3GPP TSG SA WG3 Security — S3#20 **S3-010544**

16 - 19 October, 2001

Sydney, Australia

Source: **Siemens**

Title: **Security Association Management in the IMS**

Document for: **Discussion and Decision**

Agenda Item: **7.3**

Abstract

This contribution discusses problems of managing IMS security associations(SAs) between P-CSCF and UE when there are several registrations of a user associated with different public user IDs ongoing at the same time. The contribution concludes that, for complexity reasons, all the registrations of one user should be handled by the same S-CSCF at a given time. It is further suggested to propose to SA2 to take this account in the IMS architecture.

1. Introduction

We assume that there are several registrations of a user associated with different public user IDs ongoing at the same time. There are two cases to be considered:

Case 1)

There are several SAs between UE and P-CSCF for one user at a given time.

This is undesirable for the complexity and performance reasons stated in TDs S3-010495 (Ericsson) and S3-010502 (Siemens). They are not repeated in this contribution.

Case 2)

There is only one SA between UE and P-CSCF for one user at a given time.

This contribution deals only with case 2). It aims at showing that, in case 2), the management of SAs becomes very complex unless it is assumed all the public IDs of one user are registered with the same S-CSCF at a given time.

In addition, case 2) seems to be only possible when network-initiated authentication is possible. Note, however, that the flexibility in authentication policies introduced by the possibility of network-initiated authentication is considered desirable also for other reasons which were stated in an earlier LS from S3 to N1 (TD-S3z010130)

2. Discussion

In this section, the problems associated with managing IMS security associations between the UE and the P-CSCF are discussed using a typical example scenario. It is assumed for this scenario that registrations for different public user IDs (IMPUs) are handled at different S-CSCFs.

Scenario:

Step 1: in registration1, IMPU1 is registered with S-CSCF1, authentication is performed and SA1 is established

Step 2: in registration2, IMPU2 is registered with S-CSCF2, the registration messages are

protected with SA1, authentication is not performed and no new SA is established according to the home operator's policy to minimize the number of authentications.
For this it is required that the P-CSCF informs S-CSCF2 that registration messages were actually protected by setting a "was protected" flag.

Step 3: in registration3, IMPU2 is registered with S-CSCF3, the registration messages are protected with SA1, authentication is not performed and no new SA is established according to the home operator's policy to minimize the number of authentications.
For this it is required that the P-CSCF informs S-CSCF3 that registration messages were actually protected by setting a "was protected" flag.

Step 4: now registration1 expires, and S-CSCF1 deletes the user records, but registration2 and registration3 live on.

What next and who decides what to do?

1) SA1 may live on until the maximum lifetime set for SAs expires (it need not be the same as that for registrations) or
2) a re-authentication is initiated to establish a new SA.

S-CSCF1 cannot decide what to do as it knows nothing about the existence of the other registrations, on the other hand, S-CSCF2 and S-CSCF3 know nothing about the lifetimes of registration1 or of SA1 so they cannot decide either.
But even if S-CSCF2 and S-CSCF3 could obtain this information (how?) there would still be the problem of how they could coordinate who of the two should initiate a re-authentication (certainly not both at the same time).

From the above it seems to follow that, in such a scenario, re-authentication cannot be controlled by the S-CSCF. This is in conflict with SA3's working assumption that authentication is controlled by the S-CSCF.

There are two ways forward now: stick to the working assumption and do not allow this scenario to happen, i.e. do not allow the assignment of different S-CSCFs to one user at a given time. Or else, allow exceptions from the working assumption for such scenarios. The consequences of making such exceptions are discussed in the following:

Which other entity could take the decision whether and when to re-authenticate?

- P-CSCF
- HSS

The following has to be taken into account in this context:

The deciding entity has to

1) implement operator policies on authentication which may
   - change dynamically
   - depend on user type
2) maintain timers per registration and / or per SA
3) receive a "was protected" flag from the P-CSCF

The list is not necessarily exhaustive.

It is very undesirable to take the decision in the HSS:

1) and 2) introduce considerable complexity in the HSS. The HSS is not meant to handle timers or execute dynamically changing policies.

3) would necessitate another change to the Cx-interface

It is undesirable to take the decision in the P-CSCF:

There is a preference to control authentication in the home network. There would be a need for the P-CSCF to be informed of the home operator's authentication policy and the latter would have to trust the P-CSCF to correctly execute it.

But there is a pro: the need for the "was protected" flag would go away.

3. Conclusion

The problem discussed above goes away when all the public IDs of one user are registered with the same S-CSCF at a given time. (Note that this S-CSCF may be different from one time to another: when a user has no ongoing registrations then no information about a S-CSCF associated with the user is stored, so the next time a user registers any suitable S-CSCF may be assigned.)

Therefore it should be proposed to S2 to, at least for Rel 5, reconsider their approach to allow different S-CSCFs to be assigned for registrations with different public IDs of one user at a time. This proposal is in line with the general tendency in 3GPP to reduce the complexity to the required minimum for Rel'5. This does not preclude to introduce the more general scenario later.