3GPP TSG-SA3 Meeting #24
Helsinki, Finland, Date

S3-020384

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM □ ME/UE ☒ Radio Access Network □ Core Network ☒

Title:	⌘	MITM attack for TCP SA negotiation		
Source:	⌘	Ericsson		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	2002-07-04
Category:	⌘	**F**	***Release:*** ⌘	Rel-5
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *REL-4 (Release 4)* *REL-5 (Release 5)*

Reason for change:	⌘	An attacker can mount a quite critical attack by changing the SPI for e.g. TCP SAs when UDP is used for setting up the SAs. The attack cannot be detected by neither the UE nor the P-CSCF until a request is sent over TCP but then it will not work.
Summary of change:	⌘	The P-CSCF shall repeat the TCP related parameters that was sent by the UE during sip security agreement. The UE will then check that it receives the same information as it sent in the initial message.
Consequences if not approved:	⌘	A sever attack can be mounted against TCP SAs

Clauses affected:	⌘				
Other specs affected:	⌘	☒	Other core specifications	⌘	TS24.229
		□	Test specifications		
		□	O&M Specifications		
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

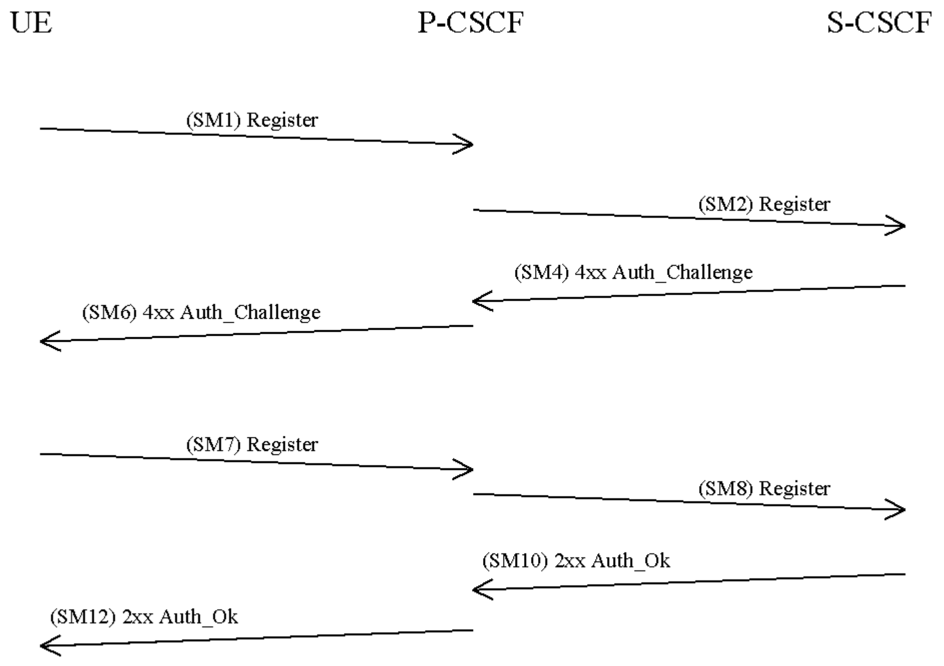
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

7.2 Set-up of security associations (successful case)

The set-up of security associations is based on [draft-IETF-sip-sec-agree]. Annex X of this specification shows how to use [draft-IETF-sip-sec-agree] for the set-up of security associations.

In this section the normal case is specified i.e. when no failures occurs. Note that for simplicity some of the nodes and messages have been omitted. Hence there are gaps in the numbering of messages, as the I-CSCF is omitted.



The UE sends a Register message towards the S-CSCF to register the location of the UE and to set-up the security mode, cf. section 6.1. In order to start the security mode set-up procedure the UE shall include a *Security-setup-line* in this message. The *Security-setup-line* in SM1 contains the SPIs and the numbers of the protected ports assigned by the UE for the SAs for TCP and UDP. It also contains a list of identifiers for the integrity algorithms which the UE supports.

> SM1:
> REGISTER(Security-setup = *SPI_U_TCP, SPI_U_UDP, Port_U_TCP, Port_U_UDP, UE integrity algorithms list)*

Upon receipt of SM1, the P-CSCF temporarily stores the parameters received in the *Security-setup-line* together with the UE's IP address from the source IP address of the IP packet header, the IMPI and IMPU. Upon receipt of SM4, the P-CSCF adds the key IK_{IM} received from the S-CSCF to the temporarily stored parameters. The P-CSCF then selects the SPIs for the inbound SAs for TCP and UDP. In order to determine the integrity algorithm the P-CSCF proceeds as follows: the P-CSCF has a list of integrity algorithms it supports, ordered by priority. The P-CSCF selects the first integrity algorithm on its own list which is also supported by the UE.
The P-CSCF then establishes the two pairs of SAs in the local security association database.

The *Security-setup*-line in SM6 contains the SPIs assigned by the P-CSCF for the SAs for TCP and UDP and the fixed number of the protected port at the P-CSCF. It also contains a list of identifiers for the integrity algorithms which the P-CSCF supports. If SM1 was carried by UDP then the P-CSCF shall repeat the TCP SA related parameters as assigned by the UE in SM1 as specifed in SM6 below. If SM1 instead was carried by TCP then the P-CSCF shall repeat the UDP SA related parameters as assigned by the UE in SM1 i.e. the TCP related parameters in SM6 below is changed to the corresponding UDP parameters.

SM6:
4xxAuth_Challenge(Security-setup = *SPI_P_TCP, SPI_P_UDP, Port_P*, *P-CSCF integrity algorithms list*, *SPI_U_TCP, Port_U_TCP)*

Upon receipt of SM6, the UE determines the integrity algorithm as follows: the UE selects the first integrity algorithm on the list received from the P-CSCF in SM 6 which is also supported by the UE.
The UE then proceeds to establish the two pairs of SAs in the local SAD. The UE shall check that the SPI values repeated by the P-CSCF are the same as in SM1 and then discard the message if this check is unsuccesful.

The UE shall integrity-protect SM7 and all following SIP messages.Furthermore the integrity algorithms list received in SM6 shall be included:

SM7:
REGISTER(Security-setup = *P-CSCF integrity algorithms list)*

After receiving SM7 from the UE, the P-CSCF shall check whether the integrity algorithms list received in SM7 is identical with the integrity algorithms list sent in SM6. If this is not the case the registration procedure is aborted. The P-CSCF shall include in SM8 information to the S-CSCF that the received message from the UE was integrity protected. The P-CSCF shall add this information to all subsequent REGISTER messages received from the UE that have successfully passed the integrity check in the P-CSCF.

SM8:
REGISTER(Integrity-Protection = *Successful,* IMPI*)*

The P-CSCF finally sends SM12 to the UE. SM12 does not contain information specific to security mode set-up (i.e. a Security-setup-line), but with sending SM12 not indicating an error the P-CSCF confirms that security mode set-up has been successful. After receiving SM12 not indicating an error, the UE can assume the successful completion of the security-mode setup.