3GPP TSG-SA WG3-LI Meeting #35 **SA3LI09_112**
Scottsdale, AZ,USA 03-05 Nov.， 2009

Title: **LI analysis of KMS-based solution on IMS media security**

Document for: **Discussion**

Date: **3 November 2009**

Source: **ZTE Corporation**

Abstract:

*This paper is about discussing some security issue, particularly LI issue, in current KMS-based solution. *

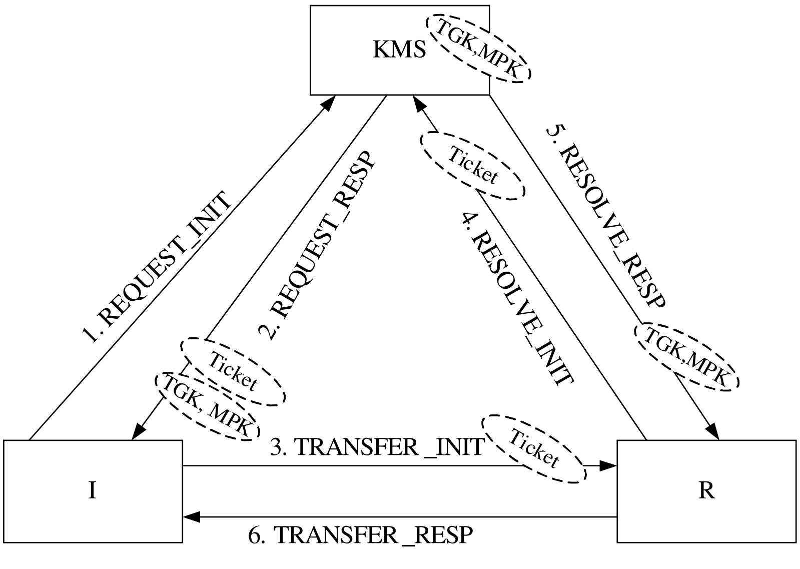
a) Introduction

KMS-based solution is based on the assumption that the signaling security is not reliable. From TS33.328, sec 4.1.1:

> “IMS media plane security is composed of two more or less independent key management solutions. The first solution, SDES, is for end-to-access edge and for end-to-end media protection. The solution relies on the security of the SIP infrastructure and in particular on SIP signalling security.
>
> The second solution is for e2e protection and aims for high security, independent of the signalling and transport network. It is based on use of a Key Management Service (KMS) and a "ticket" concept. The security offered is anchored in the KMS including the functionality used for user authentication and key generation towards the KMS. ”

Current LI solution is that the LI access point, normally CSCF, grabs the ticket and other signalling data from signalling plane. Then LI access point submits the ticket to appropriate KMS for resolving. Then LI access point can deduce the master media key.

The below figure demonstrate the basic concept of KMS-based solution. Session setup includes up to six message interchange. After the session setup, the initiator and responder get the shared key MPK, TGK, etc.



The TGK is the key which is used to derive the key used for encrypt the actual media information.

The MPK is the key which is used to do integration check of message 3(TRANSFER_INIT) and message 6(TRANSFER_RESP).

Later in this discussion paper, some threats are identified in case that some signalling middle boxes are compromised or there is no signal security infrastructure out there.

2. Discussion

2.1 MitM attack to bypass the LI

MIKEY-TICKET provides the MIKEY Protect Key (MPK) to prevent MitM attack when MIKEY-TICKET messages are exchanged between initiator and responder. But MPK only ensures the end-to-end integrity, while LI access point should reside in the middle of signaling path thus it can intercept the passing signaling messages. Therefore MPK itself cannot guarantee that the LI access point in signaling path can get the correct MIKEY-TICKET message. Given the situation that there are two man-in-the-middle, one modifies the MIKEY-TICKET message before the LI access point, while another one changes the modified message back to the original message after the LI access point, the message either on the terminal side or the KMS side can still pass the end-to-end integration check, while in the mean time, LI access point, however, gets the modified MIKEY message which cannot be used to deduce the master media key.

2.2 Reusable ticket trick

The main purpose of reusable ticket is to reduce the signalling traffic, off-load KMS from generating and resolving ticket, thus to avoid single point of failure.

But reusable ticket rules out the involvement of KMS either on the originating side or the terminating side, which makes it possible for some malicious users to take advantage of it to use corrupted ticket for their own purposes, e.g. DoS attack, bypassing the LI, etc.

