3GPP TSG SA WG3 Security **S3-030754**

18~~6~~th – 21st November, 2003

Munich, Germany

Agenda Item:

Source: Ericsson

Title: Enhancements to GSM/UMTS AKA

Document for: Discussion

1. Introduction

This document discusses the enhancements to key management for GSM and UMTS presented at SA3#30 and presents some thoughts on ways to combine them and further possible benefits of introducing a key separation mechanism.

2. Background

The special RAND proposal in [1] enables home control of allowed ciphering algorithms in the terminal. This is a flexible method to block the use of known insecure algorithms. In [2] we presented a key separation mechanism which counters attacks based on the fact that in GSM the same key can be activated for different algorithms. There we also presented further enhancements to the GSM AKA procedure in that the RAND may be MAC'ed and contain a sequence number giving simple network authentication and replay protection.

3. Solutions

The solutions discussed in connection with the attacks described in [3] can be categorized as

1. Blocking the use of specific algorithms. This can be achieved with the special RAND mechanism. This method is only effective if the compromise of an algorithm has become public knowledge so that its use can be blocked.

2. Prohibit reuse of RANDs. This requires replay protection and network authentication. It does however not protect against an active man in the middle attack using a weak algorithm as a "key-retrieving oracle".

3. Key separation. This gives protection against all weak algorithm "key-retrieving oracle" attacks, known or unknown. It can however not protect against the use of known weak algorithms.

We note that the intended use of the special RAND mechanism is really just to protect against attacks using weak algorithms as "key-retrieving oracles" as operators are in control of which algorithms that are allowed and used in their networks. Thus 1. and 3. above are competing solutions while 2, in the presently considered attack scenario, only would counter attacks in which traffic first is recorded and later the weak algorithm "key -retrieving" attack is performed by a false base station.

4. Discussion

4.1 Special RAND

The special RAND method is self-contained, doesn't require user involvement but can only be used to block specific algorithms. Its relative simplicity is its main merit along with the fact that it is very simple to introduce. Operators may use old AuCs in parallel to updated ones and thus have a gradual introduction of the feature. However, if we want to achieve more the special RAND proposal could be modified and extended. Below follows descriptions of a few possible extensions together with security gains and systems consequences:

The first modification proposal is to shorten the homing sequence, i.e. the sequence distinguishing the special RAND, and replace it with a MAC. The special RAND would then be recognized if the MAC can be verified by the terminal. Two advantages are achived, the first one being that a MAC doesn't, from a computational point of view, remove the same amount of "entropy" from the RAND as a static homing sequence. Secondly, the MAC would also give Network Authentication. This modification would increase the computational load in the AuC and the terminal as two key calculations would be required.

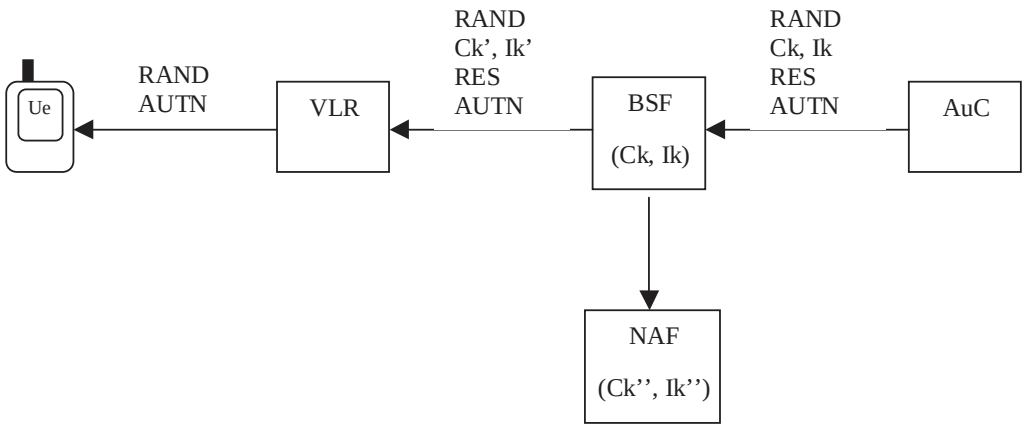
The second proposal is to include a replay counter in the special RAND. Here we need to assume that also a MAC of the special RAND is introduced. The replay counter has to be handled in the ME and of course it cannot give the same protection as UMTS AKA, but it would still protect against most attacks that a user, not changing terminal very often, would experience. We also note that a terminal certainly can handle a replay counter in a very flexible way as memory restrictions aren't that severe.

The third change considered is to let the special RAND always include information about which algorithms that are allowed. Users with new terminals getting their RANDs from updated AuCs would then have the feature enabled while users associated with old AuCs need to disable the feature. This configuration could be done by the user, by OTA or be preconfigured in the phone. This would in principle give group-wise key separation between allowed and not allowed algorithms. This proposal could also be combined with the replay counter and MAC proposal.

4.2 Key separation

Our proposal to introduce a general function for key separation in the terminal admittedly require more changes in the terminal and in the network. But it also offers greater possibilities and it might be seen as a more long-term solution and not a quick fix. To support this view we would like describe a possible use case related to GBA.

Assume that the key separation mechanism isn't only used to separate keys between encryption algorithms but also to derive other service specific keys. One such service specific key might be a key shared between the BSF and the terminal. Another key could be for WLAN access and a third for presence. However, to guarantee home control an additional layer of key separation is required as indicated in the figure below. The primed and double primed keys are derived from the original data coming from the AuC by application of a key separation function. The figure below shows this idea in a UMTS setting. One immediate conclusion is that there is no need for a separate authentication to load the BSF in GBA with the required keying material.



When quintets are delivered from the AuC they are first passed to a node, here called BSF, which stores the keys in the quintet together with a hash of it and the identity of the "user". The hash will serve as a reference to exactly this quintet for the given user. The BSF then applies a key separation function using a service name, which could be UMTS authentication as differentiation.

5. Conclusions

The special RAND proposal is a relatively simple mechanism to protect against the A5/2 attack when stronger algorithms are available for use. We have shown how this solution can be improved and also extended to protect against

other attacks. The key separation mechanism is more generic and has wider applicability. It might be seen as a more long-term solution.

As the A5/2 attack has opened up a discussion on GSM security and triggered ideas on how it can be improved our conclusion is that to resolve the question which security improvements we really need we should develop both a short-term and a long-term requirement specification. If the conclusion in the specifications is that we need more extensive protection we should open up general improvements facilitating new and simple security solutions like the general use of a key separation mechanism.

6. References

[1] S3-030588, Further development of the Special RAND mechanism

[2] S3-030542, Enhancements to GSM/UMTS AKA

[3] Elad Barkan, Eli Biham and Nathan Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Proceedings Crypto2003, Springer LNCS 2729.