3GPP TSG SA3-SA2 Joint Meeting **Tdoc S3z010034**
Madrid, Spain 26th April, 2001

Source: Motorola
Title: Security Relationships of Interogating CSCF (I-CSCF)
Document for: Discussion and Decision

1 Introduction

At the last SA2-SA3 joint meeting held in Gothenburg AT&T presented S2-010512 specifying CSCF Security Requirements for TS 23.228. Although some security relationships for P-CSCF and S-CSCF were agreed in a subsequent revised version of that contribution it was not agreed at this meeting to specify any security relationships between the I-CSCF and either the P-CSCF or the S-CSCF. This contribution proposes some text, which it is hoped can form the basis for agreement of text for inclusion in TS 23.228 that the I-CSCF will maintain a security relationship with both the P-CSCF and the S-CSCF

2 Discussion

The current situation is of concern because the architecture outlined by SA2 in TS 23.228 and the corresponding derived SIP session flows in TS 24.228 (being worked jointly by SA2 and CN1) depend on the I-CSCF being able to read and modify headers in requests and responses from the P-CSCF and the S-CSCF. The assumption during the development of the SIP session flows in TS 24.228 was always that the I-CSCF would maintain a security relationship with the P-CSCF and the S-CSCF. Without an agreed statement in TS 23.228 specifying that the I-CSCF maintains a security relationship with both the P-CSCF and the S-CSCF the work of SA2 and CN1 is at risk.

In the architecture specified in TS 23.228 and SIP flows in TS 24.228 the I-CSCF participates in the registration procedures receiving REGISTER messages from the P-CSCF and then based on data from the HSS selects a S-CSCF and forwards the REGISTER message to it. The I-CSCF can optionally ensure that it (or another I-CSCF) remain in the path for all subsequent Session Initiation Messages by adding itself (or another I-CSCF) to the PATH header in the REGISTER message.

The PATH header is used in the 3GPP architecture by the P-CSCF and S-CSCF to preload a route for SIP signalling messages. If an I-CSCF is contained in the PATH then INVITE and other SIP signalling messages will be forwarded between P-CSCF and S-CSCF via an I-CSCF. When an I-CSCF receives an INVITE message from a P-CSCF it will modify the VIA, ROUTE and RECORD-ROUTE headers before forwarding to the S-CSCF. Likewise the I-CSCF will again modify the VIA header for responses taking the return path. Similarly the I-CSCF will modify the VIA, ROUTE and RECORD-ROUTE headers for INVITE messages it receives from the S-CSCF before forwarding them to the P-CSCF and again modify the VIA in responses following the return path.

It is assumed that these SIP signalling messages being passed between the P-CSCF, I-CSCF and S-CSCF utilize security associations methods defined in the Network Domain Security Specification TS 33.200. If the I-CSCF is not party to these security associations then it cannot perform the above functions required in TS 24.228. Therefore it is proposed that these security associations also be specified in TS 23.228 between I-CSCF and P-CSCF and also between I-CSCF and S-CSCF.

It is also proposed to modify the currently agreed text for the P-CSCF to UE from **Security Association** to **Security Relationship** to indicate that a different mechanism is being utilised between P-CSCF and UE from that between the network elements and that this mechanism is not an IPsec tunnel which is commonly associated with the term Security Association. Also The term Security Association is by definition unidirectional so it is not really correct to say that the P-CSCF maintains a security association with each UE.

It is also proposed to provide a little more detail for each CSCF role of the security functions implemented and to also fill in similar security relationship statements for the Border Gateway Control Function (BGCF).

3 Proposal

It is proposed that the joint meeting after discussion agree the text in the attachment for inclusion in TS 23.228 and if agreed Motorola will bring a formal CR against TS 23.228 containing the agreed text for approval at SA2#18.

4.6 Roles of Session Control Functions

The CSCF may take on various roles as used in the IP multimedia subsystem. The following sections describe these various roles.

4.6.1 Proxy-CSCF

The Proxy-CSCF (P-CSCF) is the first contact point within the IM CN subsystem. Its address is discovered by UEs following PDP context activation, using the mechanism described in section “Procedures related to Local CSCF Discovery ”. The P-CSCF behaves like a Proxy (as defined in RFC2543 or subsequent versions), i.e. it accepts requests and services them internally or forwards them on, possibly after translation. The P-CSCF may also behave as a User Agent (as defined in the RFC2543 or subsequent versions), i.e. in abnormal conditions it may terminate and independently generate SIP transactions.
The Policy Control Function (PCF) is a logical entity of the P-CSCF. If the PCF is implemented in a separate physical node, the interface between the PCF and the P-CSCF is not standardised.
The functions performed by the P-CSCF are:

- Forward the SIP register request received from the UE to an I-CSCF determined using the home domain name, as provided by the UE.
- Forward SIP messages received from the UE to the SIP server (e.g. S-CSCF) whose name the P-CSCF has received as a result of the registration procedure.
- As part of processing of the request and before forwarding, the P-CSCF may modify the Request URI of outgoing requests according to a set of provisioned rules defined by the network operator (e.g. Number analysis and potential modification such as translation from local to international format.)
- Forward the SIP request or response to the UE.
- Detect an emergency session and select a S-CSCF in the visited network to handle emergency sessions.
- ~~The g~~Generation of CDRs.
- Maintain a Security ~~Association~~ Relationship between itself and each UE, as defined in Access Security for IP-based services Specification TS 33.2xx [19].
- ~~Provide security towards~~ Maintain Security Associations with Interrogating-CSCFs and Serving-CSCFs. The Security Associations are received or negotiated by the ~~by~~ security methods defined in Network Domain Security specification TS 33.200 [20].
    - Verify integrity of incoming messages and decrypt incoming ciphered messages based on the Security Association.
    - Apply security protections based on the Security Associations to the outgoing messages.

