3GPP TSG WG3 Security - S3#21 **Tdoc S3-010633**
Sophia Antipolis, France
27-30 November, 2001

Agenda Item: IMS

Source: Dynamicsoft, Ericsson

Title: The “Fraudulent User” Attack Against the IMS

Document for: Informative

1 Scope and objectives

This contribution describes an attack against the IMS that we believe the current specifications allow. We also invite further contributions to solve the problem.

2 The “Fraudulent User” Attack

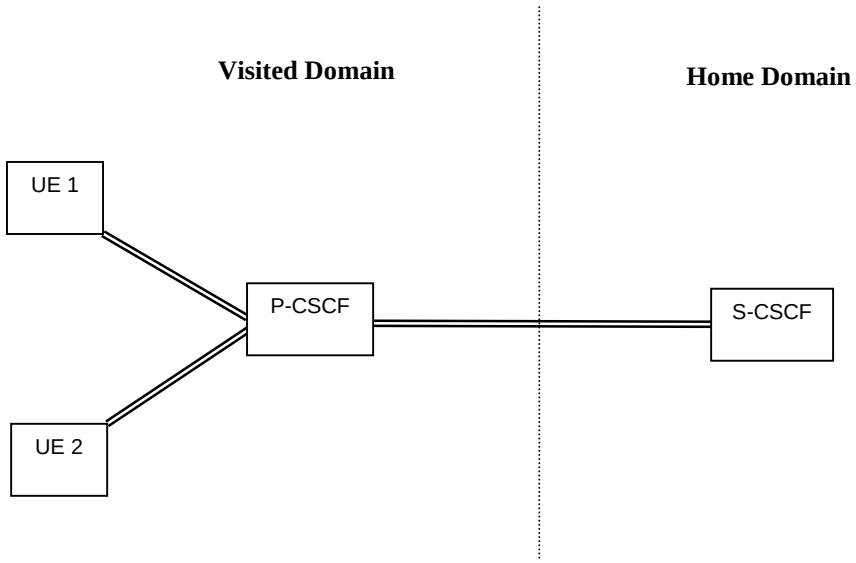

Figure 1. The network architecture.

Figure 1 shows the network architecture in which the attack is performed. In the network, we have a S-CSCF at the home network, and a P-CSCF at the visited network. The P-CSCF is currently serving two clients, UE 1 and UE 2. For clarity, we have omitted certain details such as the I-CSCF and SEGs that may exist between the P-CSCF and the S-CSCF.

In order to describe the attack, we will first outline what normally happens when the terminals use the IMS. First, both UEs must register:

1. UE 1 registers using the private identity *Priv1* and public identity *Pub1*. This involves four messages that all pass through the P-CSCF.
2. UE 2 registers using the private identity *Priv2* and public identity *Pub2*. This also involves the similar four

messages.

As a result of the registration procedure, the UE-1 shares a security association SA1 with the P-CSCF. The UE-2 also has a similar security association SA2. We also assume that secure IPsec tunnels have previously been established between the P-CSCF and the S-CSCF and that it isn't possible to attack the P-CSCF – S-CSCF traffic in any way.

Now, both UEs can make calls by sending INVITEs. This is what happens normally:

3. UE 1 sends an INVITE that is integrity protected using SA1. The INVITE contains "*From: Pub1*" header field. (We use the *From:* header as an example here, but our discussion holds regardless of the used header. For instance, the *Remote-Party-Id:* header would have a similar problem as we will describe later for From:.) *Pub1* is any of the public user identities of the user, including those that are automatically registered by the network during the registration procedures.
4. P-CSCF receives this INVITE and checks the MAC for correctness. It is correct, and the INVITE is forwarded to the S-CSCF.
5. S-CSCF accepts the INVITE as a legitimate one since it came from the IPsec tunnel, and reads the identity of the user from the "*From: Pub1*" header field in the message.
6. UE 2 sends also an INVITE using SA2 and "*From: Pub2*" header field.
7. P-CSCF receives the second INVITE and checks it. The MAC verifies correctly, and the INVITE is also forwarded to S-CSCF.
8. S-CSCF accepts the second INVITE also as legitimate, and sees that the user "*From: Pub2*" is the sender.

