3GPP TSG SA WG3 Security — S3#19 **S3-010356**

4 - 6 July, 2001

London, UK

Source: **Siemens**

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

Document for: **Discussion**

Agenda Item: **7.3, IP multimedia subsystem security**

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 like CMS, another option is to use protection at the network layer, i.e., IPsec.

In this contribution we discuss the applicability of either mechanism to provide integrity protection for IMS signalling. It shows that IPsec can eliminate the major disadvantages of CMS, but introduces different issues that require further discussion, so the contribution proposes to further study both options for integrity protection before taking a decision on a working assumption.

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, or IPsec that protects the complete SIP messages at the IP layer.

This contribution has the goal to analyse both methods for providing integrity protection between the UE and the P-CSCF. As one result we will show the general applicability of IPsec and point out the advantages and disadvantages of such a solution.

CMS protecting IMS signalling between UE and P-CSCF

In S3-010199 (Ericsson), it is proposed to use CMS for integrity protecting SIP messages between UE and P-CSCF. Although we regard an application layer security solution as feasible in principle, there are three major issues with this proposal:

- the overhead introduced by CMS integrity protection
- the effort required for standardising the CMS solution for IMS signalling
- additional replay protection required

Integrity protection using CMS adds, according to S3-010199, approximately 120 bytes to each SIP message. Since this overhead has to be carried between UE and P-CSCF, it affects the air interface and therefore must be regarded as significant. Preceding a decision for this solution, a major effort would still be required to show how much this overhead can be reduced.

Protecting IMS signalling requires an integration of CMS authenticated-data content into SIP messages. A standardisation effort will be required here that affects 3GPP as well as IETF

specifications, e.g. the SIP specification itself. 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.

The possibilities for re-using CMS in other applications like e-mail mentioned in S3-010199, seem to be somewhat limited, as S-MIME does not make use of the HMAC-based authentication method, but requires digital signatures instead. Furthermore, modifications to CMS will be necessary , e.g. the removal of mandatory fields that have no use for IMS security but create additional overhead, such that fully compliant implementations are unlikely.

Note that with the adoption of CMS the requirement to define a replay protection mechanism arises as well.

IPsec protecting IMS signalling between UE and P-CSCF

IPsec as the other alternative for protecting IMS signalling between UE and P-CSCF has quite different characteristics that result in several advantages as well as disadvantages, compared to application layer protection mechanisms. This section is meant to give an overview of the specific benefits and problems.

Assumptions:

To study the application of IPsec, we assume the use of IPsec **ESP in transport mode** at this stage. ESP allows easier processing compared to IPsec AH, and the additional functionality of AH to protect parts of IP headers is not seen as a requirement.

Furthermore, it is assumed that ESP is always used with integrity protection and message origin authentication turned on. Encryption, according to the SA3 working assumption, is optional for implementation, but can be additionally provided by ESP.

We see the following major advantages of IPsec:

- Regarding the tight schedule for Rel5, IPsec offers the advantage of being a "fast" solution that does not require any standardisation of new mechanisms, especially no changes to SIP. ESP can be used without any changes and IPsec is already listed as a possible protection mechanism in the SIP specification. SA3 work will not cause major interference with other groups, e.g. for the specification of new SIP headers.
- ESP creates a significantly smaller overhead for integrity protection, compared to an application layer solution (approx. 24 bytes according to Ericsson S3-010199 - assuming that one SIP message is transported within a single IP packet).
- 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.

In addition to this, ESP already offers a replay protection mechanism.

Although the ESP solution seems to be feasible in principal and more efficient in terms of overhead and required standardisation effort, there are several aspects that have to be considered carefully.

But the fact that security will be provided at the IP layer underneath SIP creates a requirement for binding SIP signalling between a specific user and a P-CSCF to IP parameters like IP addresses and ports of those peers. Furthermore, a protection at the network layer will introduce several restrictions for any entity between P-CSCF and UE that operates at higher layers.

In general, with using ESP the following restrictions can be deduced:

1) IPsec and intermediate hops

The ESP protected IP packet payload carrying SIP messages 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.
If encryption is required as well (note that encryption is only optional for implementation) it is not possible to read the IP payload between UE and P-CSCF, e.g. transport headers.

Currently, this restriction is not seen as important for integrity protection, since the P-CSCF is defined as the first IMS SIP hop from the UA perspective (see TS 23.228, chapter 4.6.1), and packet filters or firewalls that might be in place are still able to check the IP packet payload.

