3GPP TSG SA WG3 Security — SA3#33 **S3-040377**
10-14 May 2004 **Reactions to S3-040371 / S3-040263**
Beijing, China

Source: **Vodafone commented by Orange + Vodafone reactions**

Title: **Evaluations of mechanisms to protect against Barkan-Biham-Keller attack**

Document for: **Discussion and decision**

Agenda Item: **6.6: GERAN security**

1 Introduction

Several mechanisms have been proposed to address the Barkan-Biham-Keller attack. This contribution evaluates four of these mechanisms, discusses deployment strategies and considers which of the mechanisms should be progressed in 3GPP. The evaluated mechanisms are:

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

2 Evaluation

An evaluation of four of the mechanisms that have been proposed to protect against the Barkan-Biham-Keller attack [Bark] is provided below. The evaluation is then summarised in Table 1.

2.1 A5/2 removal

Description: A5/2 is removed from mobiles at the earliest opportunity.

Impact on mobile: Simple modification to remove A5/2. Could be combined with A5/3 deployment.

Impact on network: A5/2 networks must allow mobiles without A5/2 to connect without encryption, or they must upgrade to an algorithm which mobiles support. GSMA has recently discussed that it may be possible to distribute A5/1 more widely, so that networks, which previously had to use A5/2, can now use A5/1. Upgrade from A5/2 to A5/1 might be difficult, but ability to allow mobiles without A5/2 to connect without encryption should be a relatively simple configuration change.

Operational impact: No special operational procedures are required.

Deployment constraints: Some visited networks need be upgraded (may only be a configuration change) before first upgraded mobile is released.

Effectiveness against [Bark] A5/2 eavesdropping attack: Customers with upgraded mobiles are protected against eavesdropping attack immediately providing their MS has an encryption algorithm in common with the visited network.

Effectiveness against [Bark] A5/2 dynamic cloning attack: Operator only protected against dynamic cloning attack when vast majority of mobiles in the field are upgraded.

Protection against other active attacks: No.

2.2 Timing analysis

Description: Timing analysis of signalling messages is used to detect dynamic cloning attempts. The mechanism is described in [S3-040269].

Impact on mobile: None.

Impact on network: No changes to network protocols. Need ability to provide timing information of the authentication and cipher mode command responses to an analysis tool. Analysis tool can use timing information to detect dynamic cloning. If dynamic cloning is detected, then it may be possible to tune the system to identify cloning attempts with a high degree of certainty so that a fraudulent access attempts could be rejected, without impacting legitimate customers.

Operational impact: Monitoring and tuning of the analysis tool is needed.

Deployment constraints: No requirement on other operators to deploy the mechanism for it to become effective.

Effectiveness against [Bark] A5/2 eavesdropping attack: No protection against eavesdropping.

Effectiveness against [Bark] A5/2 dynamic cloning attack: Operators can be protected when timing analysis capability is installed in network. There is no need to wait for mobiles to be upgraded.

Protection against other active attacks: Protects against cloning if another A5 or GEA algorithm becomes vulnerable to Barkan-Biham-Keller attack.

2.3 Special RAND

Description: RAND is used to instruct the mobile about which encryption algorithms it is allowed to use. The mechanism is described in [S3-040030].

Impact on mobile: Change to handling of authenticaton, cipher mode setting and handover procedures.

Impact on network: Change to RAND generation in HLR/AuC. Requires look-up table of visited network ciphering capabilities in the HLR/AuC. May impact MSC in visited network if PLMN ID is added to MAP Send Authentication Information procedure.

Operational impact: Table of visited network ciphering capabilities needs to be maintained in HLR/AuC unless only deployed “at home”.

Deployment constraints: No requirement on other operators to deploy the mechanism for it to become effective.

Effectiveness against [Bark] A5/2 eavesdropping attack: Customers with upgraded mobiles are protected against eavesdropping attack immediately providing that home network HLR/AuC.

Effectiveness against [Bark] A5/2 dynamic cloning attack: Operator only protected against dynamic cloning attack when vast majority of mobiles in the field are upgraded. Customers with upgraded mobiles are protected against dynamic cloning attack immediately providing that home network HLR/AuC is upgraded.

