality to request a new security association independent of the UE.

Base on common practices, as described in the 3GPP Implementation Guide, the Serving System has to initiate the request for a new security association; therefore there is a real possibility that the service may be provided to a rogue shell until the real USIM appears in a new Serving System, and the Location Update procedure cancels the registration in the old system were the rogue mobile is operating. Depending on the serving system practices, this could allow for fraudulent calls to be made for a relatively long time.

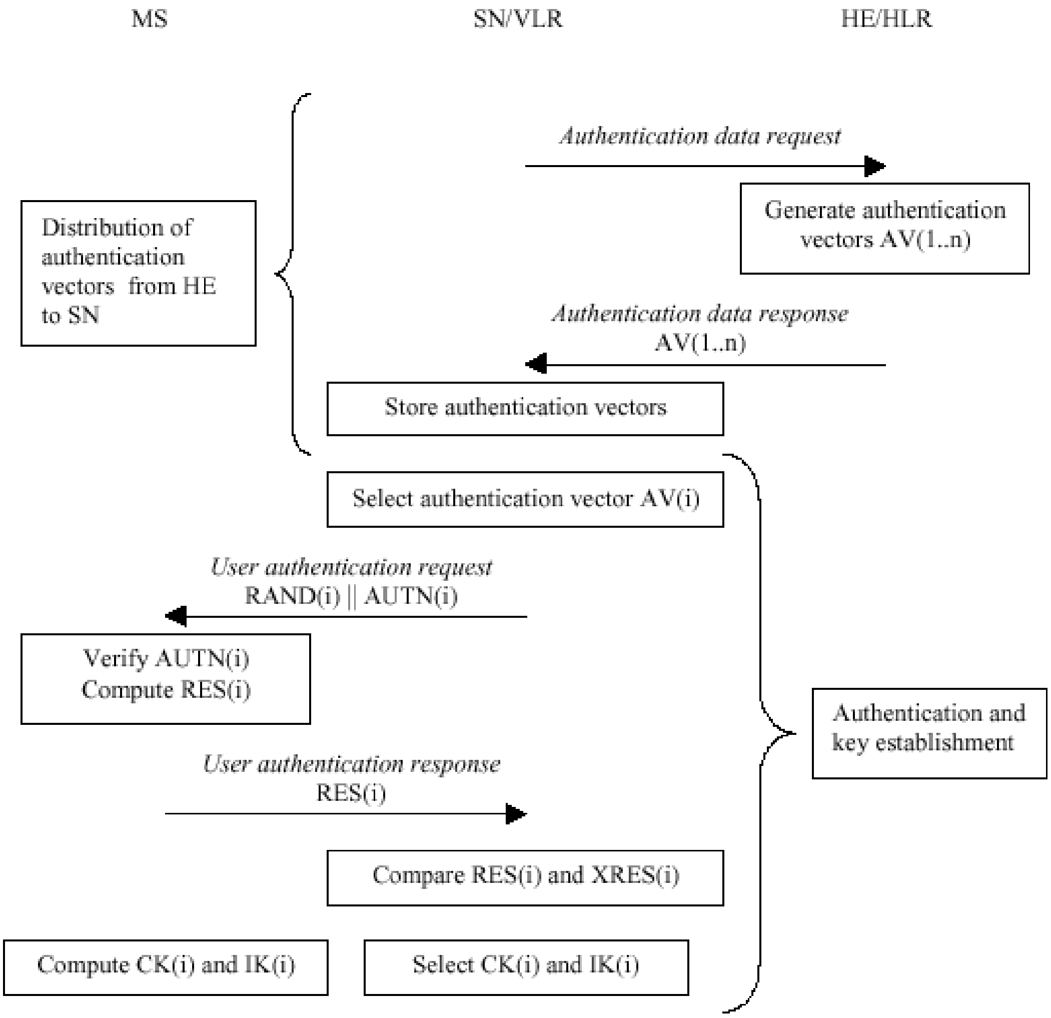
An even more malicious attack may be envisioned, whereby the IK is copied into multiple rogue shells, which can in turn be used to fraudulently access the network. This may present a very attractive opportunity for a cellular bandit who operates in a 3G environment, were multiple instances of a call/user can be envisioned as a routine operational assumption (e.g., PS, CS).

To significantly minimize, or even eliminate, this type of fraudulent use of a UE, a method is required to improve the local authentication by introducing a secret parameter unknown to the UE, but available at the USIM and the Serving Node.

5. PROPOSED NEW METHOD

To mitigate this problem, the USIM should periodically authenticate itself to the serving system using the information readily available at USIM and VLR, but not at the mobile shell (UE).

