3GPP TSG SA WG3 Security — S3#15 **S3-000561**

12-14 September, 2000

Washington D.C., USA

Source: Siemens AG

Title: Proposed changes and discussion of open issues for draft 3G TR "Access security for IP-based services"

Document for: Discussion / Decision

Work item: Access security for IP-based services

Agenda item: tbd

Abstract

This contribution proposes changes to the draft 3G TR "Access security for IP-based services" and discusses issues which have to be considered for its further development.

Proposed changes to 3G TR "Access security for IP-based services"

- **Section 5:**

  It is proposed to replace the sentence "In addition, the IM CN subsystem security mechanism shall be consistent with security techniques employed in the Internet ..." by "In addition, the IM CN subsystem security mechanisms should be as far as possible consistent with security techniques employed in the Internet ....". This would align the TR with [Rep S3#14, 7.1].

- **Section 5, figure 1:**

  It is proposed to reuse the figure for the IM CN Subsystem Security Architecture from the former version v0.0.0 of the 3G TR "Access security for IP-based services", considering the change described below.

  Replace the "IM CN Subsystem" in the figure of the old version v0.0.0 by "Serving CSCF" and "HSS" with the Cx interface in between, as in the new version v0.1.0.

  The figure (of version 0.0.0) shows the security architecture for the IM CN subsystem and indicates that the IM CN subsystem provides "Logical firewall and policy" functionality. In the section there is no accompanying text supporting the need for this. It is proposed to further examine if this functionality is really needed, for the following reason:

  Firewalls are needed to protect the overall IP-based part of the core network from attacks, and are not specifically needed to protect the IM CN subsystem. It does not seem to be likely that the IM CN subsystem has its own firewall systems irrespective of the firewall systems installed to protect the overall IP core network. In the accompanying text to the figure in [S3-000458] it is stated that the firewall functionality has to be provided from the IM CN subsystem to protect it from rogue software clients. The protection of the network from rogue clients is however provided by access security mechanisms, i.e. by authentication and by integrity protection of the messages from the client. Thereby threatening IP packets received over the air interface could be discarded without having a firewall in the communication path.

- **Section "Informative Annex":**

  It is proposed to incorporate the discussion on the security mechanisms for the provision of access security for IP-based services [S3-000446] in an informative annex. In the subsection on "HTTP security mechanism Digest Authentication" of [S3-000446] the sentence "Authentication of a server to a client is also possible [RFC 2617, 3.2.2]" should be replaced with "Authentication of a server to a client is not possible at the moment, but appropriate mechanisms are under discussion in the IETF SIP working group. (Cf. [RFC 2543bis-01] Annex G: Changes to be made.)"

- **Section 8.1:**

  The section contains the description how the UMTS AKA can be performed using the SIP protocol by introducing a new authentication mode for SIP.

  It is proposed to additionally remark in the description, that on UA and on proxy side the session keys for access confidentiality and integrity have to be derived.

Discussion of open issues of 3G TR "Access security for IP-based services"

- **Section 8.1:**

  The section contains the description how the UMTS AKA can be performed through the SIP protocol by introducing a new authentication mode for SIP. For the further development of the proposal some issues to be considered are raised below. Section 6.1 only describes the exchange of the crypto-messages for the UMTS AKA.

  - It additionally has to be clarified by which identity a user is authenticated. It is proposed to authenticate a user by his unique user identity in the IM domain (the structure of this identity is still under discussion in SA2). It then has to be clarified if this identity has to be bound to the (temporary) IP address of the terminal on the bearer level, given by the PDP context. (This would not imply that IM domain security depended on PS domain security.)
  - It is proposed to keep the description of the exchange of the AKA parameters between the MS and the CSCF separate from the description how the parameters are obtained by the CSCF from the HSS as different protocols may be used in both cases. In section 6.1 the protocol used to exchange the crypto-parameters is SIP. Between CSCF and HSS of the user the protocol to be used is not yet specified by SA2, it may be SIP as well, but also other protocols, e.g. AAA protocols may be used.
  - It has to be determined at which entity the authentication is carried out. It seems to be reasonable to carry out the AKA at the same CSCF that received the user profile data from the HSS. If this will be the serving CSCF, and whether the serving CSCF will be located in the home or in the visited network is still under discussion within SA2.