VF: But protecting individual customers against cloning is of very limited benefit compared with protecting the operator against cloning.

Protection against other active attacks: Protects against cloning/eavesdropping if another A5 or GEA algorithm becomes vulnerable to Barkan-Biham-Keller attack. Protects against bidding down (e.g. A5/3 to A5/1), but only if visited network supports the stronger algorithm in every BTS. No protection against other categories of false base station eavesdropping attacks.

2.4 Authenticated ciphering instruction

Description: Commands from the network that instruct the mobile to cipher are authenticated and sending of a cipher / no cipher instruction before call set-up is mandated. The mechanism was originally presented to SA3 in [S3-040036]. An enhanced version described in [S3-040262] is evaluated here.

Impact on mobile: Change to handling of MS classmark, cipher mode setting and handover procedures. MAC and key derivation algorithms need to be supported.

Impact on network: Change to handling of MS classmark, cipher mode setting and handover procedures in BSS. MAC and key derivation algorithms need to be supported in BSS. BSS changes probably can be done in software and probably impact BSC rather than BTS. Small impact on MSC to mandate Cipher Mode Command prior to call establishment.

Operational impact: Once all BSS are upgraded then no special operational procedures are needed.

Deployment constraints: All visited networks must be upgraded before first upgraded mobile is released.

Effectiveness against [Bark] A5/2 eavesdropping attack: Customers with upgraded mobiles are protected against eavesdropping attack immediately.

Effectiveness against [Bark] A5/2 dynamic cloning attack: Operator only protected against dynamic cloning attack when vast majority of mobiles in the field are upgraded.

Protection against other active attacks: Protects against cloning/eavesdropping if another A5 or GEA algorithm becomes vulnerable to Barkan-Biham-Keller attack. Protects against bidding down (e.g. A5/3 to A5/1), even if visited network does not support the stronger algorithm in every BTS. Protects against certain false base station eavesdropping attacks.

	A5/2 removal	**Timing analysis**	**Special RAND**	**Authenticated ciphering instruction**
Impact on mobile	Low	None	Low/Medium	Medium
Impact on network	Low	Low	Medium	Medium/High
Operational impact	Low	Low	Medium	Low
Deployment constraints	Some visited networks need upgrade first	None	None	All visited networks need upgrade first
Effective against [Bark] A5/2 eavesdropping attack	Yes	No	Yes	Yes
Effective against [Bark] A5/2 cloning attack	Yes, but need to wait for mobile upgrades	Yes, immediately	Yes, but need to wait for mobile upgrades	Yes, but need to wait for mobile upgrades
Protection against other active attacks				
[Bark] attack against other A5	No	Yes (cloning protection only)	Yes	Yes
Bidding down protection	No	No	Partly[1]	Yes
False base station eavesdropping	No	No	No	Yes[2]

Table 1: Summary of evaluation

[1] Does not protect against bidding down in a network which supports a mixture of encryption algorithms.

[2] With some limitations – see companion contribution S3-040262.

3 Discussion

Since the Barkan-Biham-Keller attacks exploit vulnerabilities in A5/2, any strategy to mitigate the attacks should include removal/replacement of A5/2 at the earliest opportunity. A5/2 removal has a low impact on mobile/network implementation and on operational costs compared with the other mechanisms. However, it only protects against the application of the Barkan-Biham-Keller attacks against A5/2, and offers no protection if another A5 or GEA algorithm becomes vulnerable to the Barkan-Biham-Keller attack. Therefore A5/2 removal alone is not considered sufficient in the long term.

The timing analysis mechanism has the advantage that it can provide a relatively low cost and quick to deploy solution to help counteract the cloning risk. However, its ability to prevent fraud relies on characteristics of networks which may change over time and may vary between manufacturers, so the mechanism should not be considered as a long-term solution. Furthermore, it offers no protection against the eavesdropping threat.

