3GPP TSG SA WG3 Security — S3#34 **S3-040528**

July 6 - 9, 2004

Acapulco, Mexico

Source: **Orange, Nokia**

Title: **Analyse of the countermeasures to Barkan-Biham-Keller attack**

Document for: **Discussion and Decision**

Agenda Item: **GERAN Security**

1. Introduction

Several countermeasures have been discussed in SA3 to counteract Barkan-Biham-Keller attack.

Evaluations of the mechanisms to protect against Barkan-Biham-Keller attack were provided by other companies in [S3-040263] and [S3-040341].

The following paper discusses the alternatives and proposes to select the Special RAND mechanism.

2. Comparison

The main countermeasures to Barkan-Biham-Keller attack that have been discussed in SA3 are:

- A5/2 removal
- Timing analysis
- Special RAND
- Authenticated ciphering instruction

Withdrawing A5/2 from the networks and the terminals as soon as possible is a part of the solution but is not sufficient : A5/1 or the weakest GPRS algorithm GEA1 would become the next target on the list, and the introduction of the strong algorithms A5/3 and A5/4 would be meaningless if the protocol weakness of GSM (lack of key separation) is not repaired at the same time. Timing analysis is also not sufficient.

Both the Special Rand and the Authenticated Ciphering Instruction are mechanisms intended to introduce a form of key separation between encryption algorithms in future GSM mobiles, that would protect against the attack in the long term. One of them should be selected by SA3.

In the following table, we describe the main comparaison elements between the special RAND and the Authenticated ciphering instruction :

	Special RAND	**Authenticated ciphering instruction**
Protection against [Bark] A5 attack	Yes	Yes
Applicable to GPRS ?	Yes	Assumed but no description provided till now and impact unknown.
Impacted elements	ME, AuC/HLR	ME, BSS

	MSC/VLR and SGSN can be impacted if *PLMN ID* need to be added in MAP messages but this is not mandatory to be able to deploy the mechanism.	MSC impacted to mandate cipher mode command, MSC should not be impacted by classmark3 modification according to [S3-040262]. (U)SIM would be impacted if the mechanism described in annex of [S3-040262] was selected. If applied to GPRS then at least SGSN is impacted.
Impacted protocols	None : only the semantic of RAND is modified. MAP can be slightly modified if *PLMN id* field is needed in MAP messages but this is not mandatory to be able to deploy the mechanism.	Radio protocols impacted : classmark 3 extended, MAC added to ciphering mode command.
Deployment constraints	None	ALL the visited networks need to be upgraded before the first upgraded mobiles can be released. New MEs are not backward compatible with old networks.
Control of the implementation of the mechanism	Home network	Visited Network
Domain separation (GSM, GPRS, WLAN …)	Yes	No
Bidding down protection	Partly	Yes
False base station eavesdropping	No	Protection against certain attacks (see [S3-040263])

3. Discussion

Special RAND

The special RAND mechanism consists in using spare bits of the authentication challenge RAND (the length of RAND is 128 bits, whereas 80 truly random bits are more than sufficient as confirmed by ETSI/SAGE, 64 bits being a minimum) to indicate to the MS that the special RAND feature is to be applied and which encryption algorithm(s) the MS is authorised to use in combination with the resulting encryption key Kc. (see [S3-030588] for more details)

This solution has the following advantages:

- Modifications are restricted to the HLR and to the mobile terminals (MSC/VLR and SGSN can be impacted but this is not mandatory to be able to deploy the mechanism).
- No modifications are needed in the protocols. Only the semantic of the parameter RAND (and the way RAND is generated in the HLR and interpreted in the MS) is modified.
- Backward compatibility and interoperability issues (new MS-old HPLMN; new HPLMN-old MS; new HPLMN-old VPLMN) are well taken into account: a modified terminal supporting the special RAND mechanism can accept to process RAND values whether they contain or not the binary pattern indicating they are special RAND values, and the introduction of the mechanism by a particular operator does not

depend on development to be done in VPLMNs. Therefore the mechanism need not to be introduced at the network side in a phased way, but at any point in time at the discretion of each individual operator.

