3GPP TSG SA WG3 Security — S3#21 **S3-010673**

27-30 November, 2001

Sophia Antipolis, France

From: **SA3**

To: **CN1, SA2**

Title: **Prevention of identity spoofing in the IMS**

Contact: **Guenther Horn**
Guenther.horn@mchp.siemens.de

Phone: +49 89 636 41494

---

1. Problem

Two contributions to SA3#21, S3-010633 (Dynamicsoft, Ericsson) and S3-010636 (Siemens), identified a problem with the current draft specifications for IMS security, TS 33.203 (S3), TS 23.228 (SA2), and TS 24.228 (CN1), which may lead to a fraudulent user setting up sessions under a false identity and consequently avoiding to be charged for the session. A more detailed description of the attack is included in S3-010633. The possible solutions of the problem involve assumptions about the use of identities for which SA3 requests guidance from CN1 and SA2.

The rest of section 1 gives background information regarding the source of the problem:

SIP messages between the UA and the P-CSCF are integrity protected. This integrity protection also provides message origin authentication. The authenticated origin may be identified by any identity to which the integrity key IK has been (explicitly or implicitly) bound in the registration procedure. These identities include the private identity (IMPI) and the registered public identities (IMPUs).

The S-CSCF needs to inform the P-CSCF about (a subset of) identities to be bound to IK when it sends IK in the registration procedure message (SM3) 4xx Auth_Challenge of TS 33.203v070, section 7.2. When the P-CSCF later verifies the integrity of a SIP message using a key IK it must (explicitly or implicitly) inform the S-CSCF about an identity bound to the IK used. E.g. the P-CSCF could be required to check the IMPUs bound to IK against any IMPU included in the received message. If no such a check is done, then a fraudulent user may e.g. use an IK bound to a registered IMPU of his to generate a correct message authentication code on an INVITE message, but include somebody else's IMPU in the INVITE message. This would lead to a number of threats, e.g. the S-CSCF would then charge the session to the false IMPU.

S3 has realised that simply adding a statement to the specifications that the P-CSCF always checks the IMPU bound to IK against any IMPU included in the received message is not sufficient. The main problem arises from the fact that IMPUs may be implicitly registered. But implicitly registered IMPUs are not known by the P-CSCF at registration time according to the current specifications; hence the P-CSCF cannot bind IK to those IMPUs. (Cf. also the LS from S3#21 to CN4 in S3-010668 where S3 informs CN4 that S3 sees a need to distribute implicitly registered IMPUs from the HSS to the S-CSCF.)

Any solution to the problem described in section 1 has to address two issues:

- which identities are bound to the integrity key IK in message (SM3) 4xx Auth_Challenge of TS 33.203v070, section 7.2?
- how does the P-CSCF inform the S-CSCF about an identity bound to the IK used to verify the integrity of a message received from the UA?

2. Possible solutions

S3 discussed various solutions and agreed to further study at least the following three possible solutions, and variants thereof:

1) The S-CSCF sends the integrity key IK and all public identities for which a user is registered (explicitly or implicitly) to the P-CSCF in message (SM3) 4xx Auth_Challenge of TS 33.203v070, section 7.2. Whenever the P-CSCF later checks the integrity of a SIP message from the UA, using integrity key IK, it checks that any IMPU in the SIP message is one of those received with IK in (SM3).
   There would be no need for the P-CSCF to know the private identity IMPI in this context. Please also note that it has not yet been specified how IK is carried in (SM3) , cf. the accompanying LS from S3#21 to CN1 in S3-010669. When addressing the issue raised in S3-010669 it could also be studied how the IMPUs could be included in (SM3).

2) When the P-CSCF verifies a SIP message from the UA using the integrity key IK it includes the IMPI which was received with IK in (SM3) before forwarding the message to the S-CSCF. The S-CSCF then checks that the IMPI corresponds to the IMPU in the received message. Note that currently there is no field to carry the IMPI in e.g INVITE messages. Note also that this assumes that the P-CSCF is able to retrieve the IMPI from message (SM3).

3) The UA includes the IMPI in the protected part of any integrity protected SIP messages. The P-CSCF verifies the integrity of that message using IK and checks that the IMPI is the one which was received with IK in (SM3). The S-CSCF then checks that the IMPI corresponds to the IMPU in the received message. Note that currently there is no field to carry the IMPI in e.g INVITE messages.

S3 is aware that other solutions are possible. However, solutions requiring additional round-trips have been ruled out. (This applies in particular to additional “end-to-middle” regular authentications for each INVITE mentioned as the third solution in S3-010633.) Also, S3 has ruled out solutions which would require two sets of user specific integrity keys, and/or integrity checks to be performed at two different IMS network entities. (This applies in particular to the creation of an additional session key mentioned as the fourth solution in S3-010633.)

3. Actions

CN1 and S2 are kindly asked to study solutions to the problem described in section 1 and comment on the three possible solutions mentioned in section 2. Other suggestions would be welcome, but should be checked by S3 from a security point of view.

4. Attachments

S3-010633, S3-010636, S3-010668, S3-010669