3GPP TSG SA WG3 Security — S3#15 **S3-000630**

12-14 September, 2000

Washington D.C., USA

Source: **S3**[1]

To: **GERAN**

Copy: **T3, S1, R2**

Title: **Modification of pre-configuration information**

S3 thank GERAN for their liaison statement on the modification of pre-configuration information (GP-000265).

S3 have studied the threat identified by GERAN and acknowledge that a denial of service attack, which takes effect after the attacker has become inactive, is possible. However, it is felt that the proposed solution should not be pursued because of the following limitations:

- Encrypting the pre-configuration information using a stream cipher offers limited protection against this threat. Even if the mobile only accepts encrypted pre-configuration information, a false base station may still be able to send misleading pre-configuration information since it may be possible to identifying the portion of ciphertext corresponding to known plaintext representing the pre-configuration data. The false base station will then be able to toggle appropriate bits in the ciphertext in order to modify the plaintext in a predictable way to cause a subsequent GSM to UMTS handover to fail.

- Similar attacks are conceivable where a false base station modifies signalling information to cause a subsequent GSM to GSM handover to fail. For this reason it is believed that there is little benefit in attempting to prevent denial of service attacks which cause a subsequent GSM to UMTS handover to fail.

S3 believe that an effective countermeasure would require significant enhancements to the GSM security architecture, in particular the introduction of a dedicated integrity protection mechanism. It is expected that such enhancements will be developed in an integrated way in future releases of the specifications as part of the GERAN security work item.

---

[1] Contact: Peter Howard, email: Peter.Howard@vf.vodafone.co.uk

12-14 September, 2000

Washington D.C., USA

3GPP TSG GERAN #1 **Tdoc GERAN GP-000265**
Seattle, USA
28 August – 1 September 2000 ***Agenda item 7.6***

From : TSG GERAN
To : S3, T3
Cc: RAN WG2, S1

Liaison Statement on preventing unciphered writing/overwritting of pre-configuration fields by the HPLMN

Background

When performing a handover from GSM to UMTS, the UE needs to know the transport format to use when accessing the new channel on WCDMA. Unlike GSM, with UMTS these formats will require a large amount of information. This cannot be passed during the Handover Command procedure and therefore the information is passed to the UE in advance, at a period that is less "time critical".

Therefore, when registered on a GSM BSS the UE receives a set of UMTS pre-configurations (e.g. in conjunction with the Location Update procedure). For information, up to 16 different pre-configurations (tagged with a pre-configuration identity) can be defined for a given PLMN, each of them tagged with a version number. Later, when a handover to UMTS is performed, the BSC sends the *Inter System To UTRAN Handover Command* message to the UE, including the pre-configuration identity that shall be used when establishing the UMTS channel.

However, the following situation has been spotted:

A false GSM BTS could maliciously send misleading pre-configurations to the UE so that when the UE comes back to a real BTS, a subsequent handover to UMTS may fail. This is a denial of service attack which persists after the false BTS attacker has been active.

Several solutions are possible to try to avoid this problem : After failure, the UE that re-connects to the GSM channel(s) could send the Handover failure message with a new cause value indicating that the failure was due to an incorrect pre-configuration. Another solution would be that the BSC runs counters to detect failures, notices this behaviour and then overwrites the pre-configurations with the correct values.

It is possible, for a network operator using ciphering, to help guard against this problem at source by indicating to the UE belonging to its network that unciphered writing/overwriting of the preconfiguration fields are not allowed by the HPLMN. This could be done by including a one bit flag on the USIM to indicate whether unciphered writing/overwriting of the preconfiguration field by the HPLMN is permitted. For the case of VPLMNs, the home network cannot know if the VPLMN will or will not support ciphering, hence there is no need to specify this bit for the fields allocated to the VPLMN.

In addition, we believe that the case of a GSM only SIM plugged into a dual GSM-UMTS UE should be considered. As in this case handover to UMTS cannot be performed, one view would be for the

default value of this bit to specify that unciphered writing/overwriting by the HPLMN is not allowed. This would help guard against a false BTS from forcing a handover to UMTS to fail when a UMTS-capable USIM is inserted and the terminal tries to use misleading pre-configurations set by the false BTS when a GSM-only SIM was previously inserted.

We thank S3 and T3 for their help in this matter in making their efforts to solve it for Release ’99.

Contact person:

Name: Claude Arzelier
Company: Vodafone Group
Telephone: +44 1635 673573 **Fax**: +44 1635 231767
E-mail: mailto:jose-luis.carrizo@vf.vodafone.co.uk