3GPP TSG SA WG3 Security **S3-030463**

15 – 18 July 2003

San Francisco, USA

Agenda Item: 7.5

Source: Vodafone

Title: Cipher key separation for A/Gb security enhancements

Document for: Discussion/Decision

1. Scope

In [S3-030361] Ericsson propose an approach for secure algorithm negotiation for the Gb interface. The mechanism seems equally applicable to the A interface.

We point out a limitation of Ericsson's proposed approach. We suggest an alternative approach, which we believe achieves a greater practical security enhancement. We recommend its application to both A5 and GEA encryption.

Acknowledgement: the alternative approach presented in this contribution is based on a suggestion made by France Telecom.

2. A limitation of Ericsson's proposal

Ericsson — correctly, we think — judge that it is not feasible for the home network to inform the USIM OTA of the visited network's capabilities whenever the mobile roams onto a new visited network. Instead, the USIM is equipped with a table of the capabilities of all possible visited networks, and chooses a value from this table based on the identity of the visited network.

Unfortunately, this approach is vulnerable to a man in the middle attack, where the attacker masquerades as a network that does not support secure algorithm negotiation. The user is not likely to notice if an unexpected visited network identity appears briefly on his screen.

3. An alternative

3.1 Overview

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 CS, 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. It is for further study to determine how the HLR/AuC determines this identity from the authentication vector request.
- It is up to the mobile equipment to enforce this restriction. If the restriction results in the cipher mode command being rejected then the use of new or existing error codes may need to be standardised. This may be needed so that the network can determine the reason for failed ciphering due to the HLR/AuC setting the algorithm restrictions incorrectly.
- The mechanism assumes that algorithm restrictions should be applied equally across a single operator's domain. It is not clear whether information about the restriction on the use of a particular K_C has to be communicated between operators (e.g. to support inter-operator handover).
- A preliminary analysis suggests that the mechanism can be deployed without requiring any change in visited networks. This would be a great advantage, since 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). However, if minimal changes to the visited network are found to be useful for the reasons outlined in the previous three bullet points, then they should be introduced as far as possible as additional options rather than as a prerequisite for the introduction of the mechanism.

3.2 Backwards compatibility

Suppose that the proposed scheme is specified as a mandatory feature in 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.

3.3 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.

4 Conclusions

It is proposed that the mechanism outlined in this document is considered as a candidate solution for enhancing A/Gb security.

5. References

[S3-030361] Ericsson: Enhanced Security for A/Gb, S3#29, 15 – 18 July 2003, San Francisco, USA