TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) **TSGR2#6(99)832**
Sophia Antipolis, France, August 16th to 20th 1999

Agenda Item:

Source: Nortel Networks

Title: Impact of two cipher key solution on multiplexing at RLC and MAC level

Document for: Discussion

Introduction

Due to separate MM signalling, the UE establishes separate ciphering keys for the CS and for the PS domain [1]. In the two-key solution, the CS-domain bearers are ciphered with the most recent cipher key agreed between the user and the 3G-MSC (Kc-CS). The PS-domain bearers are ciphered with the most recent cipher key agreed between the user and the3G-SGSN (Kc-PS). The signalling link is ciphered with the most recent cipher key established between the user and the network, i.e., the youngest of Kc-CS and Kc-PS.

This paper studies the impact in the RLC and MAC layer of the use of two different cipher keys, and proposes the use of a field to indicate the associated domain type.

RLC AM and UM mode

Ciphering is performed in the RLC sub-layer for a non-transparent RLC mode (AM or UM)[2]. There are four input parameters for the ciphering algorithm, which are Transmission Direction, Ciphering Sequence Number (CSN), Ciphering Key (Kc) and ID.

A new cipher key Kc is created each time that an authentication procedure is executed between the USIM and the CN that initiates the authentication. The cipher key Kc is then sent from the CN node to the RNC and from the USIM to the UE [3].

One cipher parameter is the Radio Bearer ID that indicates the logical channel identity. During the Radio Access Bearer Establishment procedure, one RAB is mapped to one Radio Bearer [4]. The mapping involves the assignment of one RLC instance, and associated parameters that needed to configure the RLC, MAC and L1 layers. Each logical channel is ciphered independently.

It is possible that one user may receive several services from both CS and PS domain simultaneously. In this case, the user may be assigned multiple RAB IDs. Each RAB ID corresponds to one RLC instance. The RLC instance could be UM or AM. Each specific RAB ID must have an associated Kc. This Kc could either be Kc-CS or Kc-PS. Note that CS-domain bearers must be ciphered with the Kc-CS, and PS-domain bearers must be ciphered with the Kc-PS. To ensure performing the right ciphering function at the RLC layer, two conditions must be met:

- Each logical channel can only transfer the information either from CS-domain or PS-domain, but not from both.
- The RLC layer should know which domain that each ID and Kc belongs to.

RLC TM mode

Ciphering is performed in the MAC-d sub-layer for a transparent RLC mode. Similarly, it is possible that UE may receive services from both CS and PS domain. For example, UE may receive a voice call from Cs-domain, and at the same time, have services from Ps-domain (e.g. voice over IP). In this case, the MAC must apply the appropriate Kc for each bear from different service domain

At the Radio Access Bearer Establishment procedure, if a RAB is mapped to a RLC TM instance, the SRNC will send the associated Kc to the MAC layer. The MAC layer should know the domain types for both logical channel and Kc in order to perform the right ciphering function.

Proposal

It is proposed to add a field to indicate the associated domain of the logical channel ID and ciphering key. We propose to add the following text in the document TS 25.301 "Radio Interface Protocol Archetecture" section 8 "Ciphering":

In the two-key solution, the CS-domain bearers are ciphered with the most recent cipher key agreed between the user and the 3G-MSC (Kc-CS). The PS-domain bearers are ciphered with the most recent cipher key agreed between the user and the3G-SGSN (Kc-PS). The signalling link is ciphered with the most recent cipher key established between the user and the network, i.e., the youngest of Kc-cs and Kc-PS.

To ensure performing the right ciphering function at the RLC and MAC layers, two conditions must be met:

- *Each logical channel can only transfer the information either from CS-domain or PS-domain, but not from both.*
- *The RLC layer should know which domain that each ID and Kc belongs to.*

A field in the logical channel ID and Ciphering Key Kc should be used to indicate the associated domain type.

References

[1] 3G TS 33.102, "Security Architecture".
[2] TS 25.301, "Radio Interface Protocol Architecture"
[3] Tdoc 3GPP S3-99081, "Security functionality in the RAN"
[4] TS 25.331, "RRC Protocol Specification".