3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010097**

14 September, 2001

Sophia Antipolis, France

Source: **Siemens**

Title: **IPsec for Integrity protection between UE and P-CSCF**

Document for: **Discussion and Decision**

Agenda Item:

Abstract

Currently there are different alternatives under discussion for integrity protecting the IMS signalling between UE and P-CSCF. One possibility is to use an application layer mechanism which integrates into the SIP messages, like CMS. Another option is to protect SIP messages at the network layer, i.e., IPsec.

In [S3-010356] we discussed the applicability of either mechanism to provide integrity protection for IMS signalling. It showed that IPsec can eliminate the major disadvantages of CMS.

After further studying the restrictions and open issues given in [S3-010356], we do not regard any of these as being critical within the IMS context, so this contribution proposes to provide SIP integrity and optional encryption between the UE and the P-CSCF through IPsec ESP.

Introduction

Due to the fact that SIP as the IMS signalling protocol does not provide a sufficient mechanism for the integrity protection of SIP messages itself, there is an urgent need to find a solution for Rel5 3GPP specifications. Basically there are two alternatives to provide integrity protection for SIP signalling: application layer mechanisms that provide integrity within SIP messages, or IPsec that protects SIP messages through standard security mechanisms at the IP layer.

This contribution further elaborates on the open issues identified in the context of considering IPsec. It takes a further look on CMS providing SIP integrity protection at the application layer, and summarizes the discussion and IPsec advantages in the last paragraph.

Open issues affecting the applicability of IPsec

IPsec and compression:

SIP messages that are only integrity protected by IPsec between UE and P-CSCF do not conflict with any compression schemes which are operated between these entities or terminate at an intermediate hop. The only influence here is the integrity check value that cannot be compressed effectively, but this is not seen as a restriction worth to be considered.

Header compression and encryption: Although IPsec encryption conflicts with header compression schemes that are terminated at an intermediate hop between UA and P-CSCF (which are likely to be applied for UTRAN), the use of these compression schemes, as stated in [S3-010314], together with IPsec is still possible. However, their effectiveness will be reduced for IPsec protected packets, as

higher layer headers cannot be compressed, but as SIP signalling will only constitute a relatively small part of the compressed IP traffic, we do not consider this as being problematic.

Compression at SIP level: At the draft meeting in June 2001, SA2 agreed that "the appropriate place for compression/decompression within the architecture is between the UE and P-CSCF", see [N1-011009]. Therefore IPsec should not conflict with compression/decompression of SIP messages. This is seen only as a matter of local implementation in the UE and P-CSCF entities.

Intermediate hops between UE and P-CSCF:

ESP integrity protected IP packets cannot be modified between the IPsec endpoints, the UA and P-CSCF. In particular, it is not possible to have another SIP hop between the UA and the P-CSCF. We do not rate this as a restriction, since the P-CSCF is defined as the first IMS point of contact from the UA perspective (see [TS 23.228], chapter 4.6.1), and intermediate packet filters or firewalls that might be in place are still able to check the IP packet payload when encryption is not used.

Since NAT devices will cause problems with SIP in general, and SIP-aware NAT devices are unlikely for Rel5, these are not likely to be deployed for IMS systems. These certainly will break ESP integrity.

Although encryption is only optional for implementation, it could cause problems in the case that any middleware devices are active between the UA and the P-CSCF. This is considered as being unlikely. One configuration that could have a firewall operating between UA and P-CSCF is different operators running PS domain and IMS, respectively. In such a case, it is not possible for the firewall to read the IP payload, e.g. any transport headers, of the IP packets carrying SIP messages (only).

Anyway, for IPsec protected packets filtering based on the IP header is possible. For the given scenario, this seems to be sufficient. A firewall at the IMS border could be configured to allow IPsec packets to (and from) the P-CSCF without exposing the P-CSCF's security. All IPsec packets that cannot be verified by the P-CSCF at IPsec level, and therefore were not sent by a valid UE, will be dropped. All IPsec packets from (and to) the P-CSCF IP address could be allowed, accordingly, by a firewall at the PS domain border. In addition, the IP address range used for PDP contexts in the PS domain could be used for additional filtering rules.

SIP message transported in a single IP(sec) packet:

According to [TS 23.060], section 9.3, the maximum packet size supported between the mobile station and the GGSN without fragmentation shall be 1500 octets. The Gi interface between GGSN and P-CSCF is unlikely to support a smaller maximum packet size.

The upper boundary of 1500 octets should be sufficient for carrying most SIP messages within a single IP packet. It seems to be unlikely that several ESP headers are necessary for a single SIP message (which would increase the IPsec overhead).

Note in this context, that according to [23.228], section 5.4.5, the P-CSCF will remove the network generated contents of the Via and Record-Route headers of the SIP requests to be sent to the UE, to reduce the message size.

IP fragmentation should not increase the overhead here, since according to the IPsec specifications (RFC 2401, section B.2) IP fragmentation occurs after outbound IPsec processing, and fragment reassembly must occur befor IPsec inbound processing is applied.

