3GPP TSG WG SA5 –Security SA3#15 **S3-000607**
12-14, September, 2000
Washinton D.C., U.S.A.

Title: **Protection of GTP Messages using IPSec**

Source: **TSG SA WG3**

TO: **TSG CN WG4**

Contact Person:

Name: Lily Chen

LCHEN1@email.mot.com

S3 welcomes this opportunity to convey to N4 some recent progress on IP-based network security.

S3 has been studying the problem of protecting communications links between the elements that comprise 3G networks. For the case of IP-based networks, S3 believes that the methods developed by the IETF, namely components of the IPsec protocol, should be applied for protection of GTP messages.

S3 is currently working on a draft specification for network domain security, which describes the mechanics to establish and distribute a “security association” (SA) between network elements. Security functions are applied to the GTP headers and payloads in accordance with the IPsec parameters as established in the SA. The use of IPsec permits security services to be added to GTP packets without the need for technical modifications to 3GPP TS 29.060.

S3 recommends that GTP-C messages be protected by IPsec because of the sensitivity of the information carried by these messages. GTP-C protection should be mandatory for TS 29.060 R00, and all releases going forward. S3 notes that R99 systems may be retrofitted for IPSec protection even though R99 is beyond the point of revision.

GTP-U messages are expected to have access to protection at higher layers of the IP protocol stack. If higher-layer protection is employed, the use of IPsec for GTP-U would be unnecessary and would introduce a data overhead. However, it is possible to apply IPSec to GTP-U as well.

Note that the selected use of IPsec cannot be applied to 09.60 R97 and R98 because these earlier releases do not permit GTP-C messages to be distinguished from GTP-U messages.

S3 recommends that a minimal CR be written against TS 29.060 R00 to alert the reader that IPsec shall be applied to GTP-C and that IPsec may be applied to GTP-U. A sample CR is shown in the brief sections that follow.

3GPP TSG WG SA5 –Security SA3#15 **S3-000607**
12-14, September, 2000
Washinton D.C., U.S.A.

1 Scope

The present document defines the second version of GTP used on:

- the Gn and Gp interfaces of the General Packet Radio Service (GPRS);
- the Iu, Gn and Gp interfaces of the UMTS system.

NOTE: The version number used in the message headers is 0 for the first version of GTP described in GSM 09.60, and 1 for the second version in 3GPP TS 29.060.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3G TR 21.905: "3G Vocabulary".

[2] 3G TS 23.003: "Numbering, addressing and identification".

[3] 3G TS 23.007: "Restoration Procedures".

[4] 3G TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[5] 3G TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols-Stage 3".

[6] 3G TS 29.002: "Mobile Application Part (MAP) specification".

[7] 3G TS 25.413: "UTRAN Iu interface RANAP signalling".

[8] 3G TS 33.102: "Security Architecture".

[9] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[10] GSM 03.64: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Overall description of the GPRS Radio Interface; Stage 2".

[11] GSM 04.64: "Digital cellular telecommunications system (Phase 2+); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) Layer Specification".

[12] STD 0005: "Internet Protocol", J. Postel.

[13] STD 0006: "User Datagram Protocol", J. Postel.

[14] RFC 1700: "Assigned Numbers", J. Reynolds and J. Postel.

[15] RFC 2181: "Clarifications to the DNS Specification", R. Elz and R. Bush.

[16] 3G TS 23.007: "Restoration Procedures".

[17] RFC 2406 "IP Encapsulating Security Payload"

[18] RFC 2402 "Authentication Header"

[19] RFC 2401 "Security Architecture for IP"

4 General

The present document defines the GPRS Tunnelling Protocol (GTP), i.e. the protocol between GPRS Support Nodes (GSNs) in the UMTS/GPRS backbone network. It includes both the GTP control plane (GTP-C) and data transfer (GTP-U) procedures. It also lists the messages and information elements used by the GTP based charging protocol GTP', which is described in GSM 12.15.

GTP is defined for the Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs. Only GTP-U is defined for the Iu interface between Serving GPRS Support Node (SGSN) and the UMTS Terrestrial Radio Access Network (UTRAN).

On the Iu interface, the Radio Access Network Application Part (RANAP) protocol is performing the control function for GTP-U.

GTP' is defined for the interface between CDR generating functional network elements and Charging Gateway(s) within a PLMN. Charging Gateway(s) and GTP' protocol are optional, as the Charging Gateway Functionality may either be located in separate network elements (Charging Gateways), or alternatively be embedded into the CDR generating network elements (GSNs) when the GSN-CGF interface is not necessarily visible outside the network element. These interfaces relevant to GTP are between the grey boxes shown in Figure 1.