Both the special RAND mechanism and the authenticated ciphering instruction mechanism have a higher impact on mobile/network implementation and will be relatively slow to deploy. However, either of these mechanisms could be introduced in the medium/long term to complement and address the limitations of the short term A5/2 removal and timing analysis solutions. Once the mechanisms are deployed and fully operational, both the RAND mechanism and the authenticated ciphering instruction mechanism offer a similar a level of protection against the Barkan-Biham-Keller attacks. Because of this we assume that only one of the mechanisms should be selected. In the following we evaluate the special RAND mechanism and the authentication cipher mechanism against each other:

Cost to deploy and operate: The special RAND mechanism has a lower initialisation cost, but the running costs and risks of call failure due to incorrect special RAND setting are higher. The authenticated ciphering instruction mechanism has a higher initialisation cost, but lower running costs and risks.

We do not expect such running costs and call failure with the special RAND mechanism as the algorithms in use in a visited network do not change very often. It shall also be noticed that "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)" (cf [S3-030693]).

VF: Even if special RAND is used in the way suggested above, it could still happen that the wrong special RANDs are sent to a visited network, due to the wrong configuration in the HLR. This could result in all roamers being unable to make or receive calls in the visited network. With the special RAND mechanism as currently specified, this problem may not be noticed immediately so revenue will be lost in the meantime. Note that configuration errors could happen accidentally or maliciously.

On the contrary, with the authenticated ciphering instruction mechanism, errors can be expected in the roaming case if not all the networks are upgraded, as the "new" handsets won't be backward compatible with the "old" networks.

VF: With the authenticated ciphering instruction “new” handsets should not be deployed until all visited networks are upgraded. Providing that this is done then there should be no errors in the roaming case. Furthermore, once all visited networks are upgraded then no further configuration changes are needed when new algorithms are introduced in visited networks. In special RAND, configuration changes will be needed indefinitely, as new algorithms are introduced, for the mechanism to remain effective. This will require configuration changes to be made during the entire life of the system, so the risk of operational errors is higher compared with the authenticated ciphering instruction mechanism.

Time for mechanism to provide effective protection against [Bark] A5/2 attacks: The special RAND mechanism becomes effective against the eavesdropping attack for the first upgraded mobile as soon as the home network HLR/AuC is upgraded[3]. The delay is longer for the authenticated ciphering instruction mechanism because upgraded mobiles cannot be released until all visited networks are upgraded. With both mechanisms, effective protection against the cloning attack will only come after the vast majority of mobiles in the field have been upgraded. The extra delay in protecting against cloning for authenticated ciphering instruction mechanism (due to the need to upgrade all visited networks first), is not considered to be significant compared to the delay in waiting for the vast majority of mobiles in the field to be upgraded. The criticality of the delay in the case of the authenticated ciphering instruction mechanism therefore depends on the severity of the eavesdropping risk rather than the severity of the cloning risk. We suggest that

[3] Expect if in A5/2 network or encryption disabled.

dynamic cloning is the more severe risk. Furthermore, the eavesdropping risk will diminish in the meantime due to A5/2 removal. Therefore, we consider the extra delay in protecting against the eavesdropping attack with the authenticated ciphering instruction mechanism not to be so significant.

The special RAND mechanism allows upgraded mobiles to be protected against [Bark] A5/2 attacks (eavesdropping, cloning attack…) as soon as it is implemented in the network. There is no "extra delay" as mentionned above.

VF: I accept that special RAND can protect individual customers against cloning and eavesdropping more quickly than the authenticated ciphering instruction. However, A5/2 removal/replacement (which should happen anyway) can achieve the same effect. Furthermore, protecting **individual customers** against cloning has limited benefit and it is more important to achieve protection against cloning **for the operator**, which requires a good penetration of upgraded mobiles in the field for **both solutions**. The time taken to reach a high penetration of upgraded mobiles in the field is quite similar for both special RAND and the authenticated ciphering instruction mechanism since the limiting factor is the time to upgrade mobiles not the time to upgrade visited networks.

On the contrary, the authenticated ciphering instruction mechanism requires all the operators to upgrade their network before the mechanism can be activated. (If only a part of the operators upgrade their network, error cases in roaming can be expected for the handsets with the mechanism activated as they are not backward compatible with the "old" networks.) As a consequence, extra time is needed so that the authenticated ciphering instruction mechanism can be implemented whereas there are not such constraints with the special RAND mechanism.

VF: See previous comment.

