3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010102**

14 September, 2001

Sophia Antipolis, France

Agenda Item: 6.1

Source: Ericsson, Nokia and Nortel Networks

Title: On integrity protecting SIP-signalling in IMS

Document for: Discussion and decision

1. Scope and objectives

The scope for this document is to discuss and highlight some issues and concerns related to integrity protection of SIP signalling i.e. SIP-level and IPSec.

It is proposed that SA3 should adopt SIP-level protection as a working assumption. It is also recognised that there are some issues related to that and the risk that IETF will not deliver on time. However the contributors believe that if companies in 3GPP are active in IETF it is possible to get the wanted solutions in place and on time.

2 Background

3GPP SA3 has decided as a working assumption that security protection shall be provided in a hop-by-hop fashion. The first hop is the P-CSCF. However there has been no consensus on which layer to protect SIP-signalling.

In [S3-010347] Ericsson proposed that SIP-level protection should be used in combination with CMS. At the SA3#19 meeting in Newbury it was concluded that by using SIP-compression the headers will be reduced only to a couple of bytes and the size of the MAC introduces the main overhead. Following a similar concept Nokia has proposed in [S3-010357] to use a new SIP header for integrity and a generic scheme that could include Kasumi but possibly also other algorithms. Also SIP compression applies in this case. In [S3z01xxxx] Nortel has proposed to use an HTTP-digest based scheme by introducing a new header in SIP.

Siemens has in [S3-010356] made an analysis and identified some issues with a CMS based scheme at SIP-level and IPSec. The conclusion from this analysis is that further work is needed.

Currently there is no integrity protection defined for SIP, it shall request SIP IETF standardisation work no matter what mechanisms is to be defined.

In August an IETF meeting took place in London and the IETF chairmen identified that 3GPP does not follow the principles defined by IETF since 3GPP tries to define solutions exclusively within 3GPP. The right way following the comments by the IETF chairmen is to provide with requirement drafts and then the solutions shall be worked out in IETF. This is not only valid for the work taking place in SA3 but also for the work taking place e.g. in CN1.

The work with writing a requirement draft to IETF has already started in CN1 and this draft will be submitted to IETF very soon.

SA3 decided at the SA3#19 meeting on a scheme provided by Nortel, Nokia and Ericsson in [S3-010326] on the principles behind security mode setup. The working assumption is that it shall take place at SIP-level by e.g. introducing a new SIP-header and also by using EAP formats.

S1 has in [S1-010185] proposed the introduction of end to end encryption for voice calls supported by the IP Multimedia Subsystem. SA3 has currently moved the work for end-to-end protection for R6 since not enough support for the work item could be found for R5. It is envisioned in respect to the proposal from SA1 that future architecture i.e. beyond R5 will require that end-to-end solutions is provided as a service to the end users. Hence solutions that put restrictions to that vision should be avoided. It is apparent that end-to-end secure traffic will need end-to-end integrity protection as well in a way that works through proxies.

3 Requirements

In this section some requirements are captured that a solution for SIP-signalling protection shall comply with.

- For access to IMS at least the same level of protection shall be provided as for access to services provided in the CS- and PS-domains.
- The integrity protection shall be hop-by-hop.
- It shall be possible to enhance the integrity mechanism to be applied end-to-end in the future.
- The integrity mechanism shall provide with replay protection.
- The integrity protection mechanism shall support symmetric key based solutions.
- It shall be possible to combine the protection mechanism with compression needed for the wireless channel.
- The number of added roundtrips shall be minimised.
- The added headers at SIP-level shall not add substantial amount of contents in the SIP messages.
- The solution shall if possible be self-contained such that the number of maintained states at different levels is minimised.
- Security association generation is tied to IMS AKA

4 Possible solutions with pros and cons

4.1 SIP-level protection

The SIP-level protection mechanism could be used and as it seems fulfil all 3GPP requirements and it would not break the layering structure and the number of states that have to be kept at different layers is minimised. It also seems to be more future proof in the sense that it does not put any similar restrictions on future business models as IPSec does. The biggest issue that is recognised by SA3 is that no solution exists today in IETF that fulfils all 3GPP requirements.

So far different proposals have been presented to SA3 for SIP-level protection e.g. [S3-010347] and [S3-010357]. One conclusion from SA3#19 was that SIP-compression would minimise the problem with the extra overhead with SIP-level protection. It was shown in [S3-0100347] that the extra headers could be compressed efficiently to only a couple of bytes. Furthermore the proposals from Nokia, Nortel and Ericsson all need new SIP headers which can be efficiently compressed.