Given that reusable ticket is acquired by the legal way (i.e. from KMS) and attacker has no capability to forge and amend the ticket, the validness of ticket is verified by checking whether the current time insides of the range from “valid from time” to “valid to time” defined in the ticket. Since the verification of reusable tickets is only excuted by terminals, the originator and responder can modify the time inside the valid period to make use of the reusable ticket which is already expired. Since KMS may not recognize the expired reusable ticket, the LI system cannot deduce the master media key being used. This threat can, to some extent, offset by deploying Network Time Protocol (NTP). But it needs to be verified whether it is worth, in terms of cost and performance, to deploy the NTP across all kinds of access technology supported by IMS just for media security. Besides, NTP itself also needs security consideration.

2.3 DoS/DDoS attack

If malicious originator forges the MIKEY-TICKET message or one man-in-middle changes the original message, the corrupted MIKEY-TICKET message can only be detected after several message exchanges, i.e. the ticket is transferred all the way from originator to responder then sent from responder to KMS B and finally from KMS B to KMS A, this method, however, consumes the network bandwidth, moreover makes the KMS vulnerable to DoS and DDoS attack.

3.1 Solutions

Considering the R9 will freeze soon, we suggest three solutions to handle the above-mentioned issues.

3.2Solution 1

In this solution the hop-by-hop signalling protection should be employed to prevent problems identified in section 2.1 and 2.3. Thus signalling security infrastructure should be imposed to KMS-based solution, i.e. the KMS-based solution should rely on the signalling security infrastructure, rather than independent of it. Signalling security infrastructure should at least provide the integration protection of the signalling message and confidentiality protection can be optional.

This solution provides least protection to KMS-based solution. It still cannot handle the situation when some signalling middle boxes are compromised.

But if the KMS-based solution also relies on the signalling security just like SDES, the biggest advantage of KMS-based solution that this solution is independent of underlying signalling security cannot be justified. Nevertheless the signalling protection anyway is needed because signalling security is a very important requirement for operators and users. It still can be used as a simplest solution.

3.2 Solution 2

The MitM attack makes it dangerous for LI to pick up key material from signaling path because the end-to-end integrity protection provided by MIKEY-TICKET cannot guarantee that LI get the correct key material for the reason presented in section 2.1. But end-to-end integrity protection, however, can guarantee that the user terminal gets the correct key material. So the solution is let the end-user terminal submit all key material, not only the ticket itself, but also all random numbers generated by the originator and the responder, to KMS and LI get all necessary key material from KMS instead of signalling, then the threat of bypassing LI from the MitM attack will go away.

In this solution, reusable ticket still can be used, and partially showing its advantage in signaling overhead in the sense that the originator needs not apply a ticket from KMS in every session setup, while the responder, on the other side, needs to anyway communicate with KMS for the purpose of key material transmission and ticket verification regardless whether the responder has already known the secret inside the ticket or not.

3.3 Solution 3

The lawful interaction access point located in signaling path should authenticate the MIKEY-TICKET message and check the time validness of the ticket inside the message, in this way the MIKEY-TICKET message protection key (MPK) should be deducible in LI access point. By this method, the current LI solution remains the same in the sense that the LI access point, normally CSCF, grabs the ticket and other signaling information, such as random number, ticket from signaling without worrying those information is corrupted.

Notes: The compromise of the signaling should not lead to the compromise of authentication function in LI access point.

For the problem identified in section 2.1, with the signaling middle boxes authenticating MIKEY-TICKET message, the threat of MitM attack could be ruled out.

The problem introduced by the reusable ticket also can be easily addressed. Unlike solution 2, the terminating terminal needs not submit the reusable ticket to KMS for verification in the sense that the ticket is already verified in the lawful access point. Thus the advantage of reusable ticket can be fully exploited. And most of all, the chance for terminal directly communicating with KMS will be minimized; the workload of KMS and chance of DoS and DDoS will also be minimized.

In terms of the problems in section 2.3 that user can forge/amend the message to flood attack the responder or KMS, the chance is quite distant from today's perspective. But in the predictable future, with terminal getting smarter and smarter, this kind of attack is not far-fetched any more. This solution can early detect this kind of intention before it moves further into the network.

This solution should be considered if current LI solution wouldn't like to be changed, i.e. LI grabs the key material from signaling. But because of its big impact on the current core network and approaching the freeze of R9, it is suggested to consider this in R10.