Protection against other active attacks: The authenticated ciphering instruction mechanism already provides some security advantages over the special RAND mechanism as described in Section 3. In particular, it provides enhanced protection against bidding down and protection against certain false base station attacks. It is not obvious that the special RAND mechanism could be extended or complemented with other mechanisms to provide protection against these attacks with similar or lower cost. We believe that even though these attacks may not be so important to counteract as the Barkan-Biham-Keller attacks in the medium term, we should have the means to address these attacks in the future.

Additional benefits of the special RAND mechanism: It also applies to GPRS without additional developments whereas the authenticated ciphering instruction mechanism is currently described only for CSD. Additionally, separation between CSD and GPRS domains can be ensured.

VF: The additional work to specify and implement the authenticated ciphering instruction for GPRS is not significant. Furthermore, separation between domains is achieved if both CSD and GPRS ciphering instructions are authenticated, i.e. cannot simply append a MAC from a GSM CS command to the equivalent GPRS command since the inputs to the MAC calculation are different (if required, a more explicit separation could be done by adding a unique “context” field to the MAC calculation.)

4 Conclusion

Based on the evaluation and discussion in this contribution, we believe that the authenticated ciphering instruction mechanism should be adopted in preference to the special RAND mechanism as a medium/long-term solution to mitigate the Barkan-Biham-Keller attacks. We believe that A5/2 removal/replacement and the application of timing analysis techniques to detect/prevent dynamic cloning in the short term mean that more time is available to standardise, implement and deploy a more comprehensive medium/long-term solution. The authenticated ciphering instruction mechanism has the advantage that the security enhancements it provides are aligned with 3G/UMTS security. The mechanism therefore provides a better upgrade path for evolving GSM security towards 3G level. We also favour the authenticated ciphering instruction mechanism because, although it might be more complex to deploy initially, the operational costs and risks of call failures are lower than the special RAND mechanism, and it provides effective protection against other active attacks at relatively low additional cost.

The special RAND mechanism can be deployed on the first upgraded mobiles as soon as the HLR/AuC is upgraded. It only impacts the handsets and the HLR and does not impact the protocols. (MSC can be impacted if PLMN id parameter is added in MAP_SEND_AUTHENTICATION_INFO message but it is not mandatory to be able to implement the mechanism.).

VF: This is already acknowledged in the evaluation.

On the opposite, the authenticated ciphering instruction mechanism requires changes in the handsets, the BSS and in the MSC. Radio and A interface protocols are modified.

VF: This is already acknowledged in the evaluation.

It is a more long term solution as it requires that all the networks are updated before it is activated.

VF: Not sure what is meant by "long term" here. Certainly some aspects of special RAND achieve shorter-term results compared with the authenticated ciphering instruction mechanism. However, it is important not just to compare special RAND with the authenticated ciphering instruction mechanism in isolation; we also need to look at the "big picture" and factor in other mechanisms such as A5/2 removal/replacement and the timing analysis mechanism. This is what I have attempted to do in this paper.

For these reasons, we see more disadvantages than advantages in the authenticated ciphering instruction mechanism compared to the special RAND mechanism.

VF: For the reasons explained above, I do not believe that the advantages of the special RAND mechanism compared to the authenticated ciphering instruction mechanism are significant. Furthermore, I believe that the authenticated ciphering instruction mechanism is the most future proof approach with the lowest operational costs/risks. In particular, with regard to future proofing, we should not specify, implement and deploy special RAND now to deal with the specific [Bark] attacks, and then have to introduce a mandatory authenticated cipher mode command later to deal with false base station attacks, when we can address both threats now in an integrated way.

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.

[S3-040269] 3GPP SA3 Tdoc S3-040269: "Another countermeasure for the Barkan-Biham-Keller attack on A5/2", SA3 meeting #33, Beijing, China, 10-14 May 2004.

[S3-040030] 3GPP SA3 Tdoc S3-040030: "Draft CR to 43.020: Introducing the special RAND mechanism", SA3 meeting #32, Edinburgh, Scotland, 9-13 February 2004.

[S3-040036] 3GPP SA3 Tdoc S3-040036: "Authentication: A mechanism for preventing man-in-the-middle attacks", SA3 meeting #32, Edinburgh, Scotland, 9-13 February 2004.

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