The feasibility of encryption between UE and P-CSCF needs further study in general, and therefore is seen as a restriction that not only holds for IPsec. Anyway, it has to be mentioned that ESP encryption could cause problems with some header compression schemes.

2) Binding SAs to selectors

After establishing an ESP SA, the source/destination IP addresses and ports cannot be changed without establishing a new SA. Otherwise the existing SA would break.

IP addresses:

As long as the UA is registered with an S-CSCF, neither the UA nor the P-CSCF IP address will change without a new registration. During a new registration, it is possible to establish a new SA for the new IP addresses. Therefore, it is possible to bind ESP SAs to these IP addresses.

Ports:

On the one hand, to contact the P-CSCF a UA will receive the P-CSCF IP address according to TS 23.228, 5.1.1, and will probably use the well-known port 5060. It cannot be assumed that all P-CSCFs will use port 5060, so the P-CSCF port should not be assumed as fixed. Anyway, from the user perspective a P-CSCF will not change its port during the user's registration period. Therefore the ESP SA can be bound to the P-CSCF port and IP address.

On the other hand, the UA cannot be assumed to use a well-known SIP port but probably chooses any available port number before sending and receiving UDP packets.
If there is only a single IMS user allowed per terminal who registers with a specific P-CSCF, it will not be necessary to use a client port for the required SAs. These could have the following form (given as {src IP, dst IP, src port, dst port} and assuming the well-known server port):

```
SA1 (UE->P-CSCF): {IP(UE), IP(P-CSCF), ANY, 5060}
SA2 (P-CSCF->UE): {IP(P-CSCF), IP(UE), 5060, ANY}
```

Since the current 3GPP specifications do not exclude the presence of several IMS users at the same terminal in parallel, it could become necessary to use a specific client port, instead of "ANY". In this case, a UA would be required to use the same port for SIP signalling during a complete registration period.

Note, that on the UE the UAS and UAC, depending on the specific implementation, could run on different ports. In this case two IPsec SAs (pairs) would be required between the UE and the P-CSCF. It seems to be a useful restriction here to use the same port for incoming and outgoing SIP messages on the UE.

According to the SIP specifications the UA could use different ports for different SIP messages. This does not seem to be a useful or required behaviour. If the UA port is bound to an ESP SA, it is a requirement that the UA does not change this port during the lifetime of the corresponding SA.

3) Starting integrity protection early

At the 3GPP SA3 #18 meeting it has been proposed (S3-010220, Nokia) to already transmit IK and CK to the P-CSCF in the first response from the S-CSCF (messages 12, 13, see appendix A). This would allow to start integrity protection between the P-CSCF and the UE already from the first P-CSCF "401 Unauthorized" response, message 14.

Here, a general problem arises at the UE side: The SIP message has to be parsed first, before the integrity of the message can be verified, since the UE requires the parameter RAND carried in the message. This will create a special case independent of the layer where integrity protection is applied.

If integrity protection happens at the application layer, the usual processing will first check the integrity of the message and then process the message itself. So the first integrity protected message will require a different processing and therefore creates a special case.

In the case of ESP protection, processing the first message will be even more difficult, since first the UA has to extract RAND required for the calculation of IK, then an SA has to be put in place. Finally the integrity of the original IP packet has to be checked.

Therefore, the recommendation not to start ESP integrity protection with message 14 seems to be reasonable.

The second register sent by the UE, message 15, does not create a similar special case in general, since the security is in place before the message is sent. Anyway, a problem arises during a failed run of UMTS AKA.

We consider the case of network authentication or synchronisation failure. The UA receives message 14, notices a network authentication or synchronisation failure and sends message 15 back to the P-CSCF. Since, due to the failure, the common key IK is not in place at the UA, the UA has to send message 15 without integrity protection, or with a dummy MAC. As the P-CSCF expects the message to be integrity protected, a special treatment for such messages reporting failure is required.

With application layer integrity, the P-CSCF could check, after a failed integrity check, whether the message reports a failure, and, if yes, what type of failure.

With IPsec ESP in place, the P-CSCF ESP implementation is supposed to discard any IP packets that fail the integrity check, so these messages would never reach the SIP application.

A solution to this could be that the UA binds the ESP SA to a specific port and uses another port to send unprotected packets (SIP messages reporting failure).

Note that encryption is likely to render any solution to this more complicated.

