3GPP TSG SA WG3 Security — SA3#33 **S3-040262**
10-14 May 2004
Beijing, China

Source: **Vodafone**

Title: **Analysis of the authenticated GSM cipher command mechanism**

Document for: **Discussion and decision**

Agenda Item: **6.6: GERAN security**

1 Introduction

A security mechanism to protect against the GSM active attack described by Barkan-Biham-Keller [Bark] was presented at SA3#32 [S3-040036]. The mechanism involves adding a Message Authentication Code (MAC) to the Cipher Mode Command sent by the BSS to the MS. At SA3#32 it was decided that the mechanism should be analysed and a contribution made to the next SA3 meeting. This document constitutes such an analysis. As well as analysing the basic mechanism described in [S3-040036] we also study some variants and extensions.

2 Overview of existing cipher mode setting procedure

The high-level information flow during cipher mode setting is described in Figure 1. The exact formats of the specifications are defined in the specifications listed in the Table 1.

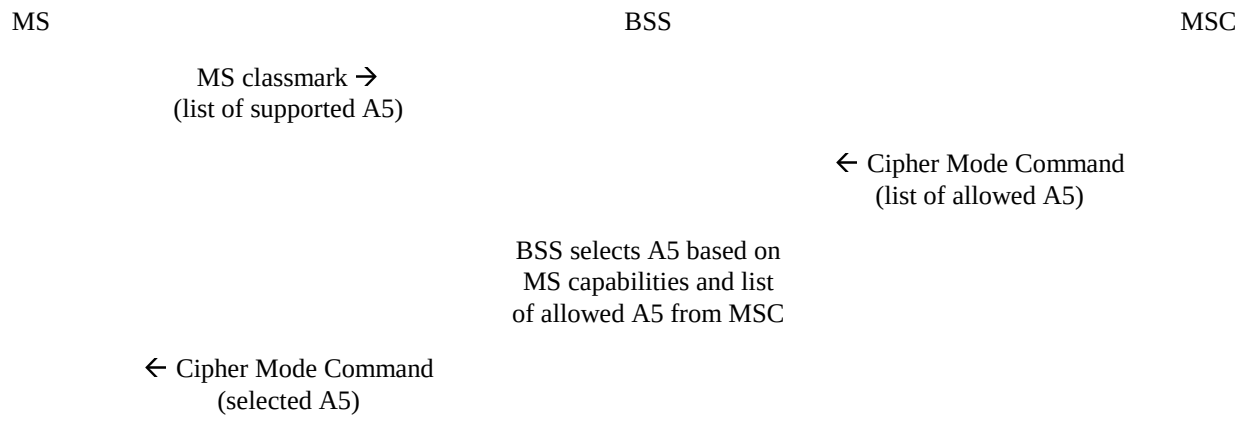

Figure 1: Cipher mode setting procedure

MS classmark	TS 24.008v6.3.0, Sections 10.5.1.5, 10.5.1.7 [24.008]
BSSMAP Cipher Mode Command (MSC→BSS)	TS 48.008v5.b.0, Sections 3.2.1.30, 3.2.2.10 [48.008]
Radio interface Cipher Mode Command (BSS→MS)	TS 44.018v6.5.0, Sections 9.1.9, 10.5.2.9 [44.018]

Table 1: References for cipher mode setting message specifications

3 Description of the basic mechanism in [S3-040036]

In [S3-040036] it is proposed that a Message Authentication Code (MAC) is added to the radio interface Cipher Mode Command. The MAC is calculated as: hash(Kc, SRES, algflag), where hash is a strong hash function, Kc is the current GSM cipher key shared between the BSS and the MS, and SRES is the GSM authentication response that corresponds to the cipher key. We assume that the MAC will actually be a truncated version of the hash function output.

Although the use of a hash function is described in [S3-040036], we note that MACs may also be based on block ciphers. For the purposes of this document we assume that a MAC function is used, but do not specify how the MAC function should be constructed.

Algflag is not defined in [S3-040036] – here, we assume that it includes at least the 3-bit algorithm identifier, which is part of the Cipher Mode Setting information element in the radio interface Cipher Mode Command [44.018]. On receipt of the radio interface Cipher Mode Command, the MS recalculates the MAC and compares it against the value received from the BSS. If the values do not match, then the MS considers the Cipher Mode Command to have been tampered with, and rejects it. The MS also rejects the Cipher Mode Command if the MAC is absent – this is done so that an active attacker cannot circumvent the mechanism by simply removing the MAC.

