3GPP TSG SA WG3 Security — S3#21 S3-010617

27 - 30 November, 2001

Sophia Antipolis, France

Source: Nokia

Title: Proposed changes to 33.210 about protecting GTP-U

Document for: Discussion

Agenda Item:

This contribution proposes clarifications to the text concerning GTP-U protection. It is edited with change marks against 33.210 v. 0.6.0.

6 Security protection for GTP

This section details how NDS/IP shall be used when GTP is to be security protected.

6.1 The need for security protection

The GPRS Tunnelling Protocol (GTP) is defined in 3G TS 29.060 [5]. The GTP protocol includes both the GTP control plane signalling (GTP-C) and user plane data transfer (GTP-U) procedures. GTP is defined for Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs.

GTP-C is used for traffic that that is sensitive in various ways including traffic that is:

- critical with respect to both the internal integrity and consistency of the network
- essential in order to provide the user with the required services
- crucial in order to protect the user data in the access network and that might compromise the security of the user data should it be revealed

Amongst the data that clearly can be considered sensitive are the mobility management messages, the authentication data and MM context data. Therefore, it is necessary to apply security protection to GTP signalling messages (GTP-C).

GTP-U carries the control planes of the user application protocols (e.g. FTP, non-IMS SIP, and telnet). They, too, may contain sensitive data, like usernames and passwords. However, distinguishing application control packets from data packets within GTP-U is not feasible. Protecting the whole GTP-U will be left to the discretion of the operators, but should be implemented whenever the data path includes a public hop (using either IPSec mechanisms or other mechanisms, e.g. link layer encryption).

Network domain security is not intended to cover protection of user plane data and hence GTP-U is not protected by the NDS/IP mechanisms defined in this document.

6.2 Policy discrimination of GTP-C and GTP-U

SGNs must be able to discriminate between GTP-C messages, which shall ~~receive~~be protected~~ion~~, and other messages, including GTP-U, that may~~shall~~ not be protected by IPSec. Since GTP-C is assigned a unique UDP port-number in (TS29.060, [5]) IPsec can easily distinguish GTP-C datagrams from other datagrams that may not need IPsec protection.

As discussed in section 5.2.2 the Security Policy Database (SPD) is consulted for all traffic (both incoming and outgoing) and it processes the datagrams in the following ways:

- discard the datagram
- bypass the datagram (do not apply IPsec)
- apply IPsec

Under this regime GTP-U will simply bypass IPsec while GTP-C will be further processed by IPsec in order to provide the required level of protection. The SPD has a pointer to an entry in the Security Association Database (SAD) which details the actual protection to be applied to the datagram.

NOTE: Selective protection of GTP-C relies on the ability to uniquely distinguish GTP-C datagrams from GTP-U datagrams. For R99 and onwards this is achieved by having unique port number assignments to GTP-C and GTP-U. For previous version of GTP this is not the case and provision of selective protection for GTP-C for pre-R99 versions of GTP is not possible