- Separation of domains (GSM, GPRS, WLAN but possibly others) can be ensured: the derived key can be used only in a certain context. Then, vulnerabilities cannot spread from one context to another. For instance, if an attacker retrieves a triplet in WLAN environment, he cannot use it in the GSM context.

An operator can decide to activate the special RAND mechanism only in its home network, thus protecting the vast majority of his subscribers. It's true that if the operator chooses to apply the mechanism in the visited networks for roaming cases, he has to maintain some information about the encryption algorithms in use in these visited networks, which was pointed as a drawback by some companies. However, this can be mitigated as the algorithms in use in a visited network do not change very often. Furthermore in case of uncertainty about the algorithm used in a roaming partner's network, the operator can still fill the table as long as it knows which algorithms are NOT used by the roaming partner (for instance, an operator can forbid A5/2 and allow A5/1 and A5/3 if it knows for sure that A5/2 is not used in the partner's network, but does not know if the partner completed migration from A5/1 to A5/3).

Authenticated ciphering instruction

The authenticated ciphering instruction basically consists in introducing the following protocol modifications (see [S3-040262] for more details):
- An additional field (MAC) is added in the cipher instruction sent to the MS, in order to allow the MS to authenticate this message and the algorithm identifier parameter.
- The existing classmark information is modified in order to indicate to the network that the mobile supports the MAC capability and the key derivation capability.
- The ciphering mode command is made mandatory.

The authenticated ciphering instruction mechanism would be nice in an ideal world where modifications of equipments and protocols could be done instantaneously at no cost, and where no backward compatibility and interoperability problems would exist. However, if one takes these constraints into account, the following drawbacks as compared with the Special Rand mechanism make it extremely difficult to deploy:

- it does not only impact the terminals (MEs) but also the BSS, the MSCs, possibly also the SIM card as an option of the proposed mechanism described in an annex, and it implies modifications of all radio subsystem protocols, so that its introduction would probably take years;

- moreover (this considerably amplifies the former drawback) it requires all operators to upgrade their networks before the first upgraded mobile is released. [As a matter of fact, if the MAC feature is activated in a MS, this MS can no longer be operated in a network where the same feature has not been introduced, because the MS must require that a MAC be present in all ciphering instructions it receives: otherwise, it would be easy for a false base station to impersonate an old network without MAC capability.]

These points are acknowledged in [S3-040263] : under the item "deployment constraints", it is written: "*all visited networks must be upgraded before first upgraded mobile is released*", and the impact on network is recognised to be "*medium/high*". However, it is really not obvious that ALL the operators will be willing to update their network, considering the amount of changes. Furthermore as some operators in some countries do not even use ciphering, it can be wondered what will be their motivation to upgrade their network to support the authenticated ciphering instruction. Then, we see a high risk that if selected, the authenticated ciphering instruction will not be implemented in fact because of the deployment constraints.

Of course, [S3-040263] highlights some advantages of the authenticated ciphering instruction, such as countermeasures against bidding down attacks and against some false base station eavesdropping attacks but we do not think that this is significant compared to the drawbacks mentioned above.

4. Conclusion

Based on the above discussion, we think that the authenticated ciphering instruction has too important deployment constraints and too much complexity compared to special RAND. The key separation provided by special RAND does not only allow to counteract Barkan-Biham-Keller attack but it also provides with context separation with other domains.

We propose to select the special RAND mechanism in addition to A5/2 removal to counteract Barkan-Biham-Keller attack. The CRs implementing the mechanism in TS 33.102 and TS 43.020 are provided in other contributions.

5. 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

[S3-040262] 3GPP SA3 Tdoc S3-040262: "Analysis of the authenticated GSM cipher command mechanism", SA3 meeting #33, Beijing, China, 10-14 May 2004.

[S3-040263] 3GPP SA3 Tdoc S3-040263: " Evaluations of mechanisms to protect against Barkan-Biham-Keller attack ", SA3 meeting #33, Beijing, China, 10-14 May 2004.

[S3-040341] 3GPP SA3 Tdoc S3-040341: "Comparison of Suggested A5/2 Attack Countermeasures", SA3 meeting #33, Beijing, China, 10-14 May 2004.

[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.