3GPP TSG SA WG3 Security — S3#31 **S3-030659**
18 - 21 November 2003
Munich, Germany

Source: **BT Group**

Contact: **Colin Blanchard colin.blanchard@bt.com**

Title: **Use of the same algorithms for encryption of VGCS-calls as for normal GSM-speech calls (i.e. A5/0-A5/7)**

Document for: **Discussion and decision**

Agenda Item: TBA

1 Introduction

There seemed to be some confusion at SA3#30, concerning the possible attacks against the stream ciphering (XOR) mechanism, if A5/0- A5/7 are used unmodified in the Voice Group Call Service (VGCS) as proposed in [1]. In order to decide if these concerns are justified or not, this paper summarises the issues raised in 1998 by SMG10 and provides some recommendations, if it is decided that the concerns are still valid.

2 Ciphering Design Principles

An initialisation vector (IV) is used as an input to the ciphering algorithm along with the cipher key to provide the synchronisation at either end. In GSM, the IV is derived from "a counter" of the TDMA frame number carried in the air interface protocol. The use of an XOR function to combine the resulting key steam with the data to be ciphered allows the same mechanism to encrypt and decrypt traffic on the air interface, but unless the input parameters are chosen very carefully to avoid "key stream repeats", an attacker can recover plain text by XORing two related cipher streams.

For 3G, the design of the IV input to the algorithms and cipher key was designed [2], [3] to ensure that:

1 Within one ciphered connection, different data is not ciphered with the same key stream into the XOR function. The cipher key is changed before the IV counter "rolls round" so that a key stream repeat is avoided.

2 Two bearers belonging to the same connection are not ciphered using the same counter and cipher key. A distinguishing bearer id was added as an input to the ciphering algorithm.

3 The uplink and downlink bearers are not ciphered using the same counter and cipher key. A distinguishing direction id was added as an input to the ciphering algorithm.

3 The Vodafone/ Siemens Proposal

It is believed that the Vodafone/ Siemens proposal [1] breaks these principles if:

- There is only one level of key hierarchy, with just a long life key stored on the SIM. It is unlikely that it will be practical to change this key often enough to overcome the "key stream repeat" problem. Unlike keys for individual calls, group keys cannot be automatically derived from the GSM AKA mechanism, which generates a new user specific ciphering key based on K for each call. As well as protecting from key stream repeat, the keys also need to be changed frequently to address the fact that in VGCS, the shared keys are exposed on an unprotected SIM- ME interface. It is noted that to address this issue, a two key hierarchy was proposed by the SMG10 WPA in 1996 [4]. In summary:

    1. At the highest level, a Master Key is used for the distribution of group call keys. The initial values are installed in the SIM of the group members at SIM personalisation. A procedure for over the air point-to-point key updating is foreseen, as it is not expected to occur frequently.

2. At the lowest level, a group call key is derived in the SIM of the group members from the active master key and group call key numbers broadcast over the MCH. Thus the update of GCK is extremely frequent, i.e. a new GCK is generated at each call.

   Recommendation 1: It is recommended that SA3 reconsider the use of a two key hierarchy. Either:

   a) As in TETRA, where GCK is the "Master Key" and the Common Cipher Key (CCK) is the group call key. In TETRA, CCK acts as a short life session key, which modifies GCK to form MGCK which is then used for the actual ciphering [5]

   Or

   b) As in the BAK proposals for MBMS, where BAK is the "Master Key" and "TEK" is the group call key. If the MBMS BAK solution were chosen, then a common approach to management of keys on the UICC may have advantages. [6]

- An attacker monitoring a ciphered group call at a location covered by two or more cell sites, may be able to XOR the ciphered data from overlapping cells, to recover the clear voice transmissions, particularly if the structure of the data is known. It is understood that no distinguishing bearer id has been specified as input to the ciphering process for VGCS.

  Recommendation 2: SA3 should consider the use of additional inputs to the ciphering algorithm e.g. TETRA combines the cipher key with the Carrier Number (CN) and Base station Colour Code (CC) and Location Area identifier (LA) to prevent attacks on the encryption process by replaying cipher text to eliminate the key stream. [5].

- If a common Group Cipher Key is used to cipher an uplink transmission into the group, then the same key stream may be used to cipher a predictable user id, as is used to cipher other predictable data e.g. downlink signalling responses. However, it is not clear if a common Group Cipher Key is used by the uplink, as the original Vodafone analysis [7] states that the service "shall permit only one talking service subscriber at any one time". This suggests that Kc is used for the uplink rather than a common Group Cipher Key. However, this means that there is no explicit authorisation of the uplink transmission into the group. The network has to trust the possibly unauthenticated id to make sure that it is valid to place the call.

  Recommendation 3: A distinguishing direction id may need to be added as an input to the ciphering algorithm.

The subject of user ids and group ids needs further consideration in general, as the concept of TMSI as used in GSM cannot be used for VGCS and certain potential users of the service may be concerned with the exposure of the unprotected real user ids on the radio interface.

4 References

[1] 3GPP S3-030559 Voice Group Call Services, Vodafone, Siemens SA3#30

[2] 3GPP S3-99062 Radio Interface Ciphering, NOKIA, March 1999

[3] 3GPP S3-99081 Security Functionality in the RAN, March 1999

[4) Group Calls Encryption – Outline of the Key Management Method proposed by SMG-SG Tdoc SMG-SG 064/96 (distributed on SA3 list on 23/07/2003)

[5] TETRA Specification ETSI EN 300 392-7 V2.1.19 (2003-05)
(Status submitted to EPT in June 03 for EPT approval prior to submission to Public Enquiry)

[6} S3-030528 Progress report on MBMS 3GPP2 solution, Qualcomm, SA3#30

[7] Tdoc SMG10 98P252 (SMG 10 report on **"**Fraud Review of Advanced Speech Call Items (ASCI), Vodafone, July 1988)