5.1 Current methodology


MS
SN/VLR
HE/HLR
Authentication data request
Generate authentication vectors AV(1..n)
Distribution of authentication vectors from HE to SN
Authentication data response AV(1..n)
Store authentication vectors
Select authentication vector AV(i)
User authentication request RAND(i) || AUTN(i)
Verify AUTN(i) Compute RES(i)
Authentication and key establishment
User authentication response RES(i)
Compare RES(i) and XRES(i)
Compute CK(i) and IK(i)
Select CK(i) and IK(i)

According to the 3GPP standard, the AKA protocol authenticates the network to the mobile by delivering the Network Authentication Token (AUTN), included in the Authentication Vector (AV) delivered from the Home Location Register (HLR/AuC) to the MS. The AUTN contains the Sequence Number parameter (SQN) concealed by the Anonymity Key (AK):

$$\mathbf{AV} := \mathrm{RAND} \,||\, \mathrm{XRES} \,||\, \mathrm{CK} \,||\, \mathrm{IK} \,||\, \mathbf{AUTN}$$

$$\Downarrow$$

$$\boxed{\mathrm{AUTN} := \mathbf{SQN} \oplus \mathbf{AK} \,||\, \mathrm{AMF} \,||\, \mathrm{MAC}}$$

Note that the USIM can calculate the AK [AK = $\mathbf{f5}_K$(RAND)], while the ME cannot.

5.2 Enhanced Local Authentication Methodology

The goal of our proposed solution is to reduce required modifications of the present 3GPP AKA to a minimum, preserving the functionality and processing requirements of present AKA architecture as much as possible, while minimizing network traffic (note that the rogue shell problem can be eliminated by establishing a new security association per call, but this is considered impractical due to the enormous traffic network volume that it may generate). Therefore this contribution introduces a new concept of Local Authentication based on a Local Authentication Key (LAK). The LAK is known only to the Home AuC, the SN, and the USIM but **NOT** to the UE.

We propose the following:

1) Upon establishment of the Security Association (successful completion of the AKA procedure), the CK and IK are copied from the USIM to the mobile shell, as it is defined in the 3GPP AKA specifications **(current architecture).**

2) The CK is used for information ciphering and the IK for message integrity for the duration of the Security Association, as it is defined in the 3GPP AKA specifications **(current architecture).**

3) Upon call setup, service request, etc., as defined by the air interface operational requirements, the local authentication, based on a new Local Authentication Key (LAK), is conducted between the Serving Node (SN) and the USIM when the SN is challenging the USIM. This could be done either via the Global Challenge (GC) or the Unique Challenge (UC) interrogation.

4) A new parameter "TYPE" is defined to uniquely identify the access type (e.g., origination, registration)**.**

5) The SN challenge is passed by the mobile shell to the USIM, which in turn uses current IK as the authentication key and the LAK as the local authentication supplement in computing the local authentication response AUTH_L (if Global Challenge option is available) or AUTH_{UL} (if Unique Challenge is used):

$$\boxed{\mathrm{AUTH}_L = f_{11}(\mathrm{TYPE},\mathrm{RAND}_G, \mathrm{LAK})_{IK} \text{ if Global Challenge is used}}$$

or

$$\boxed{\mathrm{AUTH}_{UL} = f_{11}(\mathrm{TYPE},\mathrm{RAND}_U\text{[3]}, \mathrm{LAK})_{IK} \text{ if Unique Challenge is used}}$$

Note that the Anonymity Key (AK) can be used, at a service provider’s option, as the LAK. In this case, both the AC and the USIM compute the 128-bit value of the AK, which is than truncated to the required length (48-bit) to cover the SQN. However, the whole 128-bit value of the AK is still available at each computing site.

Alternatively, the LAK can be independently calculated (up to a full 128 bit key), and transferred to the service network together with the AV or when the session is established (e.g., at registration time). Other scenarios may be devised by an operator, based on his/hers operating practices.

6) Because the LAK is known to the USIM but not known to the UE, and it’s use is randomized by RAND_G or RANDU, the mobile shell can not counterfeit the AUTH_L or the AUTH_{UL}

7) Two implementation alternatives are described:

   a) Alternative 1:

      The AUTH_{UL} is sent to the Serving Node (e.g., VLR/SGSN), which in turn validates the AUTH_{UL} by duplicating its computation.

   b) Alternative 2:

      The AUTH_L is included in the MAC-I calculations; therefore the AUTH_L would not have to be sent to the Serving System (see below for additional details).

8) For this procedure, the LAK shall be transmitted from the HLR to the VLR in the **“clear”**. Note that if the LAK=AK, there should be no concern about revealing the AK value to the VLR: present 3GPP specs require that AK is XORed with SQN to protect the SQN on the air interface only.

