TSG-RAN meeting #14 **RP-010942**
Kyoto, Japan, 11-14 December 2001

Source: **TSG-RAN**

To: **TSG-SA, TSG-SA WG3**
Cc: **TSG-RAN WG2**

Title: **Draft liaison on Ciphering of SRBs**

Contact: Bruno Schuffenecker

Email: bruno.schuffenecker@francetelecom.com

Tel: +33 1 45 29 67 36

Fax: +33 1 45 29 41 94

During TSG RAN#14, a proposal of separating user and signalling planes for ciphering has been discussed for Release 99 (see attached document). The main purpose would be to disable ciphering on the Control plane only i.e. RRC and DTAP would be in clear (thus keeping user data encrypted) for monitoring and radio investigation purposes on the Iub interface as explained in attached document RP-010909.

Given its ongoing work on active correction of the ciphering feature in the Rel'99 specifications, RAN 2 will study and report to TSG RAN on the consequences of separating the user and control planes for ciphering in Rel'99 specs by March 2002 plenary. in parallel to this feasibility analysis by TSG RAN, TSG RAN kindly asks TSG SA to give its views on the subject.

Action:
To SA1: provide feedback on service requirement
To SA3: to confirm that it would be acceptable from a on security standpoint

Attached: doc RP-01909

TSG-RAN Plenary #14
Kyoto, Japan, 11 - 14 November 2001

RP-010909

Source : France Telecom

Title : Ciphering on SRB

Agenda Item : 8.2

Document for : Discussion and decision

1. Introduction

In order to investigate problems of interworking between a mobile and the network, an operator should be able to analyse protocol data exchanged over the Iub interface.

On GSM and GPRS networks, there are many softwares using A and Abis captures. These softwares are used to observe and optimise the network. Operators should be able to connect such tools on the open Iub interface as it is done today for GSM systems.

As a consequence an operator should have an access to Iubis signalling on its UMTS network.

Using ciphering on the network will make the operator unable to easily capture and analyse signalling data on the Iub interface.

Indeed, when the ciphering is activated, it should be applied on all the radio bearers of a mobile for a given core network domain.

The purpose of this document is to explain the advantages we get in analysing Iub traces and then to propose an intermediate solution to be able to get signalling information without deactivating ciphering on user data. This proposal should be applied as an option for all the mobiles in networks.

3. Description of the need

Any interworking problem between a mobile and the network must be investigated over the Iub interface. It is the only point of the network where it is possible to get the RRC dialog between the mobile and the network. Problems of interworking will concern such critical functions as radio resources management, macro diversity. As a consequence, an operator must have an access on every Iub interface of its network in order to be able to trace a given mobile.

Moreover, many tools are developed to analyse data captured over GSM and GPRS interfaces. These tools are today very useful on GSM systems. Without these tools, it would be much more difficult to observe, optimise the network and to investigate problems.

UMTS is then the first system in Europe using CDMA. With this technology, optimisation will depend on the load and traffic on the network. As a consequence, investigating and observing the network over the Iub interface will be more useful and critical for UMTS than for other existing systems.

2. Discussion

We propose to not change the protocol but to give a different interpretation, modifying only the behaviour of the mobile and the UTRAN. The ciphering is started separately for each radio bearer. The starting point is given for each radio bearer by the messages Security Mode Command and Security Mode Complete. In case the signalling is not ciphered this starting points should not be given for signalling radio bearers.

The operator could choose among the three following options:

1) No ciphering activated

2) Ciphering activated on user data only

3) Ciphering activated on user data and signalling data

The RNC shall use this option to cipher all its mobiles.

In case the third option is chosen (ciphering activated on user data and signalling data) the UTRAN and the MS would behave as specified until now.

In case the second option is chosen.:only data radio bearers could be ciphered. Signalling Radio Bearers would not be ciphered.

The SECURITY MODE COMMAND message contains the ie Ciphering Mode info :

This ie contains time info for activation for each radio bearer. In order to indicate to the mobile that ciphering shall not be applied to signalling radio bearers, the network should not mention these radio bearers in the ie "Radio bearer downlink ciphering activation time info"

When the mobile responds with the SECURITY MODE COMPLETE message, it shall also not mention the signalling radio bearers in the ie "Radio bearer uplink ciphering activation time info"

4. Conclusions and Proposals

In this paper, we propose a solution to allow the ciphering of user data without ciphering signalling data. Since it would not be mandatory to transmit signalling data without ciphering, the operator would still be able to choose the security level for its network, considering his needs for investigation over the Iub interface.

Since ciphering sections in RAN2 specifications Release 99 are under active correction process, we propose that this SRB ciphering issue be considered in next coming RAN2 meetings. As a late proposal for Release 99, we also understand that interworking issues need to be carefully investigated and security aspects need also to be checked by SA3.

We propose to have technical discussions on this subject next RAN2 meeting and inform SA3 on the issue. In case this solution is agreed, France Telecom would draft the associated change request.

References

[1] 3GPP TS 33.102 V3.9.0 (2001-06), “Security Architecture”.