The outcome from the IETF meeting in London was that 3GPP has to define the requirements and not push directly solutions into IETF. IETF has defined the SIPPING group that will enable 3GPP and other groups to introduce requirements. The SIPPING group can then move the work that is needed into the SIP group. Hence solutions can not be defined in 3GPP, instead they have to be defined in IETF. SA3 is already aware of this and has the knowledge about this process but the IETF chairmen at the IETF London meeting highlighted this since they thought that 3GPP has not yet reached the cultural fluency that is needed to make progress in IETF.

The way forward is then to present to the SIPPING group a requirement draft that is agreed on in SA3. The work of actually specifying security at SIP level shall take place in IETF. This is also the process that e.g. CN1 has to follow so not only SA3 has to rely on that IETF deliver on time.

As already stated in Section 2 CN1 has started to work on a draft that will be sent to IETF very soon. It is proposed in this contribution that also SA3 now start up a similar process and co-ordinate this activity with CN1.

4.2 IPSec

IPSec fulfils most of the requirements stated in this document. It has already been identified in [S3-010356] that binding SIP-signalling with IP-parameters is needed. In [S3z010029] the problem with this violation is enhanced since

if there are several users using the same device it might raise some security concerns. For example a couple of SIP clients share the same IP address with individual IMS identities may not be distinguished successfully by the IMS core network.

The SIP standards allow the UA to have two different port numbers one for the UAS and one for the UAC. In relation to this the IPSec solution may mean that two SAs is needed in parallel in order to handle terminating and originating calls. This seems to add unnecessary complexity. In [S3-010356] it is said that this requirement does not seem to be useful or not even required. The solution to the problem with added complexity could be that SA3 requires that only one port number is used as proposed in [S3-010356]. This however is not a decision that can be taken by SA3. SA3 should ask for guidance from other groups e.g. CN1 and SA2 before actually requiring something that seems to violate or put restrictions to the SIP standards.

Furthermore it is also found that probably a special handling of error messages is needed. This scenario occurs since if the UE experiences an error the UA has no IK but the P-CSCF has. The P-CSCF (IPSec) then needs to discard all messages that are not integrity protected. Hence a failure message is discarded that should be sent back to the HN. This is not an allowed behaviour. A special handling of error messages is thus needed which could include the proposal in [S3-010356] to have two different port numbers; one for non-failure SIP-messages and one for failure SIP messages such that failure messages are not protected. This also put restrictions on SIP and new requirements that have to be co-ordinated with e.g. SA2 and CN1 before SA3 knows that this is allowed or not.

A couple of technical problems can be estimated on this proposal:

- Half of port numbers shall be reserved for failure report, which limits the capacity of P-CSCF.
- IPsec will not be able to check that the correct port was used for the right type of SIP message. The SIP layer must be involved to check the incoming packet's port numbers to verify that an error message was sent to the error port, and a normal message was sent to the normal port with protection. Otherwise, a masquerade attack could be launched that performed SIP actions through the use of the error port. This seems to require a non-trivial coupling between two layers which should work independently (at least according to IETF philosophy)
- Even with the additional port number checks, the SIP application will have to control the security policies at the IP layer at a very fine-grained level. For instance, policy entries will be needed to be created for newly registered clients for both normal and error cases (see further on about the need to have an API for this). Otherwise, it will not be possible to ensure that normal SIP messages really were protected.

The SIP security architecture SA3 has been working on involves a number of parts such as authentication (at SIP layer), security mode set-up (at SIP layer), and so on. We note that that if IPsec is used for integrity protection, the security solution will not be self contained and several layers co-operation is needed. In particular, the following is needed:

- Security association and policy state must be duplicated at both layers
- Software and hardware for implementing the facilities must be provided in two places, the IP and the SIP layers, as opposed to simply providing a SIP proxy application, for instance, that contains all security features and can run on top of any operating system.
- There must exist an API that allows dynamic modification of policy and security association databases from the application to the IP layer. No such standard API exists today, and it is not guaranteed that all products have such an API at all. Note that the API must be general enough to ensure, for instance, that traffic from an incorrect port enters the SIP proxy because the security policies couldn't be specified at fine enough detail.

One other drawback with IPSec identified in [S3-010356] is that it will provide with hop-by-hop protection. Hence it will (if only IPSec is used) exclude a business model where the VN provides with a service but does not necessarily need to know the content in the SIP-signalling i.e. VN could accept that parts of the SIP-signalling is encrypted. Do we want to exclude this scenario? IPSec only puts a restriction on which business models and services the operator can offer in the future. One solution could be that IPSec is the fast and simple solution today and then the solutions from the SIP community are adopted whenever they are ready. One issue with this way forward is backward compatibility and that the UE needs to have both security mechanisms implemented.