4) Re-keying

Since an ESP SA has a certain lifetime, a mechanism will be required that puts a new SA in place before this lifetime is exceeded. Anyway, this is not regarded as an IPsec-specific issue, but has to be solved for other protection mechanisms as well, independent of the layer this mechanism is applied to.

Conclusion

Concluding the above discussion, we see the following main difficulties for the protection of IMS signalling between the UE and the P-CSCF by CMS, and any similar application layer solution:

- the overhead introduced by integrity protection
- the effort required for standardizing the solution for IMS signalling
- additional replay protection required

Protecting the IMS signalling between UE and P-CSCF with IPsec ESP is regarded as generally feasible and removes the major disadvantages of CMS. But there are other constraints and issues with the IPsec solution, described in the above discussion that still have to be considered carefully.

It is therefore proposed to pursue the study of both options before taking a decision on a working assumption.

Appendix A: General IMS authentication call flow

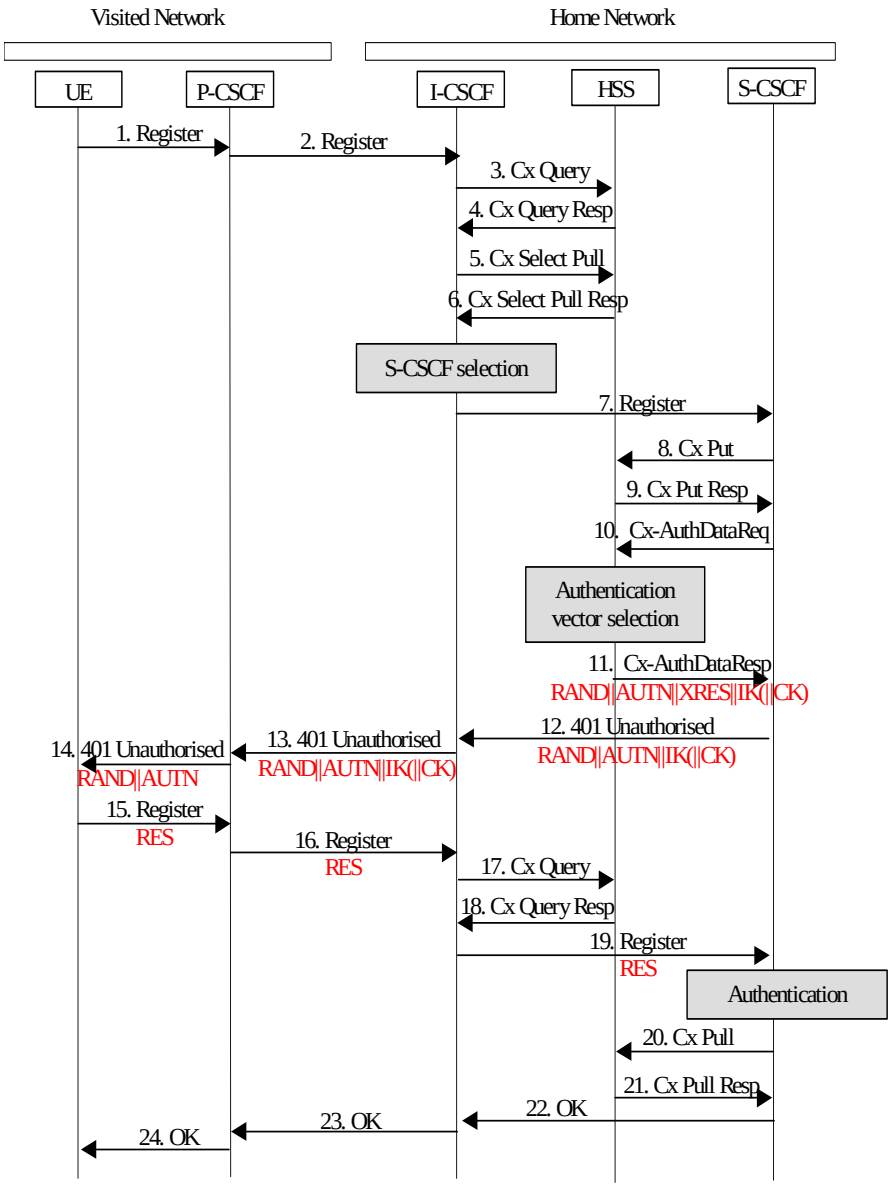

Figure 1: Authenticated registration, authentication successful