The SRES is included as an input to the MAC. Here, we assume that this is done to make it infeasible for an attacker to mount a codebook attack to discover Kc. In particular, if SRES were not included, then an attacker could build up a table of MAC values against all possible Kc values. Since the remaining input to the MAC calculation - the algorithm identifier field - is generally fixed per network, the attacker can use the table to discover Kc by observing the MAC sent in the Cipher Mode Command. Once Kc is discovered, the attacker may be able to eavesdrop and masquerade user communications.

Although generating and sorting the codebook table is time consuming, the storage of it is the main obstacle. Assuming that the effective key length of Kc is 54 bits, then the table would require 121597 Tbyte of storage! While this may deter potential attackers for some time to come, we believe that time-memory trade-off techniques may reduce the size of the table significantly. Even by applying time-memory trade-off techniques, the attack may still be quite expensive to mount. However, it should be remembered that the pre-computation part of the attack is applicable to any mobile in any network that uses the same A5 algorithm. Therefore the motivation to do the pre-computation might be quite high.

In [S3-040036] it is assumed that all networks globally need to be upgraded before the first mobiles to support the mechanism can be deployed. The upgraded network will add the MAC and any other new fields to the Cipher Mode Command for all mobiles. It is expected that old mobiles would correctly ignore the new fields.

4 Variants on the basic security mechanism

4.1 Implementation in MSC instead of in BSS

In [S3-040036] it was suggested that it might be possible for the basic mechanism to be introduced as an MSC change without any impact on existing BSS. One approach to do this would be to calculate the MAC in the MSC and use the list of allowed algorithms, rather than the selected algorithm, as an input to the calculation. This would require the MS to check that the algorithm selected by the BSS is on the authenticated list of allowed algorithms from the MSC.

For this scheme to work, the MAC and list of allowed algorithms would need to be added to the BSSMAP Cipher Mode Command in such a way that they are transparently transferred to the MS in the radio interface Cipher Mode Command, without requiring any changes to the BSS. However, this does not seem feasible, since no such information elements in the BSSMAP Cipher Mode Command are currently transferred in this way.

This variant might be worth further study if it is desirable to avoid new cryptographic calculations in the BSS, but acceptable to introduce a mechanism in the BSS to relay new information elements in the Cipher Mode Command to the mobile. However, the reduced impact on the BSS in this case is not expected to be significant, especially when compared with the cost of requiring changes in both BSS and MSC. Even if it were feasible to implement the mechanism such that it only impacts the MSC, then it is not clear that this would make the mechanism easier and cheaper to deploy than a mechanism that is implemented completed within the BSS.

In conclusion, it does not seem feasible to introduce this type of mechanism without any impact on the BSS. Therefore, we propose to restrict attention to schemes that impact the BSS and avoid impacting the MSC and the A interface.

4.2 Preventing codebook attacks to discover Kc

In the basic mechanism described in [S3-040036], it is proposed to include the SRES in the MAC calculation. We assume in this document that this is to help protect against codebook attacks, as described in Section 3. Unfortunately, SRES is not currently available in the BSS. If SRES were used in the calculation of the MAC, it would have to be passed to the BSS by the MSC. This would require a change to the BSSMAP Cipher Mode Command and require an upgrade to the MSC and the A interface. In this section we consider some alternative mechanisms to protect against codebook attacks, which avoid changes to the MSC and the A interface. Some candidate mechanisms are discussed below:

1. Include a random "salt" generated by the BSS in the calculation of the MAC. The "salt" would have to be carried in the Cipher Mode Command alongside the MAC. The length of the "salt" depends on the applicability of time-memory trade-off techniques discussed in section 3. However, the length of MAC is not expected to contribute significantly to the overall length of the Cipher Mode Command.

2. Use MS classmark in the calculation of the MAC. This may be needed anyway if we want to protect against bidding down (see section 0)[1]. However, the variation of this parameter between some mobiles is quite small. In particular, it might be feasible to pre-calculate a table, which could be used against a group of mobiles with the same classmark. Furthermore, attacks against a specific mobile are still possible. This method should therefore be ruled out.

