3GPP TSG SA WG3 Security **S3-030542**

6th – 10th October, 2003

Povoa de Varzim, Portugal

Agenda Item: 7.6

Source: Ericsson

Title: Enhancements to GSM/UMTS AKA

Document for: Discussion

1. Introduction

This document suggests enhancements to improve key management for GSM and UMTS to limit the impact of the breaking and A5/2 and future attacks on other algorithms.

2. Background

The breaking of A5/2 as described in [1] together with the described active man-in-the-middle attack exploit flaws in the security system design principles in GSM, caused by the somewhat different threat model that existed at the time GSM was designed. One specific and important flaw is to use the same ciphering key to key different ciphering algorithms. While currently not posing a threat, we note that also UMTS has the same property. If different keys were used for different algorithms then the damage of the described attack would have been limited to the breaking of the A5/2 algorithm. Furthermore the seriousness of the design error is increased by the fact that there is no protection of reuse of a key in GSM (which can be achieved by replay of the AKA procedure, i.e replaying the RAND).

It is worth noting that the A5/2 attack and the publication of GEA3 makes an attack on GPRS security possible when this strong algorithm is used while the probably weaker but not publicly known algorithms GEA1 and GEA2 still provide some security, somewhat of a “paradox”.

3. Enhancement proposal

Conceptually, we propose to introduce three new GSM algorithms A5/1’ to A5/3’ which are identical to A5/1 to A5/3 with the only difference being a cryptographic, algorithm dependent pre-processing of the keys. Put differently, we propose the introduction of a post processing of the keying material produced in the standard AKA procedures for GSM and AKA to produce algorithm dependent keys. An example procedure for GSM AKA is

Kc’ = GSM_Modify (Kc, RAND, Algo_Id)

and similarly for UMTS

Ck’ = UMTS_Modify (Ck, RAND, Algo_Id),
Ik’ = UMTS_Modify (Ik, RAND, Algo_Id)

where the GSM_Modify ( ) and UMTS_Modify ( ) functions are cryptographic functions that we propose can be based on SHA1, by truncating it to the left-most 64/128 bits respectively. (In the UMTS case one can also use some function that takes both Ck, IK as input and produces 256-bit outputs.) The Modify functions should be considered pseudo-random functions, and in particular be one-way. RAND is introduced to make pre-calculation attacks infeasible.(Some optional “other_context_info” may be introduced as input if other types of attacks can be identified, but seems not needed at the moment.)

The idea is that new terminals always should apply this postprocessing procedure while the network should be allowed to support old terminals. To make this possible it is necessary to agree on how new terminals should signal their capabilities. There are two ways: The first is to introduce new algorithms and let the post processing be part of the algorithm identity. In GSM/GPRS this would correspond to the introduction of A5/1’, A5/2’, A5/3’, GEA1’, GEA2’ and GEA3’. That is, A5/x’ is the same algorithm as A5/x, but with the above described key-processing. The second

alternative would be to signal this in some more general terminal capability info. Since GSM is specified to support up to eight algorithms, the simplest way, however, seems to be to let A5/j, j = 5, 6, 7, denote A5/1' to A5/3' respectively, which would allocate three of the remaining GSM algorithm identifiers. We do similarly with the GEA algorithms. Concerning the 128-bit algorithms A5/4 and GEA4, we for the moment do not see a need for additional variants of these, since they are assumed to be very strong and would anyway require distinct keys from a new 128-bit key-derivation function, e.g. GSM Milenage.

Thus to introduce this scheme the postprocessing procedure together with the way to signal that a terminal supports it have to standardised. Here we note that it is probably only needed to define new identifiers in already existing protocols so the standardisation effort will be very limited and could be quick.

The postprocessing of the AKA output need to take place in the terminal and the SGSN/VLR.

It is important to note that the "Modify" functions are internal to the new (e.g. A5/x') algorithm specification. Thus, the algorithm is from the outside treated as a black-box, whose only difference (e.g. to A5/x) is a few extra input parameters. For instance, in a UMTS to GSM handover, there needs to be parameter conversion. This would take place "as usual":

1. convert UMTS (Ck, Ik) to GSM Kc (according to TS 33.102, Sect 6.8)
2. convert UMTS RES to GSM SRES (dito, but not essential to our proposal)
3. Input Kc, RAND,… etc, to A5/x' (or Kc to A5/x, if the old version algorithm is to be used).

In some cases, when GSM/UMTS AKA is not re-executed, the ME may need to save the most recent RAND values to be able to re-start ciphering with the new A5/x' version algorithm. Notice that the UE/network also needs to store the RAND in UMTS access, in case a hand-over or inter-system change takes place to GSM access, so that the UE can run the appropriate Modify function before starting encryption in GSM access.

3.1 Security considerations

Reasonable cryptographic assumptions on the "Modify" functions imply that breaking A5/x' (x = 1, 2, 3) does not affect the security of A5/y', $y \neq x$, or any of the old A5/x algorithms. The proposal does not increase the security of the algorithms as such though, e.g. A5/2' can still be broken, but the "key material" obtained is not useful to attack any of the other algorithms.

Note though that until networks have been upgraded, there will still be legacy networks only supporting the old algorithms. Hence, it could still be possible for a resourceful attacker to proceed as follows:

1. Record an A5/x' encrypted session.
2. Using the false base station, trick the UE into running A5/2 with the same RAND (and Kc).
3. Break A5/2 and use the obtained Kc (and RAND) to obtain Kc' by running GSM_Modify "forwards".

Attacks of this form seem generally unavoidable as long as A5/2 is allowed to co-exist in the networks.

3.2. Other enhancements

While up for discussion, some other enhancements might be considered, albeit of larger impacts to network and terminals. For instance, it could be possible to upgrade GSM security with some basic network authentication. This could be achieved will small changes by encoding information into RAND. E.g. let R be an 80-bit random value, let c be a 16-bit counter and let k be a key derived from GSM AKA applied to (a padded) R || c. Now use the 128-bit RAND value

RAND = R || c || MAC(k, R || c)

to generate Kc and RES. Here, MAC(,) is a 32-bit message authentication code which serves similar purpose to UMTS's AUTN and c is similar to SQN.

3.3 Co-existence with other proposals

Before the attack by Barkan et al. was presented, some suggestions for GSM/GPRS security improvements (on the A/Gb interfaces) had already occurred in 3GPP, see [2,3]. As far as we can tell, the proposal(s) outlined above can (be made to) co-exist with these earlier proposals, and there may be reason to look into if the solutions together can improve the security further. For instance, while both of the proposals [2, 3] do enhance various security aspects, neither of them provides desired key-separation: if algorithms “X” and “Y” are both allowed and supported, then the UE can potentially still end up running both “X” and “Y” with the same key Kc.

4. Conclusions

We have introduced a simple enhancement to the security in the GSM and UMTS AKA procedures. For GSM, it provides security against existing, rather serious attacks. The proposed solution fits nicely into the existing protocol framework and has limited implementation consequences which makes a rapid deployment possible.

5. References

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

[2] Vodafone, “Cipher key separation for A/Gb security enhancements”, S3-030463, S3#29, 15 – 18 July 2003, San Francisco, USA.

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