3GPP TSG SA WG3 Security — S3#11 **S3-000169**

22-24 February, 2000

Mainz, Germany

Source: TSG SA WG3

To: TSG RAN WG3

Title: RANAP Signalling procedures in case of Unsuccessful Integrity check

In answer to RAN3's first question: yes, in R99 the integrity protection mechanism is applied to signalling only. In answer to the second and third questions, it should be noted that the attached CR approved by S3 proposes that the CN should simply release the connection after receiving an indication from the UTRAN that integrity checking has repeatedly failed.

The reasons for withdrawing the ability to allow the UTRAN to trigger a re-authentication are listed below:

1. The primary reason for allowing the UTRAN to trigger a re-authentication in the event of repeated integrity check failures was to recover from a mismatch in the integrity keys (IK) at the UE and RNC. Performing a re-authentication during the connection would establish a new IK at the UE and RNC and thereby allow the connection to resume in an integrity protected mode. A major problem with this approach is the fact that the UTRAN must be able to transfer the authentication messages without integrity protection in the special case that the authentication is triggered because of suspected IK mismatch. If special procedures need to be implemented to 'suspend' integrity checking during a connection, then new risks will be introduced (e.g. the likelihood of software errors in the integrity protection mechanism implemented UE or RNC is increased). Therefore, it is important to re-evaluate the value of this mechanism by considering the likelihood of an IK mismatch; two observations have been made:
   - The first observation is that the key generation is always coupled with the full mutual authentication between the user and the network. This means, in particular, that if a wrong IK were to be computed in the UE because of a transmission error on the radio interface, then there is a very high probability that the authentication fails completely. This is implied by the fact that the random challenge is always associated with a message authentication code inside the authentication token AUTN. This message authentication code is calculated in both the USIM and the 3G-AuC based on the secret authentication key of the subscriber. Furthermore, if the wrong authentication vector were selected in the core network (e.g. because of database problem), then the authentication will also fail and an IK will not be established.
   - The second observation is that an IK mismatch may be caused by transmission errors between the USIM and the UE, between the core network and the RNC, or between an old RNCs (or GSM BSC) and the new RNC after a handover. Although S3 is not qualified to estimate the probability of these errors, it is believed to be unlikely that errors that only affect the IK, and that do not result in the message being rejected completely, are extremely rare.

2. Another reason for allowing the UTRAN to trigger a re-authentication in the event of repeated integrity check failures was to guard against denial of service attacks where an attacker injects messages with invalid integrity check codes into the channel. In such a case it was felt that there should be an opportunity for the core network to run the full authentication protocol. However, on examination this seems to do little to solve the problem, and it may even exacerbate it (e.g. the attacker can effectively force the network to use many authentication vectors in a short period of time by injecting messages with invalid integrity check codes into the channel). Although it seems that little can be done to completely eliminate this type of denial of service attack, it is desirable that the core network has some visibility of suspected attacks. Therefore, it is proposed the CAUSE parameter in the RAB RELEASE REQUEST message be retained.

TSG-RAN Working Group 3 meeting #10
Gothenburg, Sweden, 24th – 28th January 2000

TSGR3#10(00)0400

Source: RAN WG3

To: TSG SA WG3

Title: RANAP Signalling procedures in case of Unsuccessful Integrity check

Cc:

Contact Person: Brendan McWilliams
E-mail: brendan.mcwilliams@vf.vodafone.co.uk
Tel: +44 1635 676264

RAN WG3 have noted within the TS 33.102 v3.3.0 (*Security Architecture)* specification (Section 6.4.6), the situation whereby the RNC can request the CN to perform a re-authentication when the current CK and IK in use, cannot be used.

- Can TSG SA WG3 confirm that Integrity checking is applied to signalling only?

RAN WG3 believe that the RNC should be able to indicate to the CN that such a scenario has occurred, and a solution within RAN WG3 is available for this implementation.

One such solution involves the RNC informing the CN by sending a *RAB RELEASE REQUEST* message (once for every signalling message that has Integrity Checksum failed) with a Cause value indicating that the reason for this request is due to integrity failure. The *RAB Release Request* procedure will be amended such if the CN receives such a message it does not mean that the RAB shall be released, rather it *should* be released. Therefore it is the decision of the CN to decide what actions should be taken – try re-authentication or if problem persists, release the RAB itself.

- Regarding the 'failure situation persists' text, at what point does the CN ignore the 'Security Check Request' from the UTRAN i.e. how many times shall the CN ignore the *RAB RELEASE REQUEST* from the RNC indicating that Integrity checking has failed, before releasing RABs, and ultimately the call?

Regarding Authentication, it was accepted that Authentication Response (within the *DIRECT TRANSFER* RANAP message) must be sent to the CN even in this integrity failure scenario. However it was unclear to RAN WG3 what the RNC should do when integrity fails:

- Does the RNC **stop transfer** of all RANAP messages or permit the transfer of **selected** RANAP messages when Integrity Check failure occurs – Can TSG SA WG3 clarify this?

If selected messages only, are allowed to be passed to the CN e.g. Direct Transfer (for Authentication Response), does the *DIRECT TRANSFER* message require an indication that Integrity checking has failed, or is it sufficient to include this only in the *RAB RELEASE REQUEST* message?