3. Include a random number in the MS classmark and use this in the calculation of the MAC. This has the advantage that it can be combined with the bidding down mechanism in section 0. The disadvantage is that the mobile needs to implement a good random number generator. To avoid this problem a sequence number could be used instead, but this offers a much lower level of protection.

4. Use RAND in the derivation of a cipher key and an authentication key from Kc. Using this approach, the attacker could build up a table to discover the authentication key, but could not build up a table to discover the cipher key or use the authentication key to obtain the cipher key.

Mechanism (2) should be ruled out since it does not offer adequate protection. Mechanism (3) should also be ruled out since it requires the mobile to implement a good random number generator. This leaves mechanisms (1) and (4). We select mechanism (1) because it is probably the simplest approach since it does not impose any special requirements on key derivation.

5 Extensions to the basic scheme

5.1 Bidding down protection

In an email to the SA3 list on 13th February 2004, James Semple (Qualcomm) described two solutions to extend the basic scheme in [S3-040036] to protect against bidding down attacks. The solutions are intended to protect against a man-in-the-middle modifying the messages in the cipher mode setting procedure to force a weak cipher algorithm to be selected when a strong one is available at both sides. This would be especially useful when A5/3 and GEA3 are deployed.

The first solution is for the BSS to include the MS's cipher capabilities from the MS classmark in the calculation of the MAC sent to the MS. The MS then recalculates the MAC and compares it against the value received from the BSS. If a man-in-the-middle has modified the MS capabilities originally sent to the network, then the MAC check will fail.

The second solution is for the BSS to add the network cipher capabilities to the Cipher Mode Command and also include these capabilities in the calculation of the MAC. The terminal then checks that the chosen algorithm is indeed the strongest of the ones it has in common with the network, and that the MAC check is successful.

[1] In the referenced section, it is proposed that only certain parts of the classmark are included in the MAC calculation. However, it is easy to conveive of an alternative where the whole classmark is used as the input instead.

A major disadvantage of the second solution is that it requires the MS to know which algorithm the legitimate network would select if it shares several algorithms in common with the MS. It would be problematic for the operator to have to configure this information in the MS (e.g. using OTA methods), and it is not realistic to assume that the customer has sufficient security awareness to be able to configure this information himself/herself. A further potential disadvantage is that the addition of the network cipher capabilities increases the length of the Cipher Mode Command. An advantage of the first solution is that it is in-line with the mechanism for bidding down protection provided in UTRAN [33.102].

In conclusion, we feel that bidding down is an essential enhancement to the basic mechanisms and that the first solution described above is the preferred approach.

5.2 Separation of encryption and authentication keys

It is a general security principle that the same key should not be used for encryption and authentication. If applied to the basic mechanism in [S3-040036], then Kc should not be used to generate the MAC and to encrypt the user traffic. An alternative approach would be to derive two keys from Kc: Kc_enc and Kc_mac. One of these keys could be used for encryption and the other for generation of the MAC.

A problem with this approach is that ciphering between an old mobile and a new BSS will not work. This is because, in the basic mechanism, the BSS does not know whether the MS supports the MAC checking mechanism or not. Therefore, the BSS does not know whether to use Kc or the derived Kc_enc for ciphering. A solution to this problem would be to include the MS key derivation capabilities in the MS classmark. The BSS would then select whether to use key derivation based on the MS capabilities and its own capabilities. If key derivation were used then the selected key derivation function would be included in the authenticated part of the Cipher Mode Command. A further advantage of this solution is that it allows the key derivation function to be upgraded in the future.

Note that a man-in-the-middle could modify the classmark to force the MS and BSS to use a weaker key derivation function than what is available. To avoid this, the key derivation capabilities of the MS from the classmark should be included in the calculation of the MAC in the Cipher Mode Command, and checked against the capabilities that were originally sent by the MS. This would be an extension of the mechanism described in section 5.1. Note that a man-in-the-middle cannot force an upgraded mobile with the MAC checking mechanism enabled to use no key derivation by modifying the classmark, because the upgraded mobile will only accept the Cipher Mode Command if a valid MAC is present.

