3GPP TSG SA WG3 Security **S3-040990**

November 23 – 26, 2004

Shenzhen, P.R.China

Agenda Item: IMS

Source: Ericsson

Title: IMS security extensions

Document for: Discussion

1. Introduction

This discussion paper is related to a new WID, i.e. IMS security extensions, that Ericsson has submitted to SA3#36. The WID proposes that IMS security needs to be extended in Release 7 because there are new IMS use scenarios with new security requirements. The current signalling protection solution does not fulfil all these new requirements. For example, IMS access security does not work with networks with NA(P)T devices (e.g. in TISPAN NGN). Also, the use of IMS over the Internet (e.g. over third party provided access network), and over 3GPP/WLAN interworking scenario 2 or 3 should be further investigated. Furthermore, media protection solution should be developed because all of these new access networks can not be trusted.

This document further discusses the new requirements, and the solution space.

2. Requirements

This section lists some initial requirements for IMS security extensions. The presented list is not exhaustive, and further investigations are required. All existing IMS security requirements are assumed to apply.

1. IMS security extensions should provide signalling and media protection, and related key management solutions that are able to pass NA(P)T devices.
2. Interoperability between different SIP based networks (such as 3GPP IMS, TISPAN NGN and/or Internet) should be promoted.
3. IMS security extensions should not prevent Legal Interception.

3. Analysis of signalling protection solutions

There are three possible alternatives for providing signalling protection to access network. They are: TLS, IPsec with some key exchange protocol and a completely new security mechanism. Of course there are other security mechanisms, like HTTP Digest or SIP S/MIME, but they do not provide extensive security features needed in the access network. The development of a new security mechanism is quite expensive and it takes a long time. IPsec can be used with many key exchange protocols, but IKEv2 is the only fully standard one that supports NA(P)T traversal. In this contribution we further investigate two signalling protection solutions that we consider the most relevant ones, i.e. TLS and IPsec/IKEv2.

Ericsson has submitted a contribution [04BTD101] to TISPAN, where these two security mechanisms are compared with each other. This section is largely based on that contribution.

TLS does not really have major downsides, when compared to IPsec/IKEv2. One of the downsides of TLS is that is cannot be used with UDP. This, however, is not a significant flaw, because we believe that more and more data traffic is going to transfer on top of TCP. IETF also shares our view. The use of UDP in the future is going to introduce at least two problems; NA(P)T traversal problem and a problem with big datagrams. Dynamic UDP bindings in NA(P)Ts will timeout in one minute or so (no standard timeout). This means that the clients need to send a datagram typically every 30th – 40th second to refresh the NA(P)T binding, which of course increases the amount of traffic significantly. UDP cannot handle fragmentation, so it is unsuitable for big datagrams.

It can also be said that TLS cannot be used for securing data plane traffic. It is true, but our view is that IPsec is not a good alternative for doing that either. The biggest problem in IPsec, in the context of media protection, is that it requires a lot of resources from the end device, and end devices (e.g. mobile SIP phones) do not usually have a lot of resources to spare.

TLS, on the other hand, has many advantages. One of them is that TLS is very mature, a lot implemented protocol. For example, 3GPP Release 6 UE already has TLS for Presence/HTTPS access. On the contrary, IKEv2 is a young, immature protocol. NA(P)T traversal is inherently supported by TLS. The ability to traverse NA(P)Ts is quite essential in wireline side, but it is also necessary in some wireless environments (e.g. in WLAN). Another advantage that TLS provides is that it can easily be supplemented with end-to-end authentication mechanism, such as HTTP Digest or HTTP Digest AKA, without serious binding problems between lower and upper layer identities. TLS can also be deployed in access networks without great costs, because of the fact that it is already implemented in most SIP-devices.

We summarize our analysis by presenting tables that list the main characteristics from both examined access security solutions. The tables below show that TLS would in fact be a good alternative for providing access security besides IPsec. Our analysis also shows, that there are several reasons why TLS could even be favoured over IPsec/IKEv2.

