3GPP TSG-SA3 Meeting #24 **_S3-~~020382~~020411_**
Helsinki, Finland, Date

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:	⌘	Mitigating reflection attacks in IMS		
Source:	⌘	Nokia and Ericsson		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	2002-07-05
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:	⌘	The IPsec SPI is currently specified in TS33.203 to ~~includes~~ include a ‘direction bit’ in order to allow~~secure~~ the use of one integrity key for both directions. However, this solution puts non-necessary restriction on ~~de facto standard~~ implementations of IPsec. In particular, compatibility of the use of IPSEC including IKE would be restricted. One example is that the P-CSCF will handle SPIs differently in IMS towards the UE being compliant with the direction bit requirement in TS33.203 and towards other network nodes being compliant with NDS/IP i.e. TS 33.210.~~. This is not desirable especially because the potential security problem that this solution solves is extremely rare. The prerequisite for the problem are: 1) the SPI values happens to be the same, 2) an active attacker reflects IPsec packets from one direction to another, 3) the anti-replay protection window at IPsec layer accepts the reflected package.~~ The same ~~amount of security~~functionality with ~~less modification~~better compatibility to the ~~implementations~~ IPSec use with IKE can be achieved by adding a rule to P-CSCF to check that the SPI values are not the same when the SIP Security Agreement is done.
Summary of change:	⌘	Two changes have been done: 1) The ‘direction bit’ from IPsec SPI has been removed. 2) A rule for P-CSCF to check that the SPI values are not the same when the same key is used for both directions has been added.
Consequences if not approved:	⌘	~~Unnecessary increased complexity to implement the direction bit requirement in existing IPSec implementations.~~It is required to implement different behaviour in the P-CSCF for IPSec towards UE compared with IPSec towards other network elements. Also the UE may be impacted in a similar fashion. The SPI will no longer have only local significance which is breaking the definition of the SPI in RFC 2401.

Clauses affected:	⌘	7.1 and 7.2

Other specs affected:	⌘	X	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.

7.1 Security association parameters

For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys that are provided by IMS AKA, and a set of parameters specific to a protection method. The security mode setup (cf. clause 7.2) is used to negotiate the SA parameters required for IPsec ESP with authentication, but without confidentiality.

The SA parameters that shall be negotiated between UE and P-CSCF in the security mode set-up procedure, are:

- **Integrity algorithm**

NOTE 1: What is called "authentication algorithm" in [13] is called "integrity algorithm" in this specification in order to be in line with the terminology used in other 3GPP specifications and, in particular, to avoid confusion with the authentication algorithms used in the AKA protocol.

The integrity algorithm is either HMAC-MD5-96 [15] or HMAC-SHA-1-96 [16].

NOTE 2: This, in particular, excludes the use of the NULL integrity algorithm.

Both integrity algorithms shall be supported by both, the UE and the P-CSCF as mandated by [13]. In the unlikely event that one of the integrity algorithm is compromised during the lifetime of this specification, this algorithm shall no longer be supported.

NOTE 3: If only one of the two integrity algorithms is compromised then it suffices for the IMS to remain secure that the algorithm is no longer supported by any P-CSCF. The security mode set-up procedure (cf. clause 7.2) will then ensure that the other integrity algorithm is selected.

- **SPI (Security Parameter Index)**

The SPI is allocated locally for inbound SAs. The triple (SPI, destination IP address, security protocol) uniquely identifies an SA at the IP layer. The UE shall select the SPIs uniquely, and different from any SPIs that might be used in any existing SAs (i.e. inbound and outbound SAs). The SPIs selected by the P-CSCF shall be different than the SPIs sent by the UE