The mechanism described above is a relatively simply extension to the basic scheme which provides a desirable enhancement. We therefore propose that it is adopted.

5.3 Negotiating the MAC function

In the basic mechanism described in [S3-040036], it is not specified whether the MAC function should be negotiable between the MS and the BSS. An advantage of making the MAC function negotiable is that new MAC functions can be introduced later. A further advantage is that an upgraded BSS does not have to add the MAC to the Cipher Mode Command for mobiles that do not support MAC checking.

A mechanism for negotiating the MAC function could be achieved by including the MS MAC function capabilities in the MS classmark. The BSS would then select whether to use MAC checking based on the MS capabilities and its own capabilities. If the MAC checking function were to be used, then the selected MAC function would be included in the authenticated part of the Cipher Mode Command.

The mechanism described above is a relatively simply extension to the basic scheme which provides a desirable enhancement. We therefore propose that it is adopted.

5.4 Mandating cipher mode setting prior to call establishment

A potential vulnerability in GSM is that an attacker, acting as a man-in-the-middle, can intercept mobile-originated calls from a target MS and connect these through to the called party. Because it is optional for the network to send the radio interface Cipher Mode Command, the MS proceeds with the call even though the attacker does not switch on encryption. This allows the attacker to eavesdrop the call. Although there may be some telltale signs (incorrect or missing CLI, call not billed, cipher indicator on compatible ME/SIM), the user is typically not aware that the attack is taking place.

This vulnerability is addressed in UMTS by making it mandatory to send the RRC Security Mode Command before certain signalling messages - like call set-up messages - can be transmitted. The RRC Security Mode Command is authenticated (in UMTS this is called integrity protection). This means that it is possible for a mobile to work in a legitimate network, which has encryption disabled, by sending a Security Mode Command, which instructs the mobile to enter an unencrypted mode. However, it is not possible for a false base station to spoof such a Security Mode Command, or to simply omit it, in order to intercept mobile-originated calls.

If we introduce a mechanism to authenticate (or integrity protect) the Cipher Mode Command in GSM – in particular authentication of the selected A5 algorithm part – then an extension of this mechanism to protect against false base station eavesdropping would be to make it mandatory to send the Cipher Mode Command before certain signalling messages can be transmitted. One approach would be to implement a simple control in the MS, which would prohibit certain signalling messages - like call set-up messages - from being sent until a cipher mode command has been successfully handled in the MS. As in UMTS, it would be possible for a mobile to work in a legitimate network which has encryption disabled by sending a Cipher Mode Command, which instructs the mobile to enter an unencrypted mode. However, it would not be possible for a false base station to spoof such a Cipher Mode Command, or to simply omit it, in order to intercept mobile-originated calls.

Although this mechanism would protect against the specific false base station attack described above, it would not protect against attacks which make use of triplets that have been previously collected by an attacker using the Barkan-Biham-Keller attack when the subscriber had the same (U)SIM but an old mobile that did not support MAC checking. This attack could be avoided by ensuring that new (U)SIMs are issued when the customer upgrades his mobile, but this is not always possible to achieve. However, this type of "time lagged" attack is very low risk, and therefore deemed less important to counteract. The longer term solution to this potential problem is to deploy USIMs and mandate USIM authentication for GSM – see the note at the end of this section.

The exact MS and BSS behaviour to support this mechanism needs to be specified. However, we believe that it would be feasible to specify and implement such mechanisms since the handling is similar to that already implemented on UMTS devices.

Special handling will be needed to ensure that this mechanism does not interfere with (U)SIM-less emergency calls. However, again we expect that the same mechanisms that exist on UMTS devices could be adopted.

In conclusion, we feel that mandating cipher mode setting prior to call establishment is a very desirable enhancement to the basic mechanism.

A further extension to GSM security: As noted above, the mechanism is this section does not protect against false base station attacks where the attacker has obtain a valid triplet for the target subscriber. A possible further enhancement to GSM security to protect against this attack would be to deploy USIMs and mandate USIM authentication for GSM communications. Note that this creates a similar deployment problem to the MAC checking mechanism whereby all GSM networks globally must be upgraded to support 3G AKA before mobiles which mandate 3G AKA for GSM communications are deployed.

