3GPP TSG SA WG3 #22 **Tdoc S3-020161**

Bristol, UK
25th February – 28th February 2002

Source: **TSG SA WG3**

To: **TSG CN WG1**

Title: **Issues with SA handling at P-CSCF**

Contact: **Adrian Escott**
Email: adrian.escott@hutchison3g.com

1 Introduction

For Release 5, it was decided that the IMPUs relating to a particular IMPI should be registered at the same S-CSCF. During normal operation, this allows a UE to only maintain one security association (SA) for each direction to protect traffic between the UE and P-CSCF. Every successful (re-) registration that includes a user authentication generates a new SA for each direction. These new SAs should then replace the previous SAs. In order to allow a smooth transition between SAs, the P-CSCF needs to keep the old SAs until it has received a message protected with the new SA. SA3 hoped that it would be enough to store at most two SAs for each direction at the UE and P-CSCF.

A recent analysis of the SA handling error cases has produced a case (see section 2), where it is not enough to store only two SAs for each direction at the P-CSCF. It could be also necessary to store more than two SAs for each direction in the case of multiple simultaneous registrations. SA3 realise that these cases introduce additional complexity at the P-CSCF and seek CN1's advice on potential solutions to these issues.

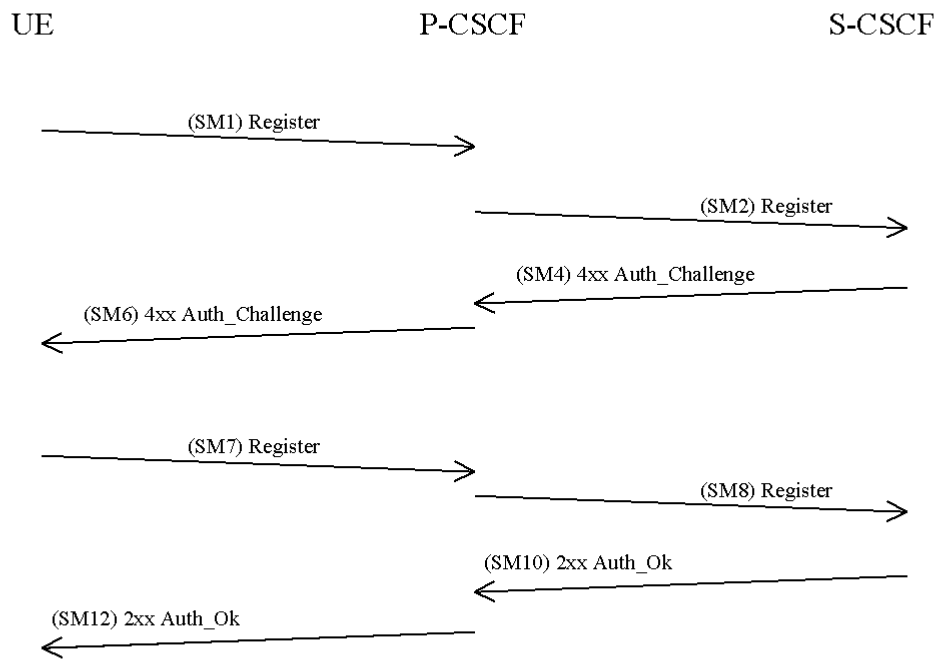
2 SA handling problems

This section describes the SA handling problem that SA3 have identified. The current SA handling procedures are described in the sections 7.3.3.1 and 7.3.3.2 of the TS 33.203v2.0.0. The below diagram gives the message flows for a successful set-up of SAs (note: for clarity, the I-CSCF is not represented in the flows).

After a successful registration with user authentication, the P-CSCF has two security associations, SA1_in and SA1_out that are used to protect inbound and outbound traffic respectively. A further successful registration with user authentication produces a second set of SAs, SA2_in and SA2_out, at the P-CSCF (note: the P-CSCF considers a registration to be successful when it receives the SM10 Auth_Ok message).

At this point the P-CSCF can not discard SA1_in and SA1_out without causing the following problems. Firstly, the UE will use SA1_in to protect non-registration (e.g. a response to an invite) traffic it sends to the P-CSCF until it receives the SM12 message in the registration procedure. The P-CSCF will not be able to check the integrity protection applied to this traffic and hence discard it. Secondly if the UE does not receive the SM12 message in a registration procedure, it throws away SA2_in and SA2_out, as the registration that created them was not successful. This would mean the UE and P-CSCF no longer share common SAs. Under the current SA handling procedures, the P-CSCF keeps SA1_in and SA1_out until it receives a message protected with SA2_in outside the registration procedure that created SA2_in.

The P-CSCF may now have two sets of SAs, SA1_in and SA1_out, and SA2_in and SA2_out. At this point, the network receives an unprotected REGISTER request for the UE. The unprotected REGISTER request could have been sent by the UE that had lost its SAs for some reason (e.g. power loss) or an attacker. The network must respond to this REGISTER with a challenge or it is potentially denying a genuine user access. Once the P-CSCF receives the message carrying the challenge, i.e. SM4 message, it can create a new pair of SAs, SA3_in and SA3_out.



At this point the P-CSCF has three pairs of SAs. If it deletes SA1_in and SA1_out, there could be the problems discussed above. If it deletes SA2_in and SA2_out and the unprotected REGISTER was sent by an attacker, the P-CSCF is deleting exactly the SAs that a UE will use to protect further traffic (if there were no problems with the second registration). Clearly the P-CSCF must keep SA3_in and SA3_out.

The above problem of SA handling becomes a lot more complicated if there are multiple simultaneous registration attempts that involve user authentications. The network chooses whether a user authentication is required for a particular registration or not, hence SA3 believe that the UE should not be allowed to initiate more than one simultaneous registration to avoid making the SA handling procedures more complex than necessary.

Of course, this does not stop an attacker flooding the network with a series of unprotected REGISTER requests. In order not to deny a valid user access to the network, the network should respond to all of these requests. This would mean the S-CSCF sending out lots of authentication vectors and the P-CSCF creating lots of SAs. Currently SA3 have not proscribed any behaviour of the P-CSCF and S-CSCF to deal with this situation.

3 Open Issues

SA3 would like CN1's advice on the following issues

- Do CN1 see anyway of ensuring the P-CSCF knows that the UE successfully received the last message in a registration procedure?
- Do CN1 see any reason why a UE should be allowed to initiate multiple simultaneous registrations for a particular IMPI?
- Can CN1 prescribe any behaviour for the P-CSCF and S-CSCF to deal with an attacker flooding the network with multiple simultaneous registrations for the same IMPI?
- Do CN1 see the need to limit the compulsory number of SAs stored at the P-CSCF to two?

4 Actions

To CN1:

- SA3 would like CN1's opinion on the above issues in order to settle on appropriate SA handling procedures.

5 Date of Next SA3 Meetings

CN1/SA3 joint meeting	9th April 2002	Fort Lauderdale, USA
SA3_23	14th – 17th May 2002	Victoria, Canada