3GPP TSG SA WG3 Security — SA3#33 **S3-040341**
10-14 May 2004
Beijing, China

Source: **Ericsson**

Title: **Comparison of Suggested A5/2 Attack Countermeasures**

Document for: **Discussion**

Agenda Item: **GERAN**

1 Introduction

Since the August 2003 publication of the Biham et al. attack on GSM A5/2, a number of countermeasures have been suggested. The purpose of this short analysis document is to compare what the respective solution really provides in terms of security, what issues there are, and how the respective "fix" affects the network.

2 Overview of Proposals

The proposals considered are

- Special RAND (Vfe/Orange S3-030588,… etc).
- Enhanced A/Gb (Ericsson, S3-030361, proposed enhancement to Gb)
- Integrity protection of alg selection (Brookson, S3-040036)
- Key separation (Ericsson, S3-030542, …etc)
- Disabling A5/2 in the handset

We shall omit details of these, since we assume the reader is familiar with them.

3 Comparison

The table below shows what security issues the respective proposal can handle (OK or NOT OK). We also write "DoS" when no privacy compromise is achieved by the attacker, but rather a denial-of-service, e.g. causing network/terminal using into different ciphering algorithms, etc. Note: as DoS attacks, we only consider ones that may go unnoticed by the ME/network and that are "related" to the A5/2 problem and the suggested solution. E.g. if the attacker modifies an added integrity protected message, we shall not consider this DoS. While the communication may still fail in this case, it will fail gracefully, as the attack is detected. Similarly, modifying the ME's RES may also be possible, but is really something which is independent of the A5/2 problems, and by the same reasoning is not considered DoS in this context.

The potential threats are:

- Eavesdropping on A5/2 (passive attack)
- Eavesdropping on A5/x (x =1 or 3) by attack on A5/2 (passive-then-active attack using a first passive record-phase, then an active attack to fool UE into using A5/2 with the same key)
- Man-in-the-middle, active-then-passive, residing between UE and BTS (eavesdropping in real-time as effect of active "bidding down" attack on algorithm selection). It is assumed that no other active actions are taken besides the bidding-down in this case.
- WLAN, potential side-effects on WLAN security by key re-use between the two systems. Note that some of the solutions, if introduced in WLAN access, can conversely also mitigate WLAN-against-GSM-attacks, see below.

· MITM2: An “up-link active” MITM, can modify any messages on up-link, but up-link only (e.g. signaling of UE capabilities to give the impression the UE does not “know” any algorithm except A5/2).

· MITM3: Conversely, a “down-link active” MITM, e.g. can claim “the access network does not know the new feature”.

· MITM2 + 3: combination of these two (the most powerful attack).

The last three rows in the table indicate:

· which part of the network “controls” the security,

· which nodes/protocols are affected,

· whether there is a need for a “deadline” when all networks/terminals need to be assumed to be updated to achieve “full” security.

Disclaimer: we do not make any claims about the complete exhaustion of all possible attacks.

Threat	Special RAND	Integrity of algorithm selection	Enhanced A/Gb	Key separation	A5/2 disable
Eavesdropping on A5/2	NOK	NOK	NOK	NOK	OK
A5/1 attack by A5/2 attack	OK	OK	OK	OK	OK
MITM	DoS	OK	OK	DoS	OK
WLAN	OK*	OK**	OK	OK*	OK
MITM2	DoS[1]	NOK[2]	OK[3]	DoS[4]	DoS
MITM3	DoS[5]	DoS[6]	DoS	DoS	DoS
MITM2+3	DoS[5]	NOK[7]	NOK[7]	DoS[8]	DoS[9]
Control	Home	Visited	Home/Visited	Visited	User
Affects	ME AuC MSC MAP-signal.	ME BTS	UE SGSN	ME MSC/VLR SGSN	ME
Deadline	No	Yes	Yes	Yes	No

1 If the MITM claims the UE only supports algorithms that have "RAND-bit = 0" (the only interesting case), ciphering will fail.

2 By claiming support of only A5/2, this will cause network to use A5/2, so integrity of that algorithm-choice does not help.

3 OK, because later integrity check will fail in the UE (in this solution, the network will eventually return a protected version of the list of algorithms that the UE "offered" in this phase).

4 If attacker removes indicated support for A5/x' in the UE, the network will propose some other algorithm. Unless this is A5/2, we are fine. (we assume A5/2 is never proposed by a network who knows A5/1). Not even this may be a threat, e.g. if updated MEs refuses to use old algorithms, it becomes just DoS.