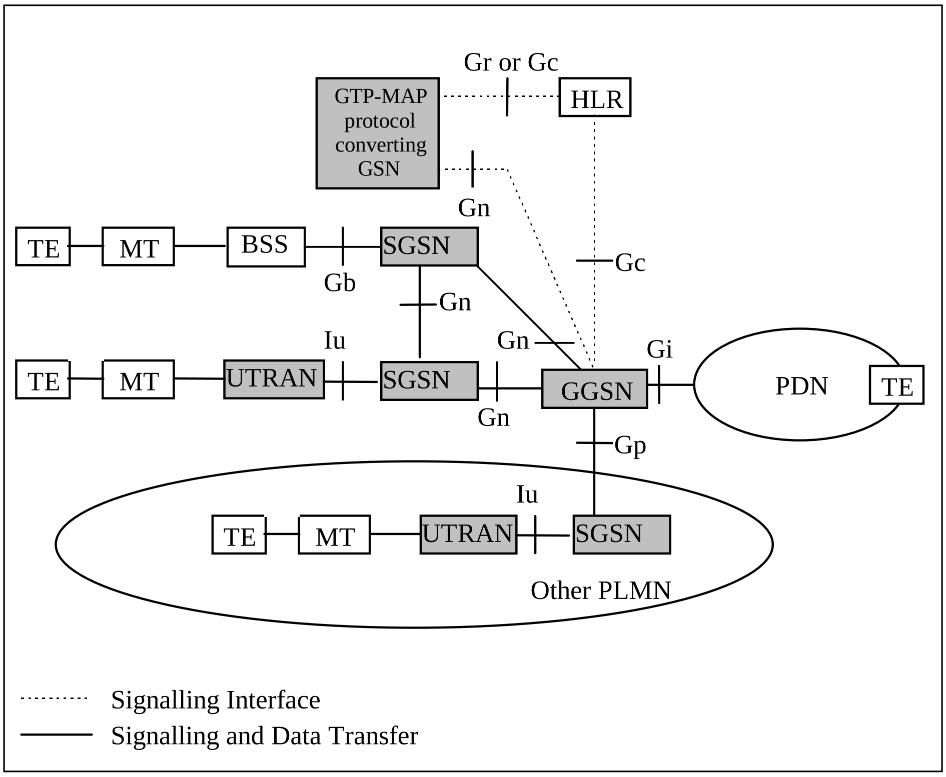

Figure 1: GPRS Logical Architecture with interface name denotations

GTP allows multi-protocol packets to be tunnelled through the UMTS/GPRS Backbone between GSNs and between SGSN and UTRAN.

In the control plane, GTP specifies a tunnel control and management protocol (GTP-C) which allows the SGSN to provide packet data network access for an MS. Control Plane signalling is used to create, modify and delete tunnels.

GTP-C includes sensitive messages. IPSec, defined by the IETF, are used to provide message confidentiality and protect message integrity.

In the user plane, GTP uses a tunnelling mechanism (GTP-U) to provide a service for carrying user data packets.

The GTP-U protocol is implemented by SGSNs and GGSNs in the UMTS/GPRS Backbone and by Radio Network Controllers (RNCs) in the UTRAN. SGSNs and GGSNs in the UMTS/GPRS Backbone implement the GTP-C protocol. No other systems need to be aware of GTP. UMTS/GPRS MSs are connected to an SGSN without being aware of GTP.

For GTP-U, security protection may be applied in the application layer. Otherwise, IPSec may be used to provide message confidentiality and ptotect message integrity.

It is assumed that there will be a many-to-many relationship between SGSNs and GGSNs. A SGSN may provide service to many GGSNs. A single GGSN may associate with many SGSNs to deliver traffic to a large number of geographically diverse mobile stations.

SGSN and GGSN implementing GTP protocol version 1 should be able to fallback to GTP protocol version 0. All GSNs should be able to support all earlier GTP versions.

10 Path Protocols

10.1 UDP/IP/IPSec

UDP/IP is the only path protocol defined to transfer GTP messages in the version 1 of GTP. A User Datagram Protocol (UDP) compliant with STD 0006 shall be used.

10.1.1 UDP Header

10.1.1.1 Request Messages

The UDP Destination Port number is 2123. It is the registered port number for GTP-C.

The UDP Source Port is a locally allocated port number at the sending GSN.

10.1.1.2 Response Messages

The UDP Destination Port value shall be the value of the UDP Source Port of the corresponding request message.

The UDP Source Port shall be the value from the UDP Destination Port of the corresponding request message.

10.1.1.3 Encapsulated T-PDUs

The UDP Destination Port number shall be 2152. It is the registered port number for GTP-U. The UDP Source Port is a locally allocated port number at the sending GSN.

10.1.2 IP Header

An Internet Protocol (IP) compliant with STD 0005 shall be used.

10.1.2.1 Request Messages and Encapsulated T-PDUs

The IP Source Address shall be an IP address of the source GSN from which the message is originating.

The IP Destination Address in a GTP request message shall be an IP address of the destination GSN. The IP Destination Address in an encapsulated T-PDU GTP shall be an IP address of the destination GSN/RNC.

10.1.2.2 Response Messages

The IP Source Address shall be copied from the IP Destination Address of the corresponding request message.

The IP Destination Address shall be copied from the IP Source Address of the GTP request message to which this GSN/RNC is replying.

10.1.3 IPSec Header

For GTP-C, the IP Encapsulating Security Payload (ESP) header (RFC 2406) is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality. ESP may be employed in either of two ways: transport mode or tunnel mode.

For GTP-U, if IPSec is applied, either the aforementioned ESP or the Authentication Header (AH) (RFC 2402) may be used. If necessary, the combination of ESP and AH may be used as defined in RFC2401.

10.1.3.1 ESP Header in Transport Mode

Transport mode is employed from one GSN to another GSN. In transport mode, the ESP header is inserted after the IP header and before the UDP header.

10.1.3.2 ESP Header in Tunnel Mode

If at least one of the source and destination addresses is a border gateway, then tunnel mode ESP is employed. In tunnel mode, the ESP header is located after the “outer” IP header and before the “inner” IP header.