5.5 Protection of cipher mode setting in handover messages

The GSM ciphering algorithm can be changed at handover. This is to deal with the situation that different BTS may support different A5 algorithms. This capability is needed when new algorithms are deployed, or in the case of inter-operator handover. Note that this mechanism cannot be used to change the cipher key at handover, or to change from encrypted mode to unencrypted mode.

It should be considered whether the cipher mode setting parameters in the Handover Command should be authenticated in a similar way to the Cipher Mode Command. If we start with the premise that the Handover Command is not protected, then it is theoretically possible for an attacker to “force” a handover to a false BTS that uses a “weak” algorithm. This might allow similar attacks to those described by Barkan-Biham_Keller [Bark].

In such a scenario the Handover Command is sent to the MS from the old BTS and is therefore encrypted under the “strong” algorithm. Since a stream cipher is used, the attacker could toggle bits 2, 3 and 4 in the ciphertext version of the Cipher Mode Setting information element [44.018] to achieve a know change to the plaintext. This could allow an attacker to change the selected algorithm from a “strong” to a “weak” algorithm. The main challenge for the attacker would seem to be to find a way to identify which bits in the ciphertext correspond to the cipher mode setting information element. This is assumed to be a difficult task.

If the attacker manages to change the selected algorithm in the Cipher Mode Setting information element, then the MS will reply with a Handover Complete message, which is encrypted using the "weak" algorithm. The attacker could then potentially perform a ciphertext-only attack on the Handover Complete message to discover the cipher key. This would allow the user's communications to be eavesdropped. Furthermore, if the attacker can discover the cipher key quickly enough, then he may be able to hijack the channel and masquerade as the target MS.

Although these types of attack are theoretically possible, there are a number of practical problems that the attacker would have to solve. While it would be prudent to protect the Handover Command, it is clear that there is significant benefit in protecting the Cipher Mode Command, even if the Handover Command is not protected.

Another factor is that the size of the Handover Command is more critical than the Cipher Mode Command, because it is sent over the radio interface, usually in conditions of disappearing coverage. On the other hand, if the MAC and any extra fields are small enough, then this may not create a major problem.

In conclusion, we believe that the Handover Command should only be protected unless the increased since of the Handover Command significantly impairs handover performance.

5.6 Protection of other signalling procedures

Once a mechanism is added to authenticate (part of) the Cipher Mode Command, the same mechanism could be extended and applied to other signalling messages. In section 5.5 we have already discussed whether the Handover Command should be protected. In a similar way, we can discuss whether other signalling messages should be protected.

In UMTS most RRC and all Layer 3 signalling messages are authenticated. The protection of the RRC Security Mode Command protects against the false base station attacks discussed in section 5.2. Protection of other messages protects against other attacks. In particular, if the network does not apply encryption, then authentication of Layer 3 call set-up messages helps protect against channel hijack. However, the authentication (integrity protection) of radio interface signalling messages in UMTS was designed into the system from the start, so the additional cost of protecting several messages is not as significant as it is in the case of GSM where we are proposing to retrofit authentication of signalling messages. It is not clear whether there is sufficient value in applying authentication to messages other than the Cipher Mode Command and perhaps the Handover Command.

In conclusion, we believe that extending the protection to other messages should only be considered if it has a very low additional impact on the MS and BSS. We propose to adopt the working assumption that these other messages need not be protected.

6 Detailed description of enhanced mechanism

In this section we assume that the basic scheme for authenticating the cipher mode command is to be standardised. Furthermore, we assume that the variants in section 4 and the extensions in section 5 are adopted according to our proposals. In the following subsections we elaborate the details of the complete mechanism.

6.1 Protocol steps

6.1.1 Cipher mode setting procedure

The protocol steps during cipher mode setting compared to the current approach are described below:

1. The MS classmark is sent to the network. The new capability information in the Classmark is defined as follows:

    - MAC function capability: This is a bitmap of supported algorithms of length 8 bits. It is envisaged that only one bit will be specified in the first release; the rest of the bits are reserved for future use.

    - Key derivation capability: This is a bitmap of supported algorithm of length 8 bits. It is envisaged that only one bit will be specified in the first release; the rest of the bits are reserved for future use.