Table 1: Characteristics of TLS

Benefits	Disadvantages
Works through NA(P)T (TLS does not add protocol specific problems to NA(P)T traversal).	Only possible for SIP/TCP not SIP/UDP, although this is not a big disadvantage.
Provides privacy even for the first REGISTER (private user identity).	
Availability of client implementation (part of IETF SIP standard). This makes the deployment of TLS cheap and quick. Furthermore, 3GPP Release 6 UE already supports TLS.	

Table 2: Characteristics of IPsec/IKEv2

Benefits	Disadvantages
Possible for both SIP/UDP and SIP/TCP, although this is not a big advantage.	NA(P)T issues in particular in combination with ALG.
	Has to be used with IKEv2 or some other new key exchange protocol. These solutions are immature and not widely available.
	Binding the IPsec layer identity with the SIP layer identity is very difficult.

4. Analysis of media protection solutions

Current IMS specifications assume that media is not separately protected. Instead, the security architecture relies on security provided by lower protocol layers. Media protection solutions should be considered for cases when the access network, and/or intermediate networks cannot be trusted.

Assuming that the media to be protected would be RTP over UDP, the protocol to be evaluated could be e.g. IPsec/IKE, and SRTP/MIKEY [SRTP, MIKEY]. In the following, we take a closer look at these two alternatives:

Re-use of existing protocols

- IPsec/IKE; IMS access security is currently based on IPsec. Re-use of the same protocol for other purposes is appealing especially from UE point of view. However, IMS key management solution () cannot be directly re-used.

- SRTP/MIKEY; UEs must implement SRTP and MIKEY for [MBMS]. Re-use of the same protocols for IMS is appealing.

NA(P)T traversal

- IPsec/IKE; Generally speaking, IPsec has NA(P)T traversal problems unless IKE is used.
- SRTP/MIKEY; SRTP and MIKEY does not add any specific NA(P)T problems.

Coverage of protection

- IPsec/IKE; All headers on top of IP can be integrity protected, and encrypted.
- SRTP/MIKEY; No headers are confidentiality protected. Headers above transport layer (e.g. RTP) may be integrity protected.

Key management and session setup

- IPsec/IKE; IKE needs separate messages (and more round trips) for setting up the security association for the media stream.
- SRTP/MIKEY; Key management can be piggybacked in SIP/SDP (either in form of a MIKEY run, or as sending the parameters and keys in raw, if SIP/SDP is already secured). Hence, no extra round-trips are introduced.

Use with SIP

- IPsec/IKE; There is no standard means of signalling the use of IPsec in SIP/SDP.
- SRTP/MIKEY; Extension to SIP/SDP to signal SRTP usage and carry MIKEY messages exists [SDP-KEY, MIKEY].

Interworking with SIP

- IPsec/IKE; Requires specific APIs for SIP application to modify IPsec security policies.
- SRTP/MIKEY; Security solution is more easily integrated to SIP [SDP-SEC].

As an initial conclusion, it can be stated that IPsec is not very promising solution for media protection. Other solutions, such as SRTP/MIKEY should be further studied.

5. Conclusions

It is suggested that SA3 further studies the new requirements and solutions related to signalling and media protection.

6. References

[04BTD101] 04bTD101, “Access Security of NGN: Proposal for Security Protocol”, contribution to TISPAN, Ericsson.

[SRTP] RFC 3711, The Secure Real-time Transport Protocol, IETF, RFC 3711.

[MIKEY] RFC 3830, MIKEY: Multimedia Internet KEYing, IETF, RFC 3830.

[SDP-KEY] “Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)”, IETF, work in progress.

[SDP-SEC] “Session Description Protocol Security Descriptions for Media Streams”, IETF, work in progress.

[MBMS] 3GPP, TS 33.246, Security of Multimedia Broadcast/Multicast Service