[3] **<u>Note:</u>** AUTH_{UL} can optionally be calculated based on the RAND_G. For text simplicity and clarity, for all future references to AUTH_{UL} read "RANDU” as RANDU or optionally RANDG

The ANSI-41 serving node can optionally broadcast a Global Random Number $RAND_G$ to be used in the new enhanced global authentication procedure.

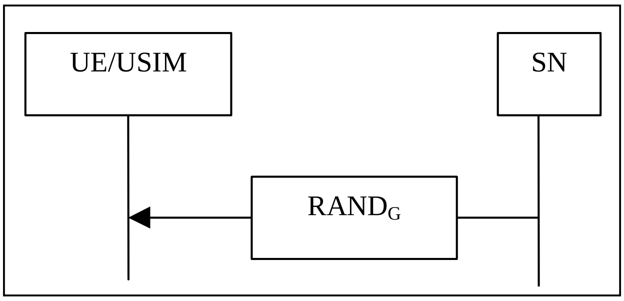


Figure 1 Broadcast RAND (Global Challenge)

As an option to the Global Challenge (RAND), the RANDU (RAND Unique Challenge) can be used in the F11 calculations,

A new standardized function (e.g., F_{11}) shall be defined in the SN and the USIM to calculate the $\underline{\mathbf{AUTH_L}}$ or the $\underline{\mathbf{AUTH_{UL}}}$ such that:

$$\boxed{\textbf{F11: (IK; TYPE; LAK;RAND}_{G}\textbf{)} \Rightarrow \textbf{AUTH}_{L}}$$

OR

$$\boxed{\textbf{F11: (IK;TYPE;LAK;RAND}_{U}\textbf{)} \Rightarrow \textbf{AUTH}_{UL}}$$

If alternative 2 is chosen, the procedure for data integrity of signaling data requires an upgrade to the F9 cryptographic function i.e., the currently defined AKA f9 MAC function shall be modified to include the $AUTH_L$:

$$\boxed{\text{F9: }\textbf{AUTH}_{L,}\text{ IK, COUNT-I, FRESH, DIRECTION, MESSAGE}}$$

The "new" MAC-I generated by the F9 from a signaling message is based on the IK agreed to in the last valid AKA process **and** the new key $AUTH_L$ (calculated by F11 based on the $RAND_G$ broadcasted by the SN and the LAK). Therefore, all attempts to access the network within a valid security association will not be based exclusively on the IK, which is known to the UE, but also on the LAK which is never transmitted over the air, never made known to the UE, and is randomized by $RAND_G$ and TYPE.