2. If the MS classmark indicates that MAC checking and key derivation is supported on the MS, the BSS sends a modified Cipher Mode Command to the MS. The modified Cipher Mode Command is constructed as follows:

- Two new fields are added to indicate which MAC function and key derivation function the MS should use. These functions are selected by the BSS based on the capabilities sent in the MS classmark. The new fields are called the MAC function identifier and key derivation identifier respectively. Based on the length of the bitmap in the MS classmark, up to eight algorithms could be specified. Therefore the MAC function identifier and key derivation identifier would each need to be 3 bits long.
- A new field is added to include a random "salt" generated by the BSS. We assume that a 32-bit salt would be sufficient, but a longer salt could be specified if needed. (ETSI SAGE should be consulted on the length of "salt".)
- A new field is added to carry the MAC. The key used for the MAC calculation is derived from the Kc using the selected key derivation function. We assume that a MAC length of 32 bits would be sufficient, but a longer MAC length could be specified if needed. One possibility might be to allow a variable length MAC field, say 32-64 bits – the exact length of the MAC could be derived by the MS from the MAC function identifier field. The feasibility of this should be discussed with GERAN2. The MAC is generated using the selected MAC function based on the following inputs:
  - The ciphering algorithm identifier from Cipher Mode Setting information element (3 bits)
  - The MAC function identifier (3 bits)
  - The key derivation function identifier (3 bits)
  - The random "salt" (32 bits)
  - The A5 algorithm capability part of the MS classmark (8 bits)
  - The MAC function capability part of the MS classmark (8 bits)
  - The key derivation capability part of the MS classmark (8 bits)

3. The MS recalculates the MAC. The connection must not proceed if the MAC check is unsuccessful or if the MAC is missing. The exact mechanism to achieve this requires input from GERAN and CN1.

Three Classmarks are defined in the specifications: Classmark 1, Classmark 2 and Classmark 3 [24.008]. Classmarks 1 and 2 cannot be extended, so the new capability information must be added to Classmark 3. Classmark 3 is passed to the MSC from the BSS, and the MSC stores it for use at handover. The MSC handles the classmark as a container so the MSC should need to be updated if the classmark is updated, unless the maximum classmark size (12 octets) is breached. The additional 2 octets for the MAC and key derivation capabilities *might* cause this limit to be exceeded. Segmentation has been suggested in GERAN to remove the 12 octet limit, but it is not clear when this would be introduced. Furthermore, segmentation of classmark 3 would add a delay of about ¼ second to call establishment. Further information is needed from GERAN on whether it is needed to reduce the size of the MAC and key derviation capability information to avoid problems on the radio interface.

It is possible to add new fields to the radio interface Cipher Mode Command providing that the total length is less than 160 bits. Based on the above parameter lengths, the modified Cipher Mode Command would be extended by 70-102 bits and is therefore not expect to cause major problems on the radio interface.

6.1.2 Handover procedure

The modifications to the handover procedure can be derived from to the cipher mode setting procedure so they are not reproduced here. If the MAC check on the Handover Command is unsuccessful, or if it is missing, then the connection must not proceed. Again, input from GERAN and CN1 is required to determine exactly how to achieve this.

It is possible to add new fields to the Handover Command in a similar way to how they are added to the Cipher Mode Command. Again there is a restriction of 160 bits on the total length of the extra bits. Note however that the size of the Handover Command is more critical than that of the Cipher Mode Command, because it is sent over the radio interface, usually in conditions of disappearing coverage.

6.2 Selection of MAC function

ETSI SAGE should be consulted regarding the selection of the MAC. However, some initial thoughts are provided in this section.

From the description in section 6.1, the MAC function will be applied to a 65 bit input string. The function will make use of a key derived from Kc. The length of the MAC key and the MAC output should be specified. At this stage, we assume that the MAC length is 32 bits, but a longer MAC could be specified if needed within the constraints imposed by radio interface on the length of the Cipher Mode Command. The key length is not specified here, but it should be noted that the MAC key length might be longer than the Kc from which it is derived.

The actual algorithm could be based on the re-use of existing algorithms on the MS. For example, it could be a mode of operation of Kasumi, which would allow potential re-use of functionality in MS that support any existing Kasumi-based algorithms (e.g. A5/3, UEA1, UIA1, etc.)