Editor’s Note: The following functions require further study:

- Authorisation of bearer resources and QoS management. Details of the P-CSCF role in QoS management and authorisation of bearer resources for the session are being investigated by the QoS ad-hoc group.

4.6.2 Interrogating-CSCF

Interrogating-CSCF (**I-CSCF**) is the contact point within an operator's network for all connections destined to a subscriber of that network operator, or a roaming subscriber currently located within that network operator's service area. There may be multiple I-CSCFs within an operator's network. The functions performed by the I-CSCF are:
Registration

- Assigning a S-CSCF to a user performing SIP registration (see section on Procedures related to Serving-CSCF assignment)

Session Flows

- Route a SIP request received from another network towards the S-CSCF.
- Obtain from HSS the Address of the S-CSCF.
- - Forward the SIP request or response to the S-CSCF determined by the step above
- Maintain Security Associations with Proxy-CSCFs and Serving-CSCFs. The Security Associations are received or negotiated by the methods defined in Network Domain Security specification TS 33.200 [20].
    - Verify integrity of incoming messages and decrypt incoming ciphered messages based on the Security Association.
    - Apply security protections based on the Security Associations to the outgoing messages.

Charging and resource utilisation:

- Generation of CDRs.

In performing the above functions the operator may use the I-CSCF or other techniques to hide the configuration, capacity, and topology of the network from the outside. When the I-CSCF is chosen to meet the hiding requirement then for sessions traversing across different operators domains, the I-CSCF may forward the SIP request or response to another I-CSCF allowing the operators to maintain configuration independence.

4.6.3 Serving-CSCF

The Serving-CSCF (S-CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services. Within an operator's network, different S-CSCFs may have different functionalities. The functions performed by the S-CSCF during a session are:
Registration

- May behave as a Registrar as defined in RFC2543 or subsequent versions, i.e. it accepts registration requests and makes its information available through the location server (eg. HSS).

Session flows

- Session control for the registered endpoint's sessions.

- May behave as a Proxy Server as defined in RFC2543 or subsequent versions, i.e. it accepts requests and services them internally or forwards them on, possibly after translation.

- May behave as a User Agent as defined in RFC2543 or subsequent versions, i.e. it may terminate and independently generate SIP transactions.

- Interaction with Services Platforms for the support of Services

- Provide endpoints with service event related information (e.g. notification of tones/announcement together with location of additional media resources, billing notification)

- - Maintain Security Associations with Interrogating-CSCFs, BGCFs, ~~Security towards~~ and Proxy-CSCFs~~.,~~ The Security Associations are received or negotiated by the methods ~~as~~ defined ~~by~~ in the Network Domain Security specification TS 33.200 [20].

    - Verify integrity of incoming messages and decrypt incoming ciphered messages based on the Security Association.

    - Apply security protections based on the Security Associations to the outgoing messages.

- Based on operator policy, maintain Security Associations with another SIP server located within an ISP domain outside of the IM CN subsystem.

    - Verify integrity of incoming messages and decrypt incoming ciphered messages based on the Security Association.

    - Apply security protections based on the Security Associations to the outgoing messages.

- On behalf of an originating endpoint (i.e. the originating subscriber/UE)

    - Obtain from a database the Address of the I-CSCF for the network operator serving the destination subscriber from the destination name of the terminating subscriber (e.g. dialled phone number or SIP URL), when the destination subscriber is a customer of a different network operator, and forward the SIP request or response to that I-CSCF.

    - When the destination name of the terminating subscriber (e.g. dialled phone number or SIP URL), and the destination subscriber is a customer of the same network operator, forward the SIP request or response to an I-CSCF within the operator's network.

    - Depending on operator policy, forward the SIP request or response to another SIP server located within an ISP domain outside of the IM CN subsystem.

- On behalf of a destination endpoint (i.e. the terminating subscriber/UE)

    - Forward the SIP request or response to a P-CSCF for a MT session to a home subscriber within the home network, or for a subscriber roaming within a visited network where the home network operator has chosen not to have an I-CSCF in the path

- Forward the SIP request or response to an I-CSCF for a MT session for a roaming subscriber within a visited network where the home network operator has chosen to have an I-CSCF in the path.

Charging and resource utilisation:

- Generation of CDRs.

4.6.4 Breakout Gateway Control Function

The Breakout Gateway control function (BGCF) selects the network in which PSTN breakout is to occur. If the BGCF determines that the breakout is to occur in the same network in which the BGCF is located within, then the BGCF shall select a MGCF which will be responsible for the interworking with the PSTN. If the break out is in another network, the BGCF will forward this session signalling to another BGCF, or an MGCF, depending on the configuration, in the selected network.

The functions performed by the BGCF are:

- Receives request from S-CSCF to select appropriate PSTN break out point for the session
- Select the network in which the interworking with the PSTN is to occur. If the interworking is in another network, then the BGCF will forward the SIP signalling to the BGCF of that network.
- Select the MGCF in the network in which the interworking with PSTN is to occur and forward the SIP signalling to that MGCF. This may not apply if the interworking is a different network.

- Maintain Security Associations with Serving-CSCFs and MGCFs. The Security Associations are received or negotiated by the methods defined in the Network Domain Security specification TS 33.200 [20].
    - Verify integrity of incoming messages and decrypt incoming ciphered messages based on the Security Association.
    - Apply security protections based on the Security Associations to the outgoing messages.

Charging and resource utilisation:

- Generation of CDRs.

The BGCF may make use of information received from other protocols, or may make use of administrative information, when making the choice of which network the interworking shall occur.