3GPP TSG SA WG3 (Security) meeting #31 **S3-030693**

18-21 November 2003

Munich, Germany

Agenda Item: 6.6

Source: Orange

Title: More elements on the Special RAND mechanism

Document for: Discussion/Decision

1. Introduction

In SA3#30 plenary meeting, a Vodafone/Orange contribution introduced a mechanism to restrict the encryption algorithms with which a particular GSM or GPRS encryption key may be used. Some open issues were raised in the document and some concerns were raised about it. A liaison statement was sent to CN1 and CN4 in order to ask their opinion on some open issues.

This contribution aims at describing the use by an operator of this mechanism, discusses the extent of standardisation and proposes some answers to some of CN1 questions sent in LS S3-030668.

2. Use of the mechanism

When the mechanism was introduced in SA3#30, some companies raised objections about the lack of clarity on how the home operator would handle making a decision on which algorithms to allow and which to restrict.

We want to point out here that the mechanism can be used in a very simple way by operators to obtain protection for their customers. We envision different use cases that require varying degrees of complexity in the HLR/AuC to create the GSM triplets:

- An operator can restrict the use of this mechanism to its own network. Without much complexity (no large table of information needed), the operator can protect all the users in his own network and accept that roamers are susceptible to attacks. While this is not perfect, this provides some security to a large majority of the operator's customers (roamers being a small minority amongst the users).

- An operator can use the special RAND mechanism to introduce key separation between GSM and GPRS. When a request comes from a SGSN, the bits corresponding to the circuit-switched algorithms A5/0 to A5/7 can be all set to 0. This would in practice permit protecting GPRS networks from attackers exploiting weaknesses in A5/2 algorithm.

- In a more complex situation, the operator could maintain a table per roaming partner and create special RANDs from information contained in this table. This table would have to be filled with information obtained from roaming agreements. Note that in case of uncertainty about the algorithm used in a roaming partner's network, the operator can still fill the table as long as it knows which algorithms are NOT used by the roaming partner (for instance, an operator can forbid A5/2 and allow A5/1 and A5/3 if it knows for sure that A5/2 is not used in the partner's network, but does not know if the partner completed migration from A5/1 to A5/3).

While we agree that the third scenario involves more development in the HLR/AuC, we feel that the two first cases are valuable enough for an operator to be outlined here.

3 Extent of standardisation

The proposal for the special RAND mechanism requires in fact not many changes to the standard. In practice, what needs to be defined in the standards is the format of the special RAND, how it is to be interpreted by the UE, and what the UE behaviour should be when using this mechanism.

CN4 liaison statement S3-030669 informs S3 that they decided to propose a change request to release 6 of MAP to include requesting node identity to MAP. This will give more information to the HLR on how to create special RAND, giving easily accessible information about PLMN identity. CN4 also indicate that they do not think that using lower layer information to find out that requesting node identity is a good practice.

We agree that the standards certainly do not have to mandate such behaviour. However, we also feel that operators can decide whether to use such behaviour if they think it is worth it in order to implement the mechanism with networks not using MAP release 6. This does not impact interoperability and is just affecting the internal procedure within the HLR/AuC, and therefore does not need to be included in the standard.

Therefore, apart from the minor modification to MAP that permit to include PLMN identity in the request, we think that the behaviour of the HLR/AuC does not have to explicitly figure in the standards. The way operators create special RAND triplets has no impact on interoperability. We would suggest that information on how to create special RAND and how to use them is to be incorporated in GSMA documents and left out of the scope of 3GPP.

Therefore we feel that the amount of changes needed to include special RAND mechanism in the standard remains limited, and we propose in a companion contribution how to modify TS 43.020 in order to include the definition of the special RAND mechanism and how the security mechanisms are impacted (behaviour of the UE when ciphering is requested).

4. Questions raised by CN1

Below is an extract from the questions raised by CN1 and some proposed answers:

1) On the Gb interface it is possible to perform authentication and start ciphering with one procedure, by including both a RAND and an appropriate ciphering algorithm in the AUTHENTICATION AND CIPHERING REQUEST message.

If the authentication challenge is a UMTS authentication and the message contains:
- *both an authentication failure (MAC failure or Synch failure) and*
- *a ciphering algorithm that is not permitted according to the special-RAND information,*

which error takes precedence? Should the UE report an Authentication and Ciphering Failure to the network or should it diagnose a 'not permitted ciphering algorithm' first and skip the authentication?

While we do not have a strong preference, we feel it'd be more logical that the authentication error takes precedence as the 'natural' order is to authenticate then cipher.

2) If the GMM layer in the UE is required to treat the request for a 'not permitted ciphering algorithm' as an error, the UE should not return an AUTHENTICATION AND CIPHERING RESPONSE message. According to TS 24.008 (subclause 4.7.7.3), however, without receipt of an AUTHENTICATION AND CIPHERING RESPONSE message the SGSN will not start ciphering. I.e. the layer 2 failure mentioned in the above scenario will not occur.
CN1 noted that possible candidates for an explicit error indication by the UE to the SGSN would be the GMM STATUS or the AUTHENTICATION AND CIPHERING FAILURE message, but did not discuss this in detail.

This points out at a mistake that was done in the original special RAND contribution. While this is a CN1 issue to decide which error message is the most appropriate, we feel it is worth mentioning to CN1 that backwards compatibility is an important issue as the visited network may not be a release 6 network.

3) When it is proposed that the UE shall not start ciphering the uplink traffic at the LLC layer, what kind of traffic is the UE allowed to send in the uplink – signalling and/or user data, or none at all?

The UE can always send signalling messages that the standard allows to send in the clear (such as messages needed to establish a connexion). However, in case the UE does not start ciphering because of special RAND information conflicting with the algorithm requested by the network, the error message decided for question 2 should be used.

4) Finally, what is the expected UE reaction after detection of a 'not permitted ciphering algorithm' error?
- *Bar the cell, as in the case the network fails a UMTS authentication procedure (TS 24.008, subclause 4.7.7.6.1)?*
- *Deactivate all active PDP contexts?*
- *Perform a detach from the network?*
- *Or any combination of these measures?*

We do not have a strong position on this issue. Some companies in CN1 have pointed out that detach could lead to DoS attacks but our feeling is that there are other easier ways to perform such an attack. For the sake of consistency with UMTS, we have a slight preference for the cell barring.

5. Conclusion

We suggest that SA3 endorses the principle of limiting the standardisation work for special RAND to special RAND format and UE behaviour as the HLR/AuC internal procedure is out of the scope of 3GPP.

We also propose that additional information over the use of the mechanism is included into some GSMA document as recommendation to operators.

Lastly, we propose to use the basis of section 4 to discuss and draft a reply liaison to CN1.