TSG-RAN Working Group 2 meeting #3
13 – 16 April 1999
Yokohama, Japan

TSGR2#3(99)271

3GPP TSG SA WG3 (Security)
Stockholm, 23-26 March, 1999

3GPP S3-99081

Agenda Item: 12.2

Source: TSG SA WG 3

Title: Security functionality in the RAN

Document for: TSG RAN WG 2

1. Encryption

TSG SA-3 “3G Security” would like to inform TSG RAN on the following working assumptions which should form the basis of the work on the design of an encryption mechanism:

1) **End-point of encryption.** Encryption is ended at the terminal at the user end and at the RNC at the network end, for both CS and PS user data connections, as well as for signalling data connections.

2) **Ciphering algorithm.** The data flow on dedicated channels is ciphered by means of a bit per bit stream cipher generated by an algorithm called UEA (UMTS Encryption Algorithm).

3) **Cipher key agreement.** The cipher key is agreed by means of the execution of a user authentiation protocol run initiated by either the 3G PS CN node or the 3G CS CN node. The output of the user authentication protocol between MS and the 3G CN node provides a shared secret cipher key CK between the two entities.

4) **Start of ciphering.** Ciphering is invoked by the network by means of a signalling message sent from the 3G CN node. At that instanct the cipher key CK is sent from the 3G CN node to the RNC and from the USIM to the terminal.

5) **Cipher key selection.** TSG SA-3 currently considers two options for the selection of cipher keys:

   a) ***Two key solution.*** The CS user data connections are ciphered with the most recently cipher key CK_{CS} agreed between the user and the 3G CS CN node. The PS user data connections are ciphered with the most recently cipher key CK_{PS} agreed between the user and the 3G PS CN node. The (common) signalling data connections are ciphered with the most recently cipher key established between the user and the network, i.e., the youngest of CK_{CS} and CK_{PS}. This requires that the cipher key of an (already ciphered) ongoing signalling connection is changed. This change should be completed within five seconds after an authentication and key establishment protocol has been executed.

   b) ***One key solution.*** All connections (CS user data, PS user data and signalling data) are ciphered with the most recently cipher key CK agreed between the user and the network, i.e., the youngest of CK_{CS} agreed between user and 3G CS CN node and CK_{PS} agreed between user and 3G CS CN node. This requires that the cipher key of any (already ciphered) ongoing connection is changed. This change should be completed within five seconds after an authentication an key establishment protocol has been executed.

   Both options are acceptable from our point of view. TSG SA-3 would therefore like the views of TSG RAN WG 2 on the complexity of both solutions such that this can be taken into account to decide which mechanism to adopt.

6) **Synchronisation.** Before or at the start of ciphering an initial hyper frame number should be established between the terminal and the RNC on a connection-per-connection basis. This hyper frame number is subsequently incremented in a synchronized way at both sides and is an input to the ciphering algorithm that produces the cipher stream.

7) **Avoid multiple use of the same cipher stream.** The use of the same cipher stream on more than one data stream should be avoided. Therefore,

a) when two bearers (belonging to the same connection) are ciphered using the same hyper frame number and cipher key, then a distinguishing BEARER ID should be an input to the ciphering algorithm as well;

b) when the uplink and downlink bearer are ciphered using the same hyper frame number and cipher key, then a distinguishing DIRECTION ID should be an input to the ciphering algorithm as well.

In order to complete the work on the design of a ciphering mechanism TSG-SA 3 requests for a joint meeting between TSG-SA 3 and TSG-RAN 2.

2. Data integrity

Integrity protection mechanism is introduced in 3G because some critical signaling must be authenticated independently. The idea is to prevent active attacks on radio interface which may cause damage to the user and/or to the network by, e.g., connection hijacking.

The mechanism appends a message authentication code, e.g. 16 bits, to each sensitive message. These bits are calculated by a specific standard algorithm the inputs to which include at least:

– current integrity key (e.g. 128 bits)

– essential message content

– time-varying parameter which must be fresh to preclude replay attacks.

So far, the following sensitive signaling messages are identified:

a) from MS to SN:

- MS capabilities, including authentication, ciphering and integrity algorithm capabilities
- Security mode accept/reject message
- Called party number in a mobile originated call
- Periodic message authentication messages

b) from SN to MS:

- Security mode command, including whether ciphering is enabled or not and the ciphering and integrity algorithms that are used
- Periodic message authentication messages.

However, this seems not to be a complete list. TSG SA WG3 considers the possibility to protect all signaling in layer 3 as oposed to a limited set of signalling messages if that proves more efficient. Sensitive messages not on the above list that could, nevertheless, be integrity protected include messages related to handovers, various location updates and detach. Some RAN signaling could also be referred here, especially URA update, cell update, intra-RAN handovers and channel allocation for dedicated channels. In order to assist SA WG 3 in finding out whether or not there are significant security threats SA WG3 would like to make use of the knowledge of RAN WG2 in a joint meeting.

If some RNC-terminated signalling also requires integrity protection the functionality must be placed in RNC. Appending a message authentication code to signaling messages introduces some overhead. The effects of this should be taken into account in RAN WG2.

The co-location of the integrity protection mechanism and the ciphering mechanism is an option that we are considering and may have advantages from the point of view of key management. Also, the hyperframe number used for encryption synchonisation can be used as a time variant parameter for the integrity protection function to prevent replay attacks.

Some technical problems may arise with protection of location update requests due to the fact that the integrity key must be transferred to RNC before an integrity check can be performed.

RAN WG2 is also encouraged to study whether there are additional uses for a message authentication code for non-security related purposes, e.g., detection of errors due to noise.