The SIP standard is not developed with that kind of architectural restrictions since e.g. in a wire line scenario hop-by-hop is difficult to have since in a general case the number of SIP proxies between the registrar and the UA is unknown.

In several contributions advantages with IPSec have been identified, cf. [S3-010356], [S3-0100199] and [S3z010029]. The advantages being e.g.

1. It is a fast solution. Only standardisation work is to define IPSec profiles done by SA3.
2. Minimised interaction with IETF and the SIP workgroup
3. IPSec is already implemented in IMS nodes
4. IPSec SAs can be derived from the AKA

However according to the discussions above bullet point 1 and 2 should be discussed. How fast solution is IPSec? And what is meant by minimised interaction? It has already been identified that e.g. some special handling on port numbers might be needed to make IPSec to fulfil 3GPP requirements on SIP. Then every modification, deviation or restriction to SIP has to be negotiated with other groups e.g. SA2 and CN1 and this should not be decided by SA3. This will introduce a delay in getting a solution in place. The companies supporting this paper believes that the best and fastest way, in general, is to use SIP as specified by IETF and that all possible modifications to SIP shall be a requirement that is put into the SIPPING group and handled in IETF. Any specialisation of SIP in 3GPP shall be avoided.

5 Time plan

In order to have a solution in place both for the SIP-level solution and the IPSec solution progress in IETF is needed.

In conjunction to that a rough time plan is presented:

Activities	IETF-decisions	Date
Start collecting 3GPP requirements towards IETF	-	September
Start development of solutions	-	Has already started
-	Preliminary agreement on the requirements on the mailing list	November
-	Final agreement on the requirements	December 2001 IETF meeting
Develop the solutions further and present them on the mailing list	-	Winter 2001
Put a stable solution to the working group for last call.	-	Beginning March 2002
-	Fine tune the solutions	March 2002 IETF meeting
Put solutions to IETF last call		April 2002

5 Conclusions

The companies supporting this contribution seek support from SA3 to have a SIP-level protection mechanism in place for IMS. It is recognised that there are concerns related to this and the possibility for IETF to actually deliver on time. However this is a concern not only valid for SA3 but also for CN1 as well. Furthermore the advantages with a SIP-level protection mechanism make the contributors believe that as a working assumption SIP-level protection shall be adopted by SA3.

The advantages with SIP-level protection are:

- Backward compatibility i.e. only one solution has to be built into the terminal for SIP-signalling protection
- It is inline with the general architecture e.g. wire line access does not assume a P-CSCF instead there will be an unknown number of SIP-proxies between the terminal and the registrar.
- The issue with having duplicated states and to enable dynamic modifications of polices etc are avoided
- No restrictions on port numbers
- Less restrictions on future business models

The only disadvantage is that SA3 has to rely on that IETF will deliver on time. The companies supporting this contribution recognises that this is an issue that needs to be taken into account. At the same time several solutions have been presented to SA3 and it is the goal for 3GPP overall and the contributors that agreed solutions can be delivered on time by IETF for R5. The only way that this can happen is that 3GPP contributes actively in IETF.

It is also proposed in this contribution that SA3 adopt the same process as CN1 already has started and write a requirement draft for IETF. Such a requirement draft is presented at this meeting.

References

[S1-010185] 3GPP TSG SA WG1 Services, *Requirement for End-to-End Encryption of IP Multimedia Subsystem Controlled Voice over IP Calls*, AT&T Wireless, February 2001, Capetown

[S3z010029] 3GPP TSG SA WG3 Security, *Open issues in IMS security*, Nokia, S3#17bis, May 2001, Madrid

[S3-010199] 3GPP TSG SA WG3 Security, *Integrity protection for SIP signaling*, Ericsson, S3#18, May 2001, Phoenix.

[S3-010326] 3GPP TSG SA WG3 Security, *Security mode setup for the IMS registration*, Ericsson, Nokia and Nortel, S3#19, July 2001, Newbury

[S3-010347] 3GPP TSG SA WG3 Security, *Integrity protection for SIP signaling*, Ericsson, S3#19, July 2001, Newbury

[S3-010356] 3GPP TSG SA WG3 Security, *Integrity protection between UE and P-CSCF*, Siemens, S3#19, July 2001, Newbury

[S3-010357] 3GPP TSG SA WG3 Security, *Integrity protection mechanism of SIP*, Nokia, S3#19, July 2001, Newbury

[S3z01xxxx] 3GPP TSG SA WG3 Security, *Digest-Based SIP Message Integrity Protection for IMS*, Nortel, S3#19bis, September 2001, Nice