So far everything has proceeded correctly. Now we start the actual attack. We assume that the UE 2 is a fraudulent one. As not all the public user identities need to the securely stored in the ISIM, the user may configure the terminal and change the public user ID. Furthermore, even if the public user ID were securely stored, someone could have succeeded in modifying software in the terminal or a laptop to achieve fraudulent behavior. The intention of the UE 2 is to have UE 1 pay for all the calls he makes. Here is what UE 2 will do to make this happen:

9. UE 2 sends an INVITE using SA2 (the right SA for him) and with a "*From: Pub1*" header field. This is syntactically correct, but it is not any of the public user IDs allocated to UE 2.
10. P-CSCF receives the INVITE and checks the MAC for correctness. It is correct, and the INVITE is forwarded to the S-CSCF. Note that even if the P-CSCF checks the integrity protection, it does not necessarily check anything about the actual contents of the message. In particular, the P-CSCF may not have knowledge of the public identities associated with users, and may not be able to know what the *From:* header should contain. While it could perhaps know the public identity that was used during registration, it may not know all the legal public identities for this user, since in general the home networks may allow the implicit registration for multiple public identities.
11. S-CSCF receives the INVITE, and accepts it as a legitimate one because it came out of the IPsec tunnel. However, at this point the S-CSCF no longer has any information from which SA between the UEs and the P-CSCF the message came from. It only has "*From: Pub1*" header field, from which it incorrectly determines that the call is being made by UE 1. Note that replies to the INVITE will be sent according to the *Via:* headers (not the current contact location of the public identifier), and would thus reach the fraudulent UE.

As a result, UEs have the capability to send messages that appear to come from a particular UE but in fact come from another. The primary cause of this problem is due to the hop-by-hop security model combined with the lack of complete information either the P-CSCF has on what is allowed in messages or the S-CSCF has on where the message actually came from.

3 Possible Solutions

We do not try to describe a solution to this problem in this contribution, but some discussion about possible solutions is in order.

First, as discussed above, it might be possible for the P-CSCF to keep the original *From:* header from the REGISTER, and check subsequent INVITEs against that. However, since we want to have functionality in the

IMS for implicitly registering a number of public identities without additional messaging, it seems that the P-CSCF can not know the correct contents of the *From:* field. We also feel that signalling the list of allowed public identities between the home and visited networks would be a too complicated solution.

Secondly, it might be possible for the P-CSCF to attach an identifier to a user during registration, and attach this identifier to all messages forwarded to the S-CSCF. The S-CSCF could then check the correct *From:* header by correlating this identifier with information stored during registration time. Those *From:* fields would be allowed that are allowed for the private identifier that authenticated during the registration, not others. It is for further study whether a new header field is needed or an existing one can be used, whether the address of the P-CSCF should be included in the identifier look-up at the S-CSCF, and what implications this solution sets for the S-CSCF data bases and so on. One concern in this approach is that different/incorrect parser implementations at the P-CSCF and S-CSCF might allow for the UEs to submit its own fraudulent identifier field without P-CSCF noticing this and yet having S-CSCF accept the UE's field and not the one attached by P-CSCF.

Thirdly, we could run "end-to-middle" regular authentication for each INVITE. This approach has the drawback that additional roundtrips may be introduced, and HSS/AAA operations are needed in the home network for each authentication.

A fourth possible solution is the generation of a session key based on the authentication at registration time, and using that session key to perform an additional authentication at each INVITE, without any HSS/AAA involvement. Variations of this approach either use Digest-like authentication without integrity protection, or full integrity protection; for the integrity protection to work through the P-CSCF we'd have to have mechanisms in place to know which parts of the message the P-CSCF may be modifying.

4 Conclusions

An attack exists in the current IMS specifications that allow fraudulent users to cause incorrect billing information, among other things. Some thoughts on possible solutions are briefly discussed, but the contributing companies are invited to propose solutions for the next SA3 meeting. A solution should fulfil at least the following requirements:

- Must prevent the attack.
- Must not introduce HSS/AAA operations for each INVITE.
- Must minimise additional roundtrips and bandwidth for each INVITE.
- Must not force the visited network to know what the legal public identities are.