3GPP TSG SA WG3 Security – S3 #13 **S3-000329**

Yokohama, Japan

May 24-26, 2000

(Ad-hoc meeting on MAP Security, May 23, 2000)

Source: Motorola Inc.

Title: Use IPSec to secure GTP messages

Document for: Discussion

Agenda item: tbd

Abstract

We propose to use IPSec to secure selected GTP messages defined in 3G TS 29.060 v3.4.0. These messages include sensitive information, e.g. authentication vectors or MM Context. In order to incorporate the security mechanisms, we also propose to add some new cause values to 3G TS 29.060 v3.4.0.

1. Introduction

GPRS Tunnelling Protocol (GTP) is defined in 3G TS 29.060 v3.4.0 (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 include sensitive information. These messages should be protected by cryptographic mechanisms.

We propose to use security mechanisms defined in IPSec. In particular, we propose to use the Authentication Header (AH) defined in IETF RFC 2402 (see [2]) for message authentication, and Encapsulating Security Payload (ESP) defined in IETF RFC 2406 (see [3]) for message confidentiality. These mechanisms are mature for IP network security with plenty of options.

2. Proposal

We believe that the following messages in GTP need to be protected:

1. Identification Request and Identification Response - Section 7.5.1 and 7.5.2 of [1].
2. SGSN Context Request, SGSN Context Response and SGSN Context Acknowledge - Section 7.5.3, 7.5.4, and 7.5.5 of [1].
3. Forward Relocation Request and Forward Relocation Response- Section 7.5.6 and 7.5.7 of [1].

In order to support the security mechanisms defined in IPSec for the messages stated above, some new cause values are also needed. We propose the following changes in [1].

2.1 Additional Cause Values

In each of Section 7.5.2, Section 7.5.4, and Section 7.5.7 of [1], add the following cause values to

the “Possible Cause Values are:”

- ‘Session key agreed between the KACs has expired’
- ‘No session key is available for communication’
- ‘No agreement on key agreement’
- ‘No agreement on SA’
- ‘Message authentication failure’
- ‘Message integrity failure’
- ‘Message confidentiality failure’

2.2 Cause Description

In Section 7.7.1 of [1], we propose to add cause description as follows:

‘Session key agreed between the KACs has expired’ is returned when the session key agreed between the KACs has expired.

‘No session key is available for communication’ is returned when no session key is available.

‘No agreement on key agreement’ is returned when the key agreement process between KACs has failed and they do not agree on a key.

‘No agreement on SA’ is returned if no agreement is achieved for security association (SA).

‘Message authentication failure’ indicates that the recipient has failed to verify the message authentication.

‘Message integrity failure’ indicates that the recipient has failed to verify the message integrity.

‘Message confidentiality failure’ indicates that the recipient has failed to decrypt the encrypted messages.

2.3 Numerical Cause Value Assignment

For each new cause value proposed above, we need to assign a numerical value as for previous existing cause values in Section 7.7.1 of [1], Table 37. We suggest using the following values for response.

Cause	Value (Decimal)
Session key agreed between the KACs has expired	225
No session key is available for communication	226
No agreement on key agreement	227
No agreement on SA	228
Message authentication failure	229
Message integrity failure	230
Message confidentiality failure	231
Cause values reserved for security	231-240

For future use	219-224

References

[1] 3G TS 29.060 v3.4.0 “GPRS Tunnelling Protocol Across Gn and Gp interface”

[2] IETF RFC 2406, “IP Authentication Header”

[3] IETF RFC 2406, “IP Encapsulating Security Payload”