TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) **TSGR2#6(99)829**
Sophia Antipolis, France, August 16th to 20th 1999

Agenda Item: 14

Source: Nortel Networks

Title: Procedure to change ciphering key of the signalling connection in Two-key solution.

Document for: Discussion

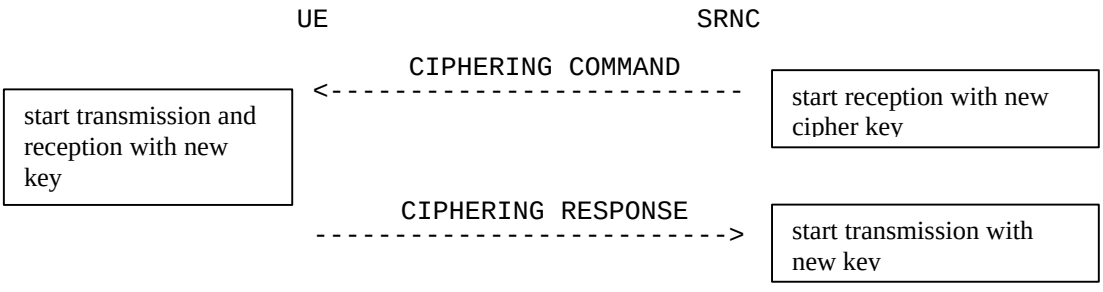
Introduction

In the 3GPP ciphering model, the UE establishes separate ciphering keys for the CS and for the PS domain. Each ciphering key is calculated during the authentication procedure between UE and SGSN or between UE and MSC.
In the two-key solution option, the CS-domain bearers are ciphered with the most recent cipher key agreed between the user and the 3G-MSC (CK-CS). The PS-domain bearers are ciphered with the most recent cipher key agreed between the user and the3G-SGSN (CK-PS). The signalling link is ciphered with the most recent cipher key established between the user and the network, i.e., the youngest of CK-CS and CK-PS.
This means in particular that the cipher key of the signalling connection has to be changed each time a new cipher key is established with any one of the CN nodes.
This paper discusses the requirements for a procedure on the radio interface to change the cipher key of the signalling connection and also for an ongoing user data connection.

Cipher key for the signalling link

After the authentication procedure with a CN node, the cipher key will be available in the UE. The CN also sends a RANAP CIPHER MODE COMMAND in order to transfer cipher information to the RNC, including the cipher key.

At that point in time, both the UE and the SRNC know the ciphering key associated to the CN node. There must then be a procedure to ensure coordination of the instants when ciphering starts (or stops) on the UE and the SRNC side. This procedure is initiated by the SRNC by sending e.g. an RRC CIPHERING COMMAND to the UE. After sending the message, the SRNC configures its signalling link to start receiving in ciphered mode. When the UE receives the message, it configures both to start sending and receiving in ciphered mode. Finally when the SRNC receives, either a CIPHERING RESPONSE, or a correctly deciphered L2-PDU, it starts sending in ciphered mode.



The same procedure is applicable both in the case when the UE establishes the first cipher key with one CN domain, and to the case when the UE already has at least one cipher key that is currently used to cipher the signalling link and is establishing a new cipher key, or when the connection to one of the CN domains is released.

In the last two cases, the CIPHERING COMMAND message would be used to trigger switching from one cipher key to the other, and the CN domain identifier parameter could be used to specify which key has to be applied. This would actually be the key that has most recently been received by the SRNC.

Cipher key for a Radio Access Bearer

It is a security requirement that the same cipher key must not be used for an unlimited period of time, in order to avoid malicious attacks.
A mechanism has been defined in 3G TS 33.102 "Security architecture" to avoid an infinite cipher key lifetime: Each time an RRC connection is released the highest value of the hyperframe number of the bearers that were protected in that RRC connection is stored in the USIM. When the next RRC connection is established that value is read from the USIM and incremented by one. The USIM triggers the generation of a new cipher key (and an integrity key) if the counter of HFN values reaches a maximum value set by the operator and stored in the USIM at the next RRC connection request.

With this mechanism, the same cipher key would potentially be in use for the duration of an RRC connection. This might be too long a period, as an RRC connection can last several days. It might be necessary to change the cipher key at any time during an RRC connection, and in particular during an on-going data transfer.

In such a case, there has to be a synchronised procedure between SRNC and UE to change the cipher key, to avoid data loss. The same asymmetric mechanism as above can be used : the SRNC sends a CIPHERING COMMAND with an indication of the Ciphering Sequence Number (CSN-start) when the new cipher key is to be applied, and configures to decipher with the new cipher key at CSN-start, but continues to encipher data with the old key. When the UE receives the message, it sends a CIPHERING RESPONSE message, starts sending with the new cipher key at CSN-start, and configures to receive with the new cipher key after a round-trip delay period. When the SRNC receives the message, it starts transmitting with the new key. Note that this mechanism is similar to the "Asymmetric transport channel reconfiguration" presented in Tdoc R2#4(99)423, except that NodeBs are not involved.

Proposal

It is proposed to add a new RRC procedure in S25.331 with a CIPHERING COMMAND message, according to the above principles.