3GPP TSG SA3 IMS ad hoc TDoc **S3z020010**
January 31st, 2002
Antwerp, Belgium

Source:	Nokia
Title:	Primary choice between IPsec and SIPsec
Document for:	Decision/Discussion
Agenda:	6, SIP signalling protection

Abstract

In current 33.203 the both IPsec and HTTP Digest first hop solutions co-exist for SIP signalling integrity protection between UE and P-CSCF. It turns out to be the critical time to take a decision on a working assumption.

The aim of this contribution is to discuss the current situation of the both solutions. It shows that both solutions are able to solve major disadvantages. From extensibility point of view HTTP Digest seems to be better choice. Therefore the contribution propose HTTP Digest as primary choice for security protection between the UE and the P-CSCF, and keep IPsec as backup plan.

Introduction

TS 33.203 has carried long time both IPsec and HTTP Digest first hop solutions for SIP signalling integrity protection between UE and P-CSCF. The version 1.0.0 was presented for information in SA #14 and got noted. It seemed like handling 2 solutions in parallel is a difficult task to S3 and also SA plenary. S3 has plan to get approval in next SA plenary meeting in March?. That means a choice is needed before that deadline. Discussion with CN1 also shows that validity of both solutions bring too much open possibilities that is blocking stage 3 progress. It turns out to be the critical time to take a decision on a working assumption.

The goal of this contribution is to investigate all previous arguments toward . A comparison work is done to aid decision making.

Discussion

So far, there are many contributions [S3z010102] [S3-010356], [S3z010029], [S3-0100199] and [S3-010347], comparing the SIPsec and IPsec solutions. After a collection work, **all diminished arguments** are listed here:

- S3-010356 points out the overhead introduced from CMS, is however not valid anymore in HTTP Digest. From terminal point of view, the HTTP Digest first hop may be a lightweight implementation regarding to IPsec specified in IETF. However when IPsec usage is restricted to only ESP transport mode, and relies on IMS AKA to generate symmetric keys, the weight is not a big problem.
- Partial protection is not valid in HTTP Digest first hop solution. Currently both protect complete SIP message.
- IPsec 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. This is true particularly when a group of equipments sharing the same address because they can not obtain IP address because of whatever reason. S3z010029 recorded this issue. During last week S2's meeting, however, a CR on IPv6 dynamic address allocation was approved. It guarantees every mobile can obtain IP address space as big as 2^{64}. In other words, it is clear that every equipment can be addressed with a unique IP address.
- S3z010102 points out that IPsec solution can not differentiate SA protected/unprotected SIP message. This is resolved by a fixed port number for unprotected messages.

Differences which are still valid:

From maturity of protocols, IPsec is in RFC since 1998, and has many implantations such as VPN. Regarding to replay protection, IPsec provides such protection by initiating two uni-direction SAs. HTTP Digest is to fixed this problem in next I-D version scheduled ?. According IETF work, HTTP Digest first hop work is going to be referred in SIP-bis6 as enhanced Digest draft in February or March 2002. The risk that IETF does not deliver on time is still open. But if it is finished before June 02, it still has a good chance to reach R5 timeframe in place and on time.

From interplay with other functions, namely SIP compression. There are essentially two places to implement SIP compression: inside SIP or under SIP. The latest I-D signalling compression is available at http://search.ietf.org/internet-drafts/draft-ietf-rohc-sigcomp-02.txt. In IPsec case, it does not matter the location of SIP compression. But in HTTP Digest case, the SIP compression must be done first for outbound signalling and vice versa. Comparatively, IPsec solution offers simpler interface to SIP and other text based protocols relying on the same compression scheme.

From confidentiality feature point of view, IPsec ESP offers the feature. However HTTP Digest does not cover it. On the other hand, the UDP/IP header compression in UTRAN shall conflict with IPsec ESP encryption. It implies that any implementation to confidentiality of SIP signalling must handled only in Transport layer or SIP layer.

Furthermore, consider we need to offer media confidentiality in R6, probably in end-to-end fashion, it seemed like IPsec can not be reused, since it will shelter requested routing QoS from intervening RANs observation.

From IMS architecture extensibility point of view, HTTP Digest can offer UA-to-further-proxy security that can be confidential from intervening Proxies. This requirements would be interesting to 3rd party vendors to offer new services for IMS; on the other hand, IPsec must play only in a hop-by-hop fashion. This may be a working load issue to P-CSCF.

Open questions

Here is a list of open questions to be discussed during this meeting. They are considered critical to make a decision as proposed in this contribution:

- An additional replay protection is required to HTTP Digest.
- The effort required for standardising is going on with effort from a SIP security team built in IETF.
- Confidentiality protection of SIP

Conclusion

It is seen that both solutions are approaching similar. From long term view, HTTP Digest maybe a better solution for interoperability since it can extend to IETF solution easily. If this is the case, we would like to propose HTTP Digest on a working assumption and prepare IPsec solution as backup plan.

Reference

[S3-010356] Siemens, Integrity protection between UE and P-CSCF.

S3z010102] Ericsson, Nokia and Nortel Networks, On integrity protecting SIP-signaling in IMS.

[S3-010347] Ericsson, Integrity protection for SIP signaling