5 The bad thing that can happen is if RAND bits are flipped, but then auth will fail.

6 If MITM claims network is "old" and strips auth tag, nothing bad will happen unless he also changes the algorithm selection the network made. However, then ciphering will be done by different algorithms, DoS.

7 The attacker claims network is not updated, and also claims the UE only supports A5/2

8 The attacker claims UE only supports A5/2'. This will, even if the network is updated, force use of A5/2', which can be eavesdropped.

9 DoS seems to be all that can be accomplished Thus, all that is accomplished by the attacker is either choice of different algorithms, or, no matching algorithms can be found.

3.1 Discussion

3.1.1 Special Rand

We have previously raised concerns that some "bad" A3/A8 implementations (perhaps COM128) would suffer security-wise from loss of entropy in RAND. This is FFS. Even a "good" A3/A8 slightly suffers resistance against off-line pre-computation attacks since the security of the SIM key Ki becomes slightly less than 128 bits in that case.

For WLAN use we need to assume that some version of the Nokia proposal is introduced and signaling of the "access type" to the home network can be done. Special RAND requires that the SIM is in a ME that is "aware" of special RAND (see note * in the table above). Also, in that case the terminal must be free of Trojans etc.

One issue is which granularity the home network can use when deciding where and when to not allow the use of A5/2. As we argued above, some UE may not support A5/1, so this cannot be taken for granted (though there are probably quite few such UEs).

3.1.2 Integrity for algorithm selection

The scope of S3-040036 is a bit unclear and leaves open some questions.

There is for instance some questions about which key to use for the MAC. E.g., if integrity is applied to more than just the algorithm selection message, this proposal should in addition use key separation so that a separate key, distinct from Kc is used for the integrity. Otherwise the MAC key can be retrieved by breaking A5/2, and subsequent MACs can be forged. Thus, use of Kc should only be allowed if the algorithm selection is the only MAC:ed message.

Note that our understanding is that the protection is on the message from the network to the UE. Thus, this solution does not solve the "MITM Signals that only A5/2 is supported in ME" attack, unless further integrity is added.

Moreover, this proposal would benefit from adding some policy decision taken on top of the basic protection, e.g. UE does not allow hand-over to A5/2 from A5/1 network, since this could open up key-recovery attacks similar to that mentioned above. (This can of course also be an issue for other proposals.)

The solution can avoid using A5/2 in an insecure way, thereby mitigating some threats against WLAN. However, unless the same level of algorithm protection is present in WLAN, a weak WLAN algorithm might affect the security of GSM (**).

The proposal can be said to be a simplified version of Ericsson's earlier Gb/A enhancements (S3-030361).

3.1.3 Enhanced A/Gb

This has properties similar to S3-040036, but has the non-negligible advantage that it protects the whole algorithm negotiation. Hence, it solves the "MITM Signals that only A5/2 is supported in ME" attack. While the control (policy issuing) is from the home network, one still has to rely that the visited network is updated.

3.1.4 Key separation

For WLAN use, just as in the case of special RAND, the terminal must of course be made "aware" of performing key separation and be free of Trojans (*).

3.1.5 A5/2 disable in UE

We note that disabling A5/2 is (as can be expected) perhaps the most "foolproof" solution. It is of course also the only fix that will remove the treat of eavesdropping on A5/2. Of course, it does not protect against possible future flaws in A5/1 etc.

4 Conclusions

Disabling A5/2 is the only bulletproof solution. We believe that regardless of what solution is chosen, on a long term, A5/2 disabling should be introduced. Of course, it does not protect against future A5/1 weakness etc.

Special RAND and key separation seem to achieve similar security. Special RAND allows more home control, and in some cases means to detect an active attack, but on the other hand, requires new signaling from Visited Network. There is a slight risk that special RAND introduces new security issues by reducing randomness. The security of key separation is better understood.

S3-040036 seems like a promising idea, but SHOULD be enhanced by key-separation (at least for the MAC key) and some hand-over policy enforcement in UE. The UE needs to be made aware which algorithms are secure and which are not. If this solution is selected, one should probably investigate if there is a need/possibility to protect also other messages.

Most of the proposals that rely on updates to the visited access network require some deadline at which terminals can be sure all networks have been updated. Otherwise, bidding down attacks by MITM seems to exist.