3GPP TSG SA WG3 Security — S3#37 **S3-050165**
21 - 25 February 2005
Sophia Antipolis, France

Title:	**Reply LS** on 'Ciphering of access bursts on VGCS channel'
Response to:	LS S3-050023 (GP-050599) 'Ciphering of access bursts on VGCS channel'
Release:	Rel-6
Work Item:	VGCS
Source:	SA3
To:	GERAN2
Cc:	----

Contact Person:
Name: Blommaert Marc
Tel. Number: +32 14 25 34 11
E-mail Address: Marc.Blommaert@siemens.com

Attachments: S3-050070

1. Overall Description

SA3 thanks GERAN2 for the LS (GP-050599) on "Ciphering of access bursts on VGCS channel" (S3-050023)

SA3 confirms that the attached CR of GP-050599 can be endorsed. The SA3-contribution, that analysed the access network threats (S3-050070) when not ciphering Access Burst for VGCS uplink channel access, is attached for information.

2. Actions

ACTION: None

3. Date of Next TSG-SA3 Meetings

SA3#38	26 – 29 April 2005 Geneva, Switzerland
SA3#39	28 June- 1 July Toronto, Canada

3GPP TSG SA WG3 Security — S3#37 **S3-050070**

21 - 25 February 2005

Sophia Antipolis, France

Source: Siemens

Title: Access burst ciphering for VGCS

Agenda item: VGCS

Document for: Discussion/Decision

1 Introduction

GERAN2 has informed SA3 about a Change Request that clarifies that VGCS access bursts are not ciphered on the uplink VGCS group channel. SA3 is being asked whether using plaintext access bursts (AB) could be a potential security threat to the system. This contribution first clarifies the particular VGCS access burst scenario under concern and then analyses the security risks. It is shown in this contribution that the effects of the attack (when using plaintext AB) are limited and the effect is not worse than a 'brute-force' jamming attack on the VGCS uplink channel. It is also shown that AB ciphering introduces additional complexity for realization which effects would need further investigation by GERAN2, if SA3 cannot endorse the recommendation to use plaintext Access Bursts.

2 Discussion

2.1 Explaining the involved VGCS access burst scenarios.

A) Where & who?

Access Bursts may be sent by the VGCS talker on the UPLINK (MS to network). Access bursts are either sent on the uplink of the group channel or on the dedicated channel allocated to the talker, depending on the message type being sent in the access burst and the channel allocation for the VGCS talker (dedicated or Group Channel).

B) What messages are sent as access burst?

The following messages are sent as access bursts:

a) Handover Access
b) Uplink Access

The content of the access burst depends on the message type:

- Handover Reference (for Handover Access)
- Subsequent Talker indication and random reference (for Uplink Access)
- Uplink Reply (for Uplink Access)

B.1) Handover Access message

The MS may send the Handover Access message as the initial message in the target cell in the case of handover to an unsynchronised cell. The message is sent on a dedicated channel when the VGCS talker is allocated a dedicated channel; otherwise it is sent on the uplink of the Group Channel.

This message is not specific to VGCS. It is also sent by a MS on handover of a CS call to a new cell. For this case the handover access is sent **unciphered**, as stated in 44.018.

B.2) Uplink Access message

The Uplink Access message is sent by the VGCS MS on the uplink of the Group Channel (I.e. shared channel). The message contains 8 bits, with a variable length cause field which can indicate either:

a) **Request permission to talk** (3 bit cause field).
b) Response to network to confirm that there are some listeners in the cell (8 bit cause field).

In case a), the remaining 5 bits contain a random number, generated by the MS. This random reference together with the frame number of the frame in which the burst was sent, are included by the network in the response to the uplink access message (i.e. in the VGCS Uplink Grant). Multiple MS's may simultaneously request the VGCS uplink, but only one MS can be granted the uplink. MS's that send the burst with the same content in the same frame number can be separated later by means of contention resolution (the mobile identity is provided in the Talker Indication and the subsequent response from the network).

In case b), there is no random reference. The network only wants to know whether there are some listeners of the group call in the cell.

It is likely for Release 7 that there will be additional cause-fields within the Uplink Access Message added to identify priority or emergency talker request. From that moment on, it will be possible to pre-empt the current talker e.g. when there is an emergency talker request.

2.2 Threat Analysis

The concern that was raised during GERAN#23 is that an unciphered (i.e. not 'implicitly' authenticated by the VGCS group key) VGCS access burst for uplink access could be a potential tool for a VGCS DoS attack. An attacker (not belonging to the VGCS group) would set the emergency talker bit (a Rel-7 enhancement) within the VGCS access burst for uplink access (See Figure 1 flow), in order to try to obtain uplink channel.

