3GPP TSG SA WG3 Security — S3#29 **S3-030413**

15 – 18 July 2003

San Francisco, USA

Source: **Siemens**

Title: **Evaluation of proposals for security at the Ut (formerly: Mt) reference point**

Document for: **Discussion and decision**

Agenda Item: **7.18 Presence**

Abstract

In SA3#27, several contributions (TD S3-030223 and 224 by Siemens, TD S3-030245 by Ericsson and TD S3-030256 by Nokia) discussed possible solutions for security for the use of HTTP at the Ut reference point. Objections were raised against all these contributions. These objections are documented in the meeting report. This contribution evaluates the objections raised. It also contains a brief summary of the alternative proposals. Siemens still prefers the IMS-based solution, but the second choice would be a BSF-based solution.

---

1. Introduction

Three proposals have been presented so far by Siemens, Ericsson, and Nokia (cf. documents TDs S3-030223 and 224, TD S3-030245 and TD S3-030256). It should be mentioned that Nokia's contribution 256 leaves the choice between two options open. One of these is close to Ericsson's solution, hence not discussed separately.

In short, the proposals can be summarised as follows:

All the proposals agree that TLS between the UE and an application server or authentication proxy should be used to provide confidentiality, integrity and server authentication. The proposals differ somewhat in the methods for client authentication where either http digest, http digest aka or a variant of the latter are proposed. There main difference lies in key management.

1) IMS-registration based (Siemens): client authentication is achieved through http digest. The keys shared between UE and application server (could also be an authentication proxy) over the Ut reference point, which are required to perform http digest, are derived at the UE and the S-CSCF from the confidentiality key CK obtained in an IMS registration, and then pushed from the S-CSCF to the application server AS over the ISC interface. A summary of the proposal is contained in the appendix to this contribution, for details see TDs S3-030223 and 224.

2) Use of http digest aka v2 (Ericsson): client authentication is achieved through a new variant of http digest aka. In order to run http digest aka v2 between the UE and the application server (or authentication proxy) over the Ut reference point 3G AKA authentication vectors need to be obtained from the HSS. For this purpose, every application server (or authentication proxy) has an interface to the HSS yet to be defined. On the UE side, the USIM has to be involved in client authentication.

3) BSF-based (Nokia): client authentication is achieved through http digest. The keys shared between UE and application server (or authentication proxy) over the Ut reference point, which are required to perform http digest, are obtained using the generic bootstrapping architecture for the support for subscriber certificates. The shared keys are obtained at the UE and the BSF (Bootstrapping Server Function) through a run of protocol A (likely to be http digest aka) between UE and BSF and protocol C between BSF and HSS (see TS on support for subscriber certificates), and then transported from the BSF to the AS using protocol D. Protocols C and D still need to be defined, but a list of requirements for protocol C is available.

2. Comments on objections raised

The following **objections** were raised **against the IMS-based approach**, according to the SA3#28 meeting report:

1 Restricted to IMS users only
Comment: *this is true. But the Ut reference point to be secured is part of the IMS architecture, so no undue restriction is seen here. Please note that the alternative proposals also rely on dedicated 3GPP Rel 6 functionality, though not on IMS.*

2 At least 1 IMS registration is needed for every profile prior to contacting the Application Server
Comment: *the number of profiles required for contacting a particular AS seems very limited, so the issue may in practice be very minor*

3 Complexity: 3rd Party Registration, Key Management, Update at each (Re-)Authentication, Key Synchronisation
Comment:
- 3rd Party Registration: the mechanism for this is already available from SIP, the ISC-interface is also available, so nothing new is introduced here;
- Key Management: this remark is a bit general. Regarding the part of the key management which relates to the interaction with the HSS and the USIM, this proposal is particularly efficient as no new protocol runs are needed. Key derivation functions are typically based on hash functions, hence efficient to implement. The keys distributed from the S-CSCF to the AS can be piggy-backed on existing messages;
- Update at each (Re-)Authentication: this is indeed part of the current proposal. The update uses the 3rd party registration function available from SIP and already specified for 3GPP in TS 23.218, so the complexity is deemed acceptable, given that the number of ASs associated with one user will be small.
- Key Synchronisation: Key synchronisation between UE and AS is achieved either through re-tries and re-registrations or through key indications from the AS to the UE, exploiting a property of http digest. The former approach requires slightly less specification while the latter avoids re-tries in rare failure conditions.

4 S-CSCF impacted
Comment: *this is true. However, this should be weighed against the fact that the alternative proposals have additional impact on the HSS. Furthermore the S-CSCF already implements large parts of the required functionality as part of it's role in the IMS (digest-AKA, Cx interface).*

5 UE requires non-volatile memory / storage of normally deleted secret data
Comment: *the UE already has a non-volatile memory in which also security-relevant data such as the parameter START is stored. So, this is nothing new for the UE. The storage in non-volatile memory is only needed for the case when IMS is not available after power-on.*

6 Key derivation done in terminal (not UE)
Comment: *this should probably read "not USIM" rather than "not UE". According to 3G specs, the key CK is available in the ME, so keys derived from CK can also be available in the ME. 3GPP has decided quite some time ago to address the problem of rogue terminals by sufficiently frequent re-authentications, rather than trough a change in the functionality split between ME and USIM.*

