3GPP TSG SA WG3 Security – S3 #14 **S3-000421**

Kjeller, Norway

August 1-4, 2000

Source: Motorola Inc.

Title: Protect GTP signalling messages by IPSec

Document for: Discussion

Agenda item: tbd

Abstract

This contribution suggests using IPSec security mechanism to protect GTP signalling messages. Some details regarding IPSec application in GTP scenario are discussed.

1. Introduction

GPRS Tunnelling Protocol (GTP) is defined in 3G TS 29.060 v3.5.0 (see [1]). It includes both the GTP signalling (GTP-C) and 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.

Some mobility management messages accommodated in GTP-C include sensitive information, for example, authentication vectors and MM context. Therefore, it is necessary to apply security protection to GTP signalling messages (GTP-C).

GTP uses UDP/IP path to transfer GTP signalling messages as well as to tunnel user data packets. IPSec is a set of protocols that integrate security into IP and provide data source authentication, data integrity, confidentiality, and protection against replay attacks. Therefore, IPSec is a natural candidate to provide protection for GTP messages.

2. Use of IPSec to protect GTP signalling messages

In this section, we discuss details of applying IPSec to protect GTP messages.

2.1 GTP-C vs. GTP-U

It is possible to protect both GTP signalling messages (GTP-C) and user data packets (GTP-U) by IPSec. However, in most of the applications, the user data may be protected by higher layer security mechanisms. It is not efficient or may not be necessary to apply double protection to user data. Therefore, in this contribution, we suggest that the protection provided by IPSec only apply to GTP signalling messages (GTP-C). We furthermore recommend that protection of GTP-U traffic by IPSec remains as an option for the network operators.

2.2 No changes in GTP messages

IPSec is independent of any higher layer protocols. Therefore, it does not require any changes in GTP messages. This differs from the approach taken by CN4 to add security to MAP messages (in TS 29.002), where the security functions were applied at the MAP layer.

2.3 Error and failure handling

In RFC 2521 (see [5]), a set of ICMP messages are defined to deal with the errors and failures in using AH and ESP. The new ICMP messages defined in [5] include “bad SPI”, “authentication failure”, “decompression failure”, “decryption failure”, “need authentication”, and “need authorization”.

IPSec error status may be conveyed to the sender by means of a local network management function. This function is beyond the scope of GTP standardization.

2.4 IPSec SPD and its implication to GTP message protection

In IPSec architecture, a look-up table, called Security Policy Database (SPD), is used to discriminate among traffic that is afforded IPSec protection and traffic that is allowed to bypass IPSec (see [4]). For any inbound or outbound datagram, three processing choices are possible: discard, bypass, or apply IPSec. We recommend that GTP-U packets simply “bypass” the IPSec process and that GTP-C packets be afforded protection by the IPSec.

SPD specifies what security services are to be applied to an IP datagram based on a set of selectors, among which the most important ones are source IP address, destination IP address, source UDP port, and destination UDP port. The SPD must be consulted during the processing of all traffic (inbound and outbound), including non-IPSec traffic.

By using SPD, different security mechanisms can be applied to GTP-C messages and GTP-U messages, since they use different UDP ports according to the latest version of 29.060 (see [1]). This will allow us, as we discussed in section 2.1, to apply IPSec mechanisms to only GTP-C messages.

It may be possible to further classify GTP-C messages so that they can be protected by different security mechanisms according to the discussion in [4]. But it is a local matter for the application layer to signal the IPSec processing for selection of security mechanisms on a message-by-message basis.

2.5 IPSec protocols and applications to GTP messages

IPSec mainly consists of IP Authentication Header (AH) (see [2]) and IP Encapsulating Security Payload (ESP) (see [3]). The Authentication Header (AH) provides data integrity, data origin authentication, and optional limited anti-replay services to IP. Encapsulating Security Payload (ESP) provides confidentiality, data origin authentication, anti-replay, data integrity, and limited traffic flow confidentiality.

The concept of Security Association (SA) is fundamental to IPSec. The SAs are unidirectional contracts between two communication entities. SAs determine the IPSec protocols used for securing the packets, the algorithms, the keys, and the duration for which the keys are valid. A “Security Association Database” (SADB) maintains the SAs.

Both AH and ESP make use of SAs. A key management protocol IKE is employed to establish and maintain SAs (see [6]). In this contribution, we assume that SAs are established by Key Administration Centers (KACs) defined in TS 33.102 (see [7]), so that both SADB and SPD are established for GTP use. The security services afforded in the SAs will be applied to GTP-C messages.

For GTP signalling messages, the provision of the following security services is suggested:

- data integrity;
- data origin authentication;
- confidentiality; and
- anti-replay.

We also suggest that the use of ESP, AH, as well as any possible combination of them, conforms to IPSec and is based on the protection requirement of GTP messages.

Two types of SAs are defined in IPSec: transport mode and tunnel mode. In transport mode, only the higher layer protocols (transport and above) are protected by IPSec, while tunnel mode is used to protect entire IP diagrams. According to RFC 2401 [4], “a host MUST support both transport and tunnel mode. A security gateway is required to support only tunnel mode. If it supports transport mode, that should be used only when the security gateway is acting as a host, e.g., for network management.”

For GTP messages, a host-to-host SA can be either transport mode or tunnel mode. However, whenever at least one end is a gateway, then it must be in tunnel mode. Furthermore, tunnel mode would provide source and destination address confidentiality. The GTP system architect may opt to afford (and implement) the security services to GTP packets at Border Gateways (BG). Therefore, in this case, it is mandatory to support tunnel mode.

References

[1] 3G TS 29.060 v3.5.0 “GPRS Tunnelling Protocol Across Gn and Gp interface”.

[2] S. Kent and R. Atkinson “IP Authentication Header” IETF RFC 2402, November 1998

[3] S. Kent and R. Atkinson, “IP Encapsulating Security Payload (ESP)” IETF RFC 2406, November 1998.

[4] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol”, IETF RFC 2401, November 1998.

[5] P. Karn and W. Simpson, “ICMP Security Failures Messages”, IETF RFC 2521, March 1999.

[6] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE)”, IETF RFC 2409, November 1998.

[7] 3G TS 33.102 v3.4.0 “Security Architecture”.