3GPP TSG SA WG3 (Security) meeting #30 **S3-030651**

7-10 October 2003

Povoa de Varzim, Portugal

Agenda Item: 7.6

Source: Orange, Vodafone

Title: Further development of the Special RAND mechanism

Document for: Discussion/Decision

1. Introduction

In [S3-020463] a mechanism was proposed to restrict the encryption algorithms with which a particular GSM or GPRS encryption key may be used. The mechanism is based on the use of a "Special RAND" generated by the HLR/AuC and interpreted by the mobile. In this contribution we further develop the Special RAND mechanism and address some of the open issues identified in [S3-020463].

2. Overview of mechanism

2.1 General description

Use RAND to restrict the encryption algorithms with which an authentication vector may be used.

Here is an illustrative scheme; it should be understood that the exact numbers, lengths and coding is still up for discussion, but it is probably easiest to understand the kind of scheme we are suggesting by means of a concrete example:

- If bits 0–31 of RAND are equal to a particular "flag" string, then this is a "Special RAND"; otherwise everything is treated as it is today.
- In a Special RAND, bits 32–47 indicate which encryption algorithms the resulting K_C may be used with. Bits 32-39 indicate which of A5/0…A5/7 it may be used with, and bits 40–47 indicate which of GEA0…GEA7 it may be used with. For instance, if bits 0–31 are equal to the flag string, and bits 32–47 are equal to 00010000 00000000, then the resulting K_C may only be used with A5/3 — not with any other A5 algorithm, and not for GPRS encryption at all. A second example: if bits 0–31 are equal to the flag string, and bits 32–47 are equal to 11011111 00000000, then the resulting K_C may only be used over GSM circuit-switched, not over GPRS — and specifically not with A5/2.
- The HLR/AuC sets the algorithm restriction in the Special RAND based on the identity of the requesting visited network.

2.2 Timescales

To get full benefit from this mechanism we strongly recommend that all mobiles supporting A5/3 and/or GEA3 should also support this mechanism. It will prevent possible man-in-the-middle attacks which could completely undermine the increased strength of A5/3 by exploiting the lack of cryptographic separation between a K_C destined for use with A5/3 and a K_C destined for use with either A5/1 or, more importantly, A5/2.

It is proposed that this mechanism is specified as a mandatory feature in 3GPP Release 6.

2.3 Backwards compatibility

Suppose that the proposed scheme is specified as a mandatory feature in 3GPP Release 6, and implemented in all Release 6 mobiles.

Possible problems:

- The HLR deliberately creates a Special RAND, but the mobile is a pre-Release-6 one, and does not recognise the Special RAND as such. This will not cause a failure.
- The HLR does not know about Special RANDs, and by chance creates a RAND whose first 32 bits are equal to the flag string. This could lead to a call failure when ciphering is activated. But it will only happen with probability 2^{-32}, which is surely negligible compared to the other possible causes of call failure. It will not lead to an enduring inability to make calls.

3 Issues

3.1 Loss of Special RAND information associated with a Kc

In a Special RAND capable mobile it is conceivable that the Special RAND information associated with a particular Kc could be lost. In this case it is proposed that the mobile shall:

- set the Cipher Key Sequence Number (CKSN) to “111” in all messages including the CKSN sent from the mobile to the network, to indicate that no key is available. When the network receives a CKSN=“111” it shall be required to re-authenticate the mobile to generate a new Kc prior to establishing a new cipher mode [24.008];
- behave as if no Kc value was available in the mobile when a cipher mode command is received from the network without prior Kc update.

To avoid having to re-authenticate after every power off/on, it should be allowed for the mobile to store the Special RAND information for a particular Kc in non-volatile memory in the mobile. Kc and the corresponding CKSN is stored on the SIM rather than in non-volatile memory on the mobile. However, we do not believe that it would be beneficial to specify a new field on the SIM to store the Special RAND information alongside the Kc and CKSN, or more generally to make any modification to the SIM.