- **Sections 8.2 and 8.3:**

  - It has to be determined at which entity encryption / integrity protection of SIP messages has to be performed, using the session keys agreed in the previous run of the AKA. It seems to be reasonable that this is the CSCF (most likely the serving CSCF) that also carries out the AKA, but it may also be possible that there are reasons that a different CSCF is used. (This may e.g. be the case if the serving CSCF is located in the home environment of the user and a CSCF in the visited network acts as a SIP proxy.)
  - It has to be specified which mechanisms are to be used to carry out encryption / integrity protection of SIP messages.

    In [S3-000447] the security mechanisms specified by the IETF for SIP are discussed and evaluated. It is concluded that IPSec meets the security as well as the system requirements of [S3-000446] (if an appropriate AKA protocol would be specified). The other security mechanisms proposed so far for SIP which are also discussed in [S3-000447] do not meet these requirements.

- **It is therefore proposed as a working assumption to use IPSec to provide confidentiality and integrity of SIP messages between UE and CSCF. The following issues need to be addressed in order to show the viability of this working assumption:**
  - **Establishment of security associations (SAs):** In the course of the SIP registration procedure, authentication and key agreement has to be carried out. If IPSec were used for the protection of SIP messages besides the keys themselves also other parameters for the IPSec SA (security association) would have to be established. All these parameters have to be made available to the UE in the course of the AKA procedure.
  - **Replay protection for IPSec:** If an automated key management is used for IPSec then IPSec also provides replay protection. If this is not the case then a replay protection has to be additionally specified.
  - **Security session concept**: It is desirable that the security association for IPSec established in the course of the registration procedure is used to protect subsequent calls until the user de-registers himself at the CSCF (or the security association expires). We denote the life-time of a security association by " security session".) This would avoid that for each call the AKA protocol would have to be run between UE and CSCF.
  - **Change of IP addresses:** Under certain circumstances a new run of the AKA may be required, however: The IP addresses of the communicating endpoints are at least part of the selectors for an SA. This implies, that if for a roaming user the IP address of the UE or of the serving CSCF changes during a session a new SA has to be established. This could occur if the user roams into the area of another GGSN during a security session and subsequently gets a new PDP context with a new temporary IP address or if the serving CSCF changes.
  - **Multiple users on a terminal**: If there is only one user on a UMTS terminal, then the IP-addresses of the UE and the CSCF, respectively, are sufficient to identify the appropriate SA established in the AKA procedure.

    If, however, there are two or more users (which should be charged based on their different IM identities) using the same UE (e.g. a mobile laptop) for overlapping security sessions then the IP-addresses of CSCF and UE are not sufficient as selectors for the SAs. As the IM identities are not available at IP level, additionally the port numbers of the SIP applications on the UE are needed to distinguish between users, whereas on the server side the IP address of the CSCF is still sufficient. As port numbers used by SIP clients may change in each SIP request, the support for multiple users on a terminal would raise the new requirement for UMTS IM-capable terminals that SIP is implemented in a way that an instance of a SIP client relating to one user on the UE always uses the same port number during a session.

    It has to be clarified whether multiple users on an IM-terminal are a requirement, and if so, whether SIP implementations can satisfy the above requirement.

References

[S3-000446] 3GPP TSG SA WG3 Security: *Requirements on access security for IP-based services*; Siemens, July 2000.

[S3-000447] 3GPP TSG SA WG3 Security: *Overview of security mechanisms for access security for IP-based services*; July 2000.

[S3-000458] 3GPP TSG SA WG3 Security: Security requirements for access to R'00 IM subsystem; Nortel, July 2000.

[Rep S3#14] 3GPP TSG SA WG3 Security: *Draft Report on S3#14, v.0.0.6*; Oslo, 1-4 August, 2000.

[TR 33.xxx] 3GPP TSG SA WG3 Security, TR 33.xxx: "Access security for IP-based services"; v0.1.0, September 2000.

[RFC 2543bis-01] IETF RFC 2543bis-01: *SIP: Session Initiation Protocol*; August 2000.

[RFC 2617] IETF RFC 2617: *HTTP authentication: Basic and digest access authentication;* June 1999.