3GPP TSG SA WG3 Security — S3#21 **S3-010667**

27-30 November, 2001

Sophia Antipolis, France

From: **SA3**

To: **CN1**

Title: **Identity spoofing attacks in the IMS**

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

Phone: +49 89 636 41494

1. Problem

Two contributions to S3#21, S3-010633 (Dynamicsoft, Ericsson) and S3-010636 (Siemens), identified a problem with the current specifications for IMS security, draft TS 33.203 (S3) and draft 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. The problem stems from the fact that the fraudulent user may use an integrity key correctly associated with him by the network to generate a correct message authentication code on an INVITE message, but include somebody else's public identity in the INVITE message. This would be possible because the current specifications do not demand a check by the network that the included public identity belongs to the same user as the integrity key used to verify the message authentication code. A more detailed description of the attack is included in S3-010633.

2. Possible solutions

It was agreed at S3#21 that this problem must be addressed properly in the specifications for IMS security. It was also agreed that it is necessary, as proposed in both S3-010633 and S3-010636, to verify on the network side that any SIP user identity included in a SIP message belongs to the same user as the integrity key used to provide integrity protection for that message between UE and P-CSCF. The S-CSCF, or the P-CSCF, or the two in cooperation, could perform this verification.

The P-CSCF has the integrity keys and performs the integrity check on the network side. However, in view of two recent developments relating to SIP user identities, the P-CSCF may not have the full information on user identities:

- In a REGISTER message the IMPI is now carried in an EAP packet rather than in the From field (cf. LS from S3#20 to CN1 in S3-010539). This means that the IMPI would only be available to the P-CSCF if it could extract it from the EAP packet;
- Public identities (IMPUs) may be implicitly registered. Implicitly registered IMPUs are not sent in registration messages and, hence, are not seen by the P-CSCF unless they are explicitly distributed to it. (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.)

On the other hand, the S-CSCF has the full information on user identities (provided that S3's suggestions in S3-010668 are accepted), but it does not perform the integrity check.

So, neither the P-CSCF nor the S-CSCF may be able to perform the required check that the integrity keys are used together with the correct SIP user identities, unless additional measures are employed. Basically, there are two options: either make sufficient information on user identities available to the P-CSCF, or make sufficient information on the integrity keys used available to the S-CSCF.

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

1) The S-CSCF makes all public identities for which a user owning a particular integrity key IK is registered (explicitly or implicitly) available to the P-CSCF. This could be done e.g. in the same message of the registration procedure in which IK is sent to the P-CSCF. There may still be some room for flexibility as it seems it has not yet been specified how IK is carried in SIP messages, cf. the accompanying LS from S3#21 to CN1 in S3-010669.
   The P-CSCF checks that the integrity key is used with the correct IMPU.
   There would be no need for the P-CSCF to know the private identity IMPI.

2) The P-CSCF is able to retrieve the IMPI from the EAP part of registration messages and, hence, bind it to the integrity key (or agree some other identifier with the home network). The P-CSCF then adds the IMPI (or this other identifier) to all messages sent to the S-CSCF whose integrity could be verified by the P-CSCF.
   The P-CSCF checks that the integrity key is used with the correct IMPI (or identifier), the S-CSCF checks that the IMPI (or identifier) is used with the correct IMPU.

3) The UE includes the IMPI in the protected part of any integrity protected SIP messages. The P-CSCF forwards this message to the S-CSCF.
   The P-CSCF checks that the integrity key is used with the correct IMPI, the S-CSCF checks that the IMPI is used with the correct IMPU.

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, solutions, which would require two sets of integrity keys, and integrity checks to be performed at two different network entities, have been ruled out. (This applies in particular to the creation of an additional session key mentioned as the fourth solution in S3-010633.)

3. Actions

CN1 is 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.