6.3 Selection of key derivation function

ETSI SAGE should be consulted regarding the selection of the key derivation function. However, some initial thoughts are provided in this section.

As observed in section 6.2, the length of the MAC key may be longer than the Kc from which it is derived. Note also that the Kc may be variable length. For example, if support for 128 bit A5/4 or GEA4 encryption is provided, then Kc will be 128 bits long. The key derivation function shall be able to cope with variable length Kc.

6.4 Error handling

The detailed error handling should be defined in the case that the MAC check in the MS fails, or when the MAC is missing when the MS expects it to be present. From a security point of view the call should not be allowed to proceed in this case. As mentioned above, CN1 and GERAN2 should be consulted to determine how best to achieve this from a signalling point of view. Some initial ideas are described in this section.

One option could be for the MS to send an IMSI Detach Indication to the network. A new cause value should be added to IMSI Detach Indication to indicate to the network that the MAC check failed. The MS will then try to re-attach and go through authentication and cipher mode setting again. Note that repeated attempts to re-attach due to incorrect or missing MAC should not happen in normal operation.

7 Conclusions

The following conclusions are drawn regarding the suitability of mechanism described in [S3-040036]:

- The possibility to adapt the mechanism so that it can be implemented without any impact on the BSS was considered, but found not to be feasible.
- The basic mechanism has the disadvantage that SRES is used in the calculation of the MAC to protect against codebook attacks. This disadvantage can be overcome by including a “salt” in the Cipher Mode Command and using this as an input to the calculation instead of SRES (see section x.x).

The following extensions to the basic mechanism should also be adopted:

- The MS cipher capabilities should be included in the calculation of MAC to protect against bidding down.
- Separate cipher and authentication keys should be derived from Kc.
- The key derivation function and the MAC function capabilities should be included in the MS classmark and subsequently used in the calculation of the MAC. The key derivation function is used to generate separate cipher and authentication keys from Kc. It is possible to securely negotiate the key derivation function and MAC function, so that the algorithms can be upgraded in the future if needed.

- The Cipher mode setting procedure should be mandated prior to call establishment to protect against man-in-the-middle eavesdropping attacks.
- The Handover Command should be protected in a similar way to the Cipher Mode Command to protect against attacks that apply the Barkan-Biham-Keller to the handover procedure.

If the extended mechanism is adopted then the following issues need to be addressed:

- Consult with ETSI SAGE regarding selection of the MAC and key derivation function, and the length of "salt".
- Consult with GERAN and CN1 regarding error cases.
- Consult with GERAN regarding the available space in Classmark 3 to carry the MAC and key derivation capability information.
- Applicability of the mechanism to GPRS

8 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.

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

[24.008] 3GPP TS 24.008, Mobile radio interface Layer 3 specifications; Core network protocols; Stage 3.

[48.008] 3GPP TS 48.008, Mobile radio interface Layer 3 specifications; Radio Resource Control (RRC) protocol.

[44.018] 3GPP TS 44.018, Mobile Switching Centre – Base Station System (MSC-BSS) interface; Layer 3 specification.

[33.102] 3GPP TS 33.102, 3G Security; Security Architecture.

Annex: Allowing "new" mobiles to roam in "old" networks

The basic MAC checking mechanism requires that all networks globally need to be upgraded before the first mobiles to support the mechanism can be deployed. This is to avoid interoperability problems due to the fact that an upgraded mobile will not work in networks that have not been upgraded because the mobile always expects the MAC to be present in the Cipher Mode Command. An alternative approach, which could be considered, would be to allow new mobiles to be configured to disable the MAC check so that they can work in old networks in certain situations. This could be done using a flag on the (U)SIM.

Using this mechanism, the (U)SIM would be issued with an initial configuration based on the operator's preferences, but it would also be possible, as an operator option, to change the flag later using OTA methods. If OTA is used to change the flag, then the OTA commands should be secured using the mechanisms defined in TS 23.048. The following issues are considered:

- Use of a (U)SIM which does not support the flag: In this case the terminal must assume a default configuration. If the default configuration is to deactivate the mechanism, then this avoids interoperability problems with networks that have not been upgraded in the case that an old (U)SIM is used in an upgraded terminal.
- MMI override: It should be considered whether to allow the user to override the default setting via the MMI. This could allow the customer to be protected against certain attacks while roaming in their upgraded home network without limiting their ability to roam on networks that have not been upgraded. However, an MMI override may also create a bad user experience if the user accidentally enables the MAC check and then roams to a network that has not been upgraded.