Binding SAs to selectors:

It was already shown in [S3-010199] and in [S3-010356] that IPsec is feasible in principal for protecting SIP signalling between UE and P-CSCF, related to the binding of IPsec SAs to the ports and IP addresses used by the UA and the P-CSCF. See the related Siemens contribution "IPsec SA setup procedures between UE and P-CSCF".

Early start of integrity protection during security mode setup:

As identified in [S3-010356], by starting integrity protection between the UE and the P-CSCF already with the second REGISTER message sent by the UE, a problem arises during a failed run of UMTS AKA (e.g. synchronization failure).

Due to the failure, the common key IK is not in place, so the UA has to send this message without integrity protection. As the P-CSCF already expects ESP protected packets from the UE, a special treatment for such messages reporting failure is required.

This problem can be solved by the UA binding the ESP SA to a specific port and by using a different port for sending packets (SIP messages) reporting failure. In this case, the SIP application in the P-CSCF must only accept such messages reporting failure on this specific port. See the related Siemens contribution "IPsec SA setup procedures between UE and P-CSCF".

CMS for protecting IMS signalling between UE and P-CSCF

In [S3-010347], Ericsson showed in principal that the large overhead that would be created by CMS could be fairly reduced by appropriate compression schemes. SA3 decided at SA3#19 that the overhead is not a critical issue any more.

We still consider the effort required to specify the CMS solution for IMS signalling within 3GPP as being high. Interaction with other groups within 3GPP, e.g. SA2 will be required.

Furthermore, specifying any application layer mechanism for SIP should be aligned as far as possible with the process of the IETF SIP workgroup. At the last IETF-51 meeting in London the discussion at a SIP security subgroup meeting showed that even the progressed specification of EAP for providing SIP authentication, in addition to the current HTTP digest authentication mechanism is not likely to become part of the upcoming SIP specification [sipbis04].

Note, that the 3GPP presentations during the SIPPING WG session at IETF-51 were not well received and all mechanisms proprietary to 3GPP will increase the "gap" between 3GPP and IETF work.

To protect SIP messages in the IMS, CMS will have to be modified, e.g. some mandatory fields will have to be dropped to reduce the integrity overhead. In addition, a mechanism for replay protection needs to be added. As stated in [S3-010356], the possibilities to reuse this modified CMS version as sketched in [S3-010199] within the UE seem to be quite limited.

It should be kept in mind that the full specification of the CMS solution must happen within the given timeframe for Rel5, including the required interworking with other 3GPP groups, as well as the IETF.

Conclusion and proposals

We see the following major advantages of IPsec:

- Regarding the tight schedule for Rel5, IPsec offers the advantage of being a ready solution that does not require specification of new or modification of existing mechanisms, especially does IPsec not require any changes to SIP. ESP can be used according to the IETF RFCs.
- SA3 work will not require much interaction with other groups, e.g. for the specification of new SIP headers. Especially no interaction with the IETF will be required for Rel5.
- IPsec is already listed as one protection mechanism in the current SIP specification [sipbis04].Therefore SIP integrity provided by 3GPP will not conflict with any future SIP protection mechanism at the application layer.
- IPsec will be part of the P-CSCF for core network security anyway, and could prove useful in the UE as well. For instance, many remote access solutions rely on IPsec protection. Note, that ESP is mandatory for any fully compliant IPv6 implementation.
- ESP already offers a replay protection mechanism.

Taking into account the solutions that were proposed in SA3 for SIP integrity between UA and P-CSCF in SA3, and taking into account that it does not seem to be feasible to come up with any different

solution in time for Rel5, we therefore propose to use IPsec for providing integrity protection for IMS signalling between UE and P-CSCF.

We propose to use IPsec ESP in transport mode. ESP shall always be used with integrity protection and message origin authentication turned on. Encryption, according to the current SA3 working assumption, is optional for implementation, and could be additionally provided by ESP.

References:

[ESP] IP Encapsulating Security Payload (ESP), RFC 2406, IETF, November 1998.

[N1-011009] " LS on SIP Compression between UE and P-CSCF ", LS from TSG SA2 draft meeting 06/2001.

[S2-010314] " Response to LS (GAHW-010109, R3-010890 and S2-010383) on Optimised IP speech and header removal support in GERAN ", SA3#19, LS by TSG-RAN WG2

[S3-010199] " Integrity protection for SIP signalling", SA3#18 contribution, Ericsson

[S3-010347] "Integrity protection for SIP signalling", SA3#19 contribution, Ericsson

[S3-010356] "Integrity protection between UE and P-CSCF", SA3#19 contribution, Siemens

[sipbis04] IETF draft-ietf-sip-rfc2543bis-04.txt

[TS 23.060] 3GPP TSG SA, "General packet radio service (GPRS), Service description Stage 2 (Release 4)", version 4.1.0, 06/2001

[TS23.228] 3GPP TSG SA2, " IP Multimedia (IM) Subsystem - Stage 2 (Release 5)", version 5.1.0., 06/2001.