7 Keys transported over SIP which it is not designed to do
Comment: *this seems an argument of more philosophical nature. The proposal shows a specific way how to embed keys in a particular SIP message.*

8 Terminal needs TLS connection with many Network End-Points
Comment: *this seems to be a misunderstanding. The remark probably refers to the fact that the proposal only mentions application servers, but not authentication proxies. But, as remarked above, authentication proxies could be supplied with keys in the very same way as application servers. The key management solution discussed here can be considered rather independent of the question of how to secure http or use TLS based on the resulting keys.*

Comments on the IMS-based approach in the LS from CN1 (S3-030325)

CN1 sees that the solutions described in the liasion are feasible. However from a CN1 point of view the solutions have the following drawbacks:

- This would be the first case where a Release-6 service in an Application Server requires the S-CSCF to be updated to Release-6 which causes backward compatibility problems.
  Comment: *the alternative is a Release 6 update of the HSS which requires a new interface to the application server, creating similar backward compatibility problems. It seems more reasonable to update the S-CSCF to support a new IMS-based service.*

- It is anticipated that the key derivation in the S-CSCF puts additional processing load on the S-CSCF which is multiplied by the number of application servers involved.
  Comment: *there is indeed additional processing load, but typically key derivation functions can be implemented quite efficiently.*

- CN1 thinks that registration should be used exclusively for authentication of the UE to the IMS.
  Comment: *apart from the fact that such a consideration should be the concern of SA3, it is not quite clear what is meant here. Registration is indeed used also in the proposal under discussion for authentication of the UE to the IMS. The fact that the UE is authenticated to the IMS is then used to authenticate the user to the AS. Similar approaches are quite commonly used, e.g. the fact that a user has been authenticated to GSM may be used to authenticate the user towards some service.*

The following **objections** were raised **against the approach** using http digest aka v2, according to the SA3#28 meeting report:

1 RFC [on http digest aka v2] is still under development in IETF
  Comment: *this is true. Although, admittedly, the difference between version 1 and 2 of http digest aka is small, IETF timetables are difficult to predict.*

2 New Cx-like interface is needed
  Comment: *this is true. So far, no requirements for the new interface are available, CN4 has not started the work yet.*

3 Number of elements having an interface to HSS
  Comment: *this is a major concern. If every application server had an interface with the HSS this would be unacceptable from a security point of view. The situation would be improved if only one or a small number of authentication proxies were used.*

4 Complexity: Heavy consumption of AVs
  Comment: *this is also an important issue. For each client authentication after TLS tunnel establishment, an authentication vector is consumed. Authentication proxies would not help here.*

5 Effects on SQN handling
  Comment: *more authentication domains are likely to be needed than with the other approaches. This may have a negative impact on sequence number handling.*

6 Server Authentication is done twice
  Comment: *this is efficiency issue, though not a security issue.*

7 Detail of Proxy Functionality missing
  Comment: *the proposal has concentrated so far on the protocol alternatives to mitigate man-in-the-middle attacks. No complete architecture is currently available, and no description of the functionality of an authentication proxy and the security protocols it supports.*

Additional objection raised **against the BSF-based approach:**

8 Dependency on BSF specification
  Comment: *this is true. But the dependency could perhaps be reduced by observing that it may suffice for a start that the specifications of protocols A and C, and the requirements on protocol D are available.*

3. Comparison with guidelines suggested in the companion contribution on HSS/HLR-related security architecture issues

A companion contribution on HSS/HLR-related security architecture issues expressed a concern with the proliferation of different security mechanisms in 3GPP Release 6, and in particular with the potentially negative impact on the HSS or HLR. The reader is referred to that contribution for details.

1) *IMS-registration based solution:* the proposal is completely in line with the guidelines suggested as it does not introduce any new nodes or interfaces handling authentication vectors. It does not lead to additional consumption of authentication vectors either as the authentication comes for free with the IMS registration. It does not introduce an additional authentication domain.

2) *Use of http digest akav2:* the degree to which this solution is compatible with the guidelines from the contribution on HSS/HLR-related security architecture issues depends on the use and the precise role of an authentication proxy. If each application server has a direct interface to the HSS, then the solution seems to be completely incompatible with those guidelines. But if only one authentication proxy is used then the compliance with the guidelines could be better. The authentication proxy could assume a role similar to that of a BSF. But if the authentication proxy would assume a role similar to that of a BSF then the questions would arise why not the same approach is used. Furthermore, secure connections are likely to be required between an authentication proxy and the application servers. Also, an authentication proxy would probably have to handle all traffic, not only security traffic.

3) *BSF-based solution:* this proposal also seems to be largely in line with the above guidelines. It is true that a new node, the BSF, and a new interface, namely C, are introduced. Also, a new domain would be introduced. But the solution has the potential to make the introduction of further nodes, interfaces and domains unnecessary. The additional consumption of authentication vectors depends on the particular way shared keys are obtained in the subscriber certificate architecture, but could be quite small, see section 5 below.

Conclusions

The IMS-based solution does not have any negative impact on the HSS or the 3G authentication scheme, as opposed to the other two solutions. It uses only available IMS interfaces and SIP messages, hence does not require the specification of new interfaces. The objections were addressed, and are not seen as a fundamental obstacle. Hence, the IMS-based solution is preferred. If that cannot be agreed a BSF-based solution would be the second choice.