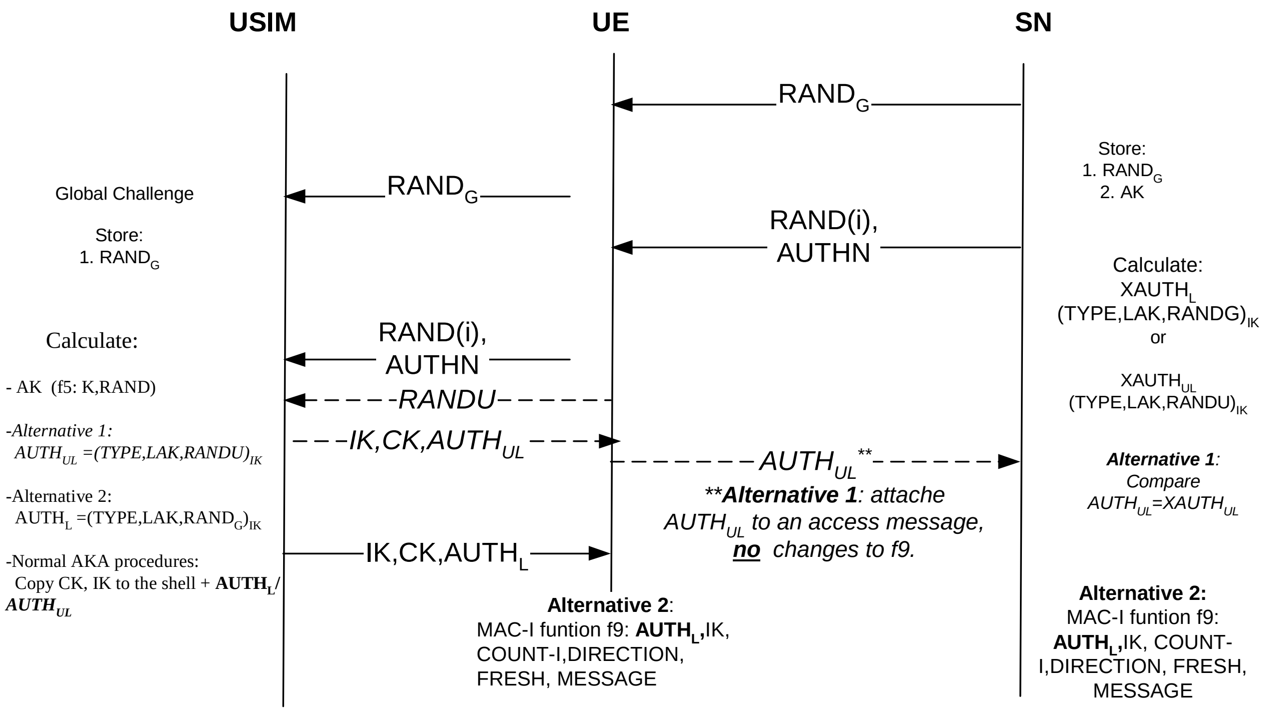

USIM
UE
SN
$RAND_G$
Store:
1. $RAND_G$
2. AK
Global Challenge
$RAND_G$
Store:
1. $RAND_G$
RAND(i), AUTHN
Calculate:
$XAUTH_L$
$(TYPE,LAK,RANDG)_{IK}$
or
$XAUTH_{UL}$
$(TYPE,LAK,RANDU)_{IK}$
Calculate:
RAND(i), AUTHN
- AK (f5: K,RAND)
RANDU
-Alternative 1:
$AUTH_{UL}$ $=(TYPE,LAK,RANDU)_{IK}$
IK,CK,$AUTH_{UL}$
$AUTH_{UL}$**
Alternative 1: Compare $AUTH_{UL}$=$XAUTH_{UL}$
**Alternative 1: attache $AUTH_{UL}$ to an access message, no changes to f9.
-Alternative 2:
$AUTH_L$ $=(TYPE,LAK,RAND_G)_{IK}$
-Normal AKA procedures:
Copy CK, IK to the shell + $AUTH_L$/ $AUTH_{UL}$
IK,CK,$AUTH_L$
Alternative 2:
MAC-I funtion f9: $AUTH_L$,IK, COUNT-I,DIRECTION, FRESH, MESSAGE
Alternative 2:
MAC-I funtion f9: $AUTH_L$,IK, COUNT-I,DIRECTION, FRESH, MESSAGE

Figure 1 Local Authentication Procedure – Global Challenge Local Authentication / *Unique Challenge Local Authentication*   (Based on the AK, IK values agreed at the last successful AKA procedure

5.3 Impact on the Present AKA Scheme and Nodes Functionality

Impact on the AuC (Authentication Center) is absolutely negligible.

- If LAK is calculated independently, the AuC shall calculate the 128-bit LAK, and deliver it to the SN.
- If LAK=AK, the AuC still computes the AK and XORs it with the SQN to generate the AUTN. The proposed enhancement will required that the LAK shall be delivered to the SN, in the clear, together with the Authentication Vector.

Impact on Network capacity is negligible: the LAK is transmitted, together with the Authentication Vector when the security association is established.

Impact on VLR/MSC functionality depends on whether or not the Serving Node supports the new proposed local authentication procedures. If those procedures are not supported, the additional LAK parameter in the received message is simply ignored. If those procedures are supported, both IK and LAK parameters are readily available to the VLR as parts of established Security Association, and additional minor computational functionality is expected. If alternative 2 is chosen, the additional computational functionality is negligible (i.e., need modification to F9 only, as described above).

The impact on the UE is minimal. If the mobile shell is designed to operate in the ANSI-41 environment with Serving Systems that support local authentication, than, in addition to the conventional 3GPP ciphering and integrity functionality, the shell shall be required to send the RAND_G or the RANDU to the USIM and:

If alternative 1 is implemented: attach returned AUTH_{UL} to the access message.

Else for alternative 2: the f9 (in the UE and the SN) shall be modified to include the AUTH_L as an additional input to the MAC-I function. If this alternative is chosen, the AUTH_L does not have to be attached to the access message. If the AUTH_L is not available (i.e., the USIM does not support the new enhance local authentication) the AUTH_L input will be null and the F9 output will be identical to the current 3GPP F9 output.

Impact on the USIM is minimal. It still computes the AK to recover the SQN from the AUTN, and IK is also available to occasionally compute the $\text{AUTH}_L/\text{AUTH}_{UL}$ as needed.

Both the USIM and the SN shall support the new F11 function.

6. CONCLUSION

The new enhanced integrity MAC function or the AUTH$_{UL}$ is unique for a user, and is based on the secret parameter, Local Authentication Key (LAK), not transmitted over the air and not known to the UE. Therefore, the removal of the USIM shall disable the UE, and no fraudulent network access by a rogue shell is possible.