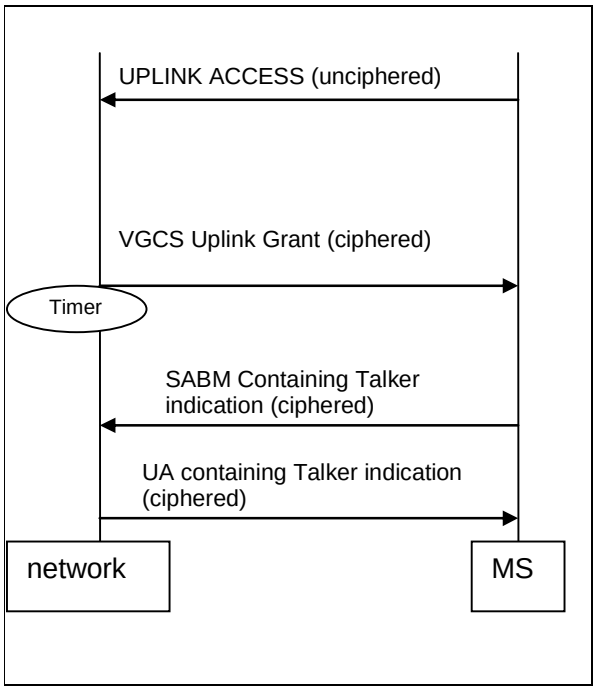

Figure 1: VGCS uplink channel access flow

However as the VGCS Uplink Grant message (which is sent back from the network to the MS) is ciphered using the VGCS group key, and the expected message back (Talker indication) are both ciphered, the attacker will not be able to grab the uplink channel (so respond successfully to the network). A couple of retransmissions of the ciphered uplink grant access message may take place. The introduced delay is dependent on the network configuration (timer value and maximum number of retransmission (Timer T3115- See Annex for a detailed description)).

We distinguish three cases of sending AB. The first and second case refers to the one channel (i.e. uplink VGCS channel for VGCS talker) model, where either the VGCS uplink is busy or free. A third case is using the 1,5 channel model (i.e. the VGCS talker is always put on a dedicated channel), which will be used for high priority and emergency calls in Rel-7. The evaluation of the third case seems very similar as the one channel model with free uplink.

Currently a genuine MS is only allowed to send an UPLINK ACCESS AB on a free uplink channel. (It is legal to send handover access since this MS should be the current talker – only a talker is subject to handover.) If there is a talker on the uplink of the Group Channel and a malicious ME sends an AB on that uplink VGCS channel, then there will be interference on the uplink resulting in lost frames. The AB in this case may not be interpretable by the network.

The result of the attack in the second case (i.e. UPLINK FREE) might be that further VGCS uplink access requests from genuine MS will be delayed (The free VGCS uplink channel stays free) depending on how the network responds to the AB's. This result is not worse than from an attack where garbage frames are sent on the VGCS uplink channel.

An attacker could also blindly attack the free VGCS uplink access channel by sending plain text high priority AB in a repetitive way. Only if the repetitiveness of the access bursts would perfectly fit with the network timer for 'uplink grant access repetition', and no other emergency call AB were received in any other VGCS cell, the attack might result in a disabling of the uplink access allocation. Fortunately, the network function (still to be specified within Rel-7) that will evaluate the priority/emergency of the calls might be made robuster against a repetitive AB-attack. A simple countermeasure could be to assign a lower priority to the UPLINK ACCESS AB of that attacked cell (the cell where the uplink grant access did previously fail). Also if the network determined it was under attack (considered equal to repetitively observing unanswered VGCS Uplink Grants), perhaps the group channel could be reconfigured – i.e. moved to a different location. The reconfiguring message could be sent on the group channel ciphered to move the current listeners and the talker. Sometime later the NCH could be updated for the late entrants.

Conclusion: The use of plain text AB for a ciphered VGCS uplink channel access might only result in a DoS against the uplink channel under certain circumstance. In all cases it will not prevent a dispatcher from talking or will completely disable the current talker. Especially for the Rel-7 enhancement, for which there was a concern, the priority/emergency

evaluation could be made robust to the AB-attack. The (repetitive) AB-attack may be more subtle, but is less efficient than just sending 'garbage' on the VGCS uplink channel. A ciphered AB could mitigate the resulting temporary inefficient uplink or dedicated channel allocation, but has some implementation drawbacks too, as will be analysed later in this paper.