The main advantage of allowing the mechanism to be configured using the (U)SIM is that the operator can control when to enable the mechanism based on an assessment of the risks. For example, the mechanism could be used to deploy the MAC checking mechanism in the following phased approach:

- Phase 1: Mechanism enabled only for selected customers to protect against eavesdropping: Initially, all new (U)SIMs would have the MAC check disabled. However, once an operator has upgraded its network to support the MAC check, the mechanism would be enabled for certain customers that require additional assurance that their communications are not subject to the eavesdropping attack described in [Bark]. Those customers would not be able to make calls in networks which have not been upgraded without requiring the operator to change the flag on the (U)SIM again[2]. For the vast majority of customers, the MAC check would be disabled to avoid interoperability problems in networks which are not yet upgraded. Thus, the mechanism would only be enabled on a very small number of mobiles at the start, which would mean that the operator is still vulnerable to the dynamic cloning attacks described in [Bark]. This is because an attacker could easily find a target mobile in his vicinity, which does not support the new security mechanism.

- Phase 2: Mechanism enabled for all customers that support it to protect against dynamic cloning and eavesdropping: Once all networks globally support the mechanism, then it is possible to enable the mechanism on all (U)SIMs without causing interoperability problems during roaming. This protects customers with upgraded terminals and (U)SIMs against the eavesdropping attack described in [Bark]. As the proportion of mobiles and (U)SIMs which support the mechanism increases, the mechanism also starts to provide protection against the dynamic cloning attacks described in [Bark]. This is because it becomes more difficult for an attacker to find a target mobile in his vicinity, which does not support the new security mechanism.

To determine whether this phased approach based on configuration of the terminal using the (U)SIM is worth pursuing, we need to understand the relative risks of the eavesdropping attack versus the dynamic cloning attack. While the dynamic cloning attack has a high impact on the operator and the customer, it is a more complex attack since the attacker has to act as a man-in-the-middle during the call set-up phase. Furthermore, the attacker has to perform the cryptanalysis to discover the cipher key within a small time window, which is governed by the network-based authentication and cipher mode command timers. Although the eavesdropping attack has a lower impact on the operator, it is likely to be a bigger concern for customers. Furthermore, it is a less complex attack since the attacker does not need to act as a man-in-the-middle and can instead act as a stand-alone false network. In addition, the cryptanalysis to discover the cipher key can be done off-line.

The analysis above shows that there may be some value in protecting some customers against the eavesdropping attack, even if dynamic cloning is not counteracted. This is further supported by the fact that the mechanism could be complemented with interim countermeasures that are aimed at mitigating the dynamic cloning threat. In particular, timing analysis of the authentication and cipher mode command responses in the network could help detect dynamic cloning. Furthermore, if dynamic cloning did start to occur, then it may even be possible to tune the system to identify cloning attempts with a high degree of certainty so that a high proportion of fraudulent access attempts can be barred, whilst at the same time ensuring that legitimate customers are not affected.

Note that the existence of phase 1 could delay phase 2. This is because the ability to prevent the eavesdropping attack for selected customers could reduce the pressure placed on operators globally to implement MAC checking. However, it may be possible to manage this risk so that phase 2 is either not delayed, or not delayed significantly.

Note also that the error cases in phase 1 must be considered carefully. If upgraded mobiles are only deployed after all networks are upgraded then rejection of the Cipher Mode Command (or Handover Command) due to an incorrect or missing MAC should not happen in normal operator. However, if upgraded mobiles are deployed before all networks are upgraded then the above-mentioned error cases could happen in normal operation. This means that it becomes more important to achieve a graceful error behaviour. In this case of handover a Handover Failure message could be sent if the MS roams to a network which does not add the MAC to the Handover Command. The Handover Failure message would keep the MS on the MAC supporting network and avoid a dropped call.

[2] An alternative solution could be for the home network to update the flag dynamically when the user roams into a new network, but this does not seem feasible since the delay in updating the flag using OTA methods is probably too great. Furthermore, this mechanism would not prevent cross border dynamic cloning.