3GPP TSG SA WG3 Security — S3#25 **S3-020457**
8 - 11 October 2002
Munich, Germany

3GPP TSG-CN1 Meeting #25 ***Tdoc N1-021848***
Helsinki, Finland, 29 July – 2 August

Title: Secure registration of IP addresses
Response to: N1-021544 (S3-020316)
Release: REL-5
Work Item: IMS-CCR
Source: CN1
To: SA3
Cc:

Contact Person:
Name: Gábor Bajkó
Tel. Number: tel:+36 20 9849259
E-mail Address: gabor.bajko@nokia.com

Attachments: None

1. Overall Description:

CN1 thanks SA3 for the liaison statement regarding the secure registration of IP addresses.

CN1 had difficulties understanding the problems which SA3 wants to solve. Once the first REGISTER request is sent unprotected, it is always exposed for DoS attacks. An intruder may modify the source IP address of the packet, but it may also modify other parts, even the payload of it. The result of these attacks will never be a successful registration of the intruder to the network.

CN1 can acknowledge that the IP addresses in the Via and Contact header (for Rel5) of the REGISTER request contain the identifier of the subscriber (IP address or domain name). In an integrity protected REGISTER request this information is reliable and can be used for whatever verification SA3 would like to make. CN1 would like to draw SA3 attention to two aspects:

- If the not-integrity protected REGISTER is modified by an intruder and the P-CSCF sets up an SA with wrong selectors, the protected REGISTER will be dropped by the IPSec layer in the P-CSCF. The P-CSCF will not have the opportunity to verify anything.
- For Rel5 the identifiers in the Via and in the Contact header must point to the same IP address. However, it is expected that in further releases the Contact header may contain an address which is different from the address the UE sent the REGISTER request from, and as a consequence more SAs will need to be established.

CN1 would like to advise SA3 that when setting up the SA in the P-CSCF, the P-CSCF will read the address from the Via header of the REGISTER request instead of the source IP address of the packet carrying the REGISTER request. This may solve the problem when the intruder only modifies the source IP address of the packet, but leaves the payload intact.

The problem described in the SA3 LS could only be eliminated if prior to any communication with the P-CSCF the UE would be able to set up a secure tunnel towards the P-CSCF and use the tunnel when sending the REGISTER requests. Such a mechanism is not part of Rel5, and the set up of the security tunnel would also be exposed to DoS attacks and the same problem may occur.

2. Actions:

To SA3 group.

ACTION: SA3 is kindly asked to take into consideration the above suggestions.

3. Date of Next TSG-CN1 Meetings:

CN1_26	23rd – 27th September 2002	Miami, USA
CN1_27	11th – 15th November 2002	Bangkok, Thailand