3GPP TSG SA WG3 Security - S3#36 **S3-040983**

23 - 26 November 2004

Shenzhen, China

Title: **Adoption of key separation for GSM/GPRS in the short term**

Source: **Orange**

Document for: **Discussion and Decision**

Agenda Item: **6.6**

Work Item: **GERAN Security**

1 Introduction

Several countermeasures against BBK attack [Bark] have been discussed in SA3. Among them, removal of the mandatory support of A5/2 in the handsets, which has already been agreed by SA3, and key separation between the different GSM/GPRS encryption algorithms. Special RAND mechanism which has been the working assumption for about one year allows introducing some key separation (which can also be considered as a long term enhancement) in the short term. Authenticated Ciphering Instruction also provides key separation but it is not on the same timescale as Special RAND as it requires all GSM networks to be upgraded before the first upgraded terminals can be issued.

A new work item is proposed to provide long-term security enhancements to protect GERAN Access Network in the future [S3-040790]. One of the key issues is whether key separation should be handled together with the other long-term security enhancements mentioned in the proposed work item or whether this should be handled in the short term. The present document recommends adopting a key separation mechanism in the short term.

2 Discussion

Scenario 1: Key separation is not introduced in the short term but included in long term security enhancements.

If we remove A5/2 and then only focus on the long term we will leave for years a security flaw in the encryption algorithms negotiation protocol. However, the limited protection offered by the A5/1 algorithm will gradually become insufficient, so A5/1 will become the next weak point of GSM security after A5/2, but due to the unsolved security flaw in the protocols, the introduction in terminals (planned for release 6) of the stronger security algorithms A5/3 will be almost useless. As a matter of fact terminals with A5/1 and A5/3 capabilities will be vulnerable to simple variants of the BBK attack scenario exploiting known cryptanalyses of A5/1, even in the networks of operators who would make the investment of implementing A5/3 in their PLMN.

More precisely, if the existing flaw of the algorithm negotiation protocol is not removed using a realistic key separation mechanism, e.g. Special Rand, future terminals with A5/1 A5/3 capabilities will remain vulnerable to eavesdropping attacks against their A5/3 communications, where the adversary records an A5/3 communication, and later on triggers A5/1 encryption with the same encryption key Kc using a false base station, recovers Kc based on the analysis of the first encrypted signalling block received from the mobile, and decrypts the A5/3 communication using

the recovered value of Kc. There are other eavesdropping scenarios (where the victim is kept in unciphered mode) but in the case described here, eavesdropping could not be detected even by handsets implementing the ciphering indicator.

Scenario 2: Key separation is introduced in the short term and additional long term security enhancements are introduced in a second step.

- The advantage of this scenario is that if the introduction of key separation is done in the short term, it can prevent that vulnerabilities spread from A5/1 to A5/3 from the beginning of the introduction of A5/3. It would also be in accordance with the recommendation made by GSMA Security Group in the LS [S3-030490] (September 2003) to introduce a key separation mechanism together with A5/3 introduction. "*Having considered the matter at its last meeting, in the light of the new attacks that have recently been presented on GSM ciphering, SG came to the conclusion that it should be a priority to introduce a mechanism that separates keys for use with different encryption algorithms. For this reason SG wishes to express that the introduction of such a key separating mechanism should be aligned with the introduction of A5/3.*"

As all the proposed solutions require upgrading the handsets, in order to protect the maximum number of users, it is better to introduce the key separation mechanism in the handsets as soon as possible (and it makes sense to introduce it at the same time as A5/3). We cannot wait until the threat is implemented to begin to renew the handsets in the field.

- It is true that this scenario leaves the possibility that the long term solution provide another key separation mechanism different from the one decided in the short term. However, this is not necessarily a drawback.

For instance, special RAND (the only short term key separation mechanism discussed in SA3 to our knowledge) could be selected in the short term and Authenticated Ciphering Instruction in the long term. It can be noticed first that Special RAND is optional for the operators to deploy, so if they wish they may only wait for the batch of long term enhancements to deploy a mechanism. Also, adopting special RAND in the short term does not prevent from implementing Authenticated Ciphering Instruction in the long term. Besides, Authenticated Ciphering Instruction and Special RAND do not exclude each other: they can live together.

- This scenario would not contradict IREG principles about deployment of new mechanisms expressed in [S3-040826] in the context of SMS fraud countermeasures: "*IREG also desires to have designs which can be implemented in a staggered manner by operators, so as to provide immediate protection to those operators who implement early. Conversely any mechanism which requires all bodies to install before any security uplift can be achieved would fail to achieve success.*"

3 Conclusion

As a conclusion, we think that the removal of A5/2 is a useful but insufficient short term countermeasure against the BBK attacks, and that a key separation mechanism between GSM/GPRS encryption algorithms (namely special RAND) should be introduced as soon as possible in the short term, at the same time as the introduction of A5/3 in terminals. Therefore, we suggest that SA3 agree on the need of the key separation mechanism in the short term and adopt special RAND mechanism.

It should also be highlighted that this decision does not prevent to continue the long term global work proposed in the work item on "Access Network Security Enhancement".

4 References

[Bark] E. Barkan, E. Biham, N. Keller: “Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication”, In D. Boneh (Ed.): Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings. Lecture Notes In Computer Science Volume 2729, Springer 2003, pp600-616

[S3-030490] 3GPP SA3 Tdoc S3-030490: "LS (from GSMA-SG) on introduction of A5/3 in GSM handsets", SA3 meeting #30, Povoa de Varzim, Portugal, 7-10 October 2003.

[S3-030588] 3GPP SA3 Tdoc S3-030588: "Further development of the Special RAND mechanism", SA3 meeting #30, Povoa de Varzim, Portugal, 7-10 October 2003.

[S3-030693] 3GPP SA3 Tdoc S3-030693 "More elements on the Special RAND mechanism", SA3 meeting #31, Munich, Germany, 18-21 November 2003.

[S3-040528] 3GPP SA3 Tdoc S3-030528: "Analysis of the countermeasures to Barkan-Biham-Keller attack ", SA3 meeting #34, Acapulco, Mexico, 6-9 July 2004.

[S3-040529] 3GPP SA3 Tdoc S3-030529: "Proposed CR to TS 43.020 : Introducing the special RAND mechanism as a principle for GSM/GPRS ", SA3 meeting #34, Acapulco, Mexico, 6-9 July 2004.

[S3-040745] 3GPP SA3 Tdoc S3-030745: "Key separation mechanism in GSM/GPRS", SA3 meeting #35, St Paul's Bay, Malta, 6-9 October 2004.

[S3-040790] 3GPP SA3 Tdoc S3-030790: "Proposed WID: Access Network Security Enhancements ", SA3 meeting #35, St Paul's Bay, Malta, 6-9 October 2004.