3.2 Error handling involving the mobile

3.2.1 GSM circuit switched

It should be considered what happens when a Special RAND capable mobile receives a CIPHER MODE COMMAND instructing it to start ciphering using an algorithm that is forbidden to be used with the current cipher key. It is proposed that the mobile treats this in the same way as other specified error cases where an invalid CIPHER MODE COMMAND is received by the mobile by returning a RR STATUS message with cause "Protocol error unspecified" [44.018]. After returning the message the mobile should then take no further action.

When the CIPHER MODE COMMAND indicates "start ciphering" the BTS starts deciphering with the requested algorithm immediately after having sent the CIPHER MODE COMMAND [43.020]. In the error case described above this will result in the connection being lost, so the BSS will send a CLEAR REQUEST to the visited MSC with a "radio interface message failure" cause value [48.008].

In summary no special error handling needs to be specified.

3.2.2 GSM packet switched

It should be considered what happens when a Special RAND capable mobile receives an AUTHENTICATION AND CIPHERING REQUEST instructing it to start ciphering using an algorithm that is forbidden to be used with the current cipher key. It is proposed that the GMM layer in the mobile treats this as an error case and does not start ciphering

uplink traffic at the LLC layer [24.008, 43.020]. Since the SGSN is expecting uplink traffic to be encrypted it will result in a layer 2 failure in the SGSN.

In summary no special error handling needs to be specified.

3.3 Error handling in the core network

Based on the proposals for error handling involving the mobile, the core network cannot distinguish between failed ciphering due to incompatible MS capabilities and failed ciphering due to restrictions imposed by a Special RAND. Nevertheless it would be possible for the core network to react to failed ciphering by indicating that the radio link failed due to a ciphering problem, deleting any unused authentication vectors and sending a new authentication vector request to the HLR/AuC. This may help the HLR/AuC determine that the Special RAND was set incorrectly for that particular visited network. While this might be useful in some scenarios[1] it does require new functionality to be implemented in the visited network. Furthermore, it is assumed that the Special RAND configuration will not change very often for a particular visited network, which means that any problems due to incorrect Special RAND setting could be dealt with during roaming testing, without the need for explicit error signalling in MAP. Therefore it is proposed not to introduce any special error signalling in the core network as a mandatory feature in Release 6. However, it should be left for further study as to whether or not special error signalling should be introduced as an optional feature.

3.4 Handover

In the GSM system specifications, no mechanism is specified to change the encryption algorithm during handover. Therefore no special procedures need to be defined to specify what happens if a handover results in a mobile being instructed to use an algorithm that is forbidden according to the Special RAND associated with the current cipher key.

4. Conclusions

Our analysis indicates that the Special RAND mechanism can be deployed without requiring any mandatory change in visited networks. This has the advantage that it would allow networks to protect their own subscribers without relying on enhancements to visited networks (which the visited networks might not be motivated to introduce with much urgency).

It is requested that

- SA3 adopt the proposals set out in this document as the basis for the development of corresponding 3GPP specifications
- other 3GPP groups are involved as appropriate to ensure that the specifications are developed within Release 6 timescales.

5. References

[S3-030463] 3GPP Tdoc S3-030463: Cipher key separation for A/Gb security enhancements, Vodafone, SA3#29, 15–18 July 2003, San Francisco, USA.

[24.008] 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols; Stage 3

[43.020] 3GPP TS 43.020: Network related security functions

[44.018] 3GPP TS 44.018: Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol

[1] Consider the scenario where a visited network upgrades his BSS from A5/1 to A5/3 and some time later the home network sets Special RAND to prohibit the use of A5/1. If the visited network then has to rollback the BSS software to the previous version (not necessarily because of encryption problems) then it would result in roamers from the home network being unable to make or receive encrypted calls in the visited network.

[48.008] 3GPP TS 48.008: MSC-BSS interface: layer 3 specification