2.3 System impacts for VGCS uplink access burst ciphering

A) Can the access bursts on VGCS uplink (when used by MS using VGCS ciphering) be unciphered in Release-6 but ciphered in Release-7?

No. The access bursts are sent on a shared channel in the case of Uplink Access, so the senders of these bursts may be a mixture of Release-6 and Release-7 MSs. The network does not know from the access burst whether the MS is according to Release-6 or a later or earlier release.

B) Can the access burst be ciphered with the existing A5 algorithms ?

According to 43.020 (Annex C), the A5 algorithm acts on a block of 114 bits. In the case of an access burst, the current block size would only be 36 bits (TS 45.003). Thus some modifications are needed.

There seem to be two possible solutions:

SOL-1: Specify how the output of the A5 algorithm can be applied to less than 114 bits (i.e. 36 bits).

Since the A5 algorithm is used to generate a ciphered key stream, the output could be truncated to 36 bits. With the current weaker A5 algorithms[1], and the (nearly known) short plaintext (only 5-bits random input), a known plaintext, cipher text attack could be tried. If successful, this would result in revealing the cell-dependent VGCS cipher key V_Kc, but not VSTK or V_Ki. Additional random bits could be added to the plaintext, in which case the SOL-2 remarks apply.

SOL-2: Enlarge the access burst length, to fit to the input block size of 114 bits.

Adding additional bits to the access burst (AB) is not desired. The access bursts for VGCS are sent on the uplink of the Group call channel- so this channel is dedicated to this group call in this cell but shared among all listeners of this specific group call in this cell. Since the timing advance is not known in advance and therefore the position of the access burst within the timeslot may vary depending on the position of the sending MS towards the position of the BTS antenna it might not be possible to increase the number of usable bits in AB so easily since this would increase the time needed for transmission of the data and therefore MS located far away from the BTS may violate timeslot boundaries. This non-security issue has to be evaluated by GERAN2 if a ciphered AB is desired.

[1] With a strong ciphering algorithm with a sufficient key length, the attack would not be a concern.

3 Conclusion

This contribution first clarified the VGCS access burst scenario and analysed the security risks. It was shown that the use of plain text AB for a ciphered VGCS uplink channel access might only result in a DoS against the uplink channel under certain circumstance. In all cases it will not prevent a dispatcher from talking or will completely disable the current talker. Especially for the Rel-7 enhancement, for which there was a concern, the priority/emergency evaluation could be made robust to the AB-attack. The (repetitive) AB-attack may be more subtle, but is less efficient than just sending 'garbage' on the uplink or any dedicated channel.

It was also shown that AB ciphering introduces additional complexity for realization which would need further investigation by GERAN2. Hence Siemens proposes that a Liaison Statement is sent back to GERAN2 concluding that the access bursts for VGCS uplink channel access need no ciphering.

4 References

[1] S3-050023 (GP-050599) LS from GERAN2 on 'Ciphering of access bursts on VGCS channel'.

5 Annex (AB handling and timing in Rel-6)

VGCS Uplink Grant is sent ciphered to the MS. Only the MS that has the correct keys on its USIM will be able to decode the VGCS Uplink Grant. The Uplink Grant will contain the Request Reference and some timing advance information. **The Request Reference contains the code that was sent in the Uplink Access together with the frame number of the frame in which that the Uplink Access was sent**. The MS should verify the contents of the Request Reference (i.e. it should contain the contents of the access burst). The network on sending the VGCS Uplink Grant starts a timer – T3115. The timer is stopped on receiving a correctly decoded frame from the MS. If T3115 expires, the network retransmits the VGCS Uplink Grant and restarts T3115. The network may repeat the transmission of VGCS Uplink Grant up to Ny2 times. If T3115 expires Ny2 times, the network marks the link as free and send UPLINK FREE on the group channel. The values of T3115 and Ny2 are network dependent.

After the MS receives a VGCS Uplink Grant, it may then send a **Talker Indication that contains the MS identity**. This information is sent in a SABM frame. The MS then expects to receive a UA that contains the same information as sent in the SABM. The network can only grant uplink access to one MS at a time. Thus if two MS's respond to the VGCS Uplink Grant by sending Talker Indication, only one of these will be accepted by the network.

If a badly behaving MS sent the access burst on the uplink, and the network granted the uplink to it, then the Uplink could be incorrectly seized for T3115 times Ny2. The badly behaving MS could then reattempt to gain Uplink access, thus preventing other MSs from accessing the uplink. However, note that MS should only transmit access bursts if the link has been marked as free. The MS may retransmit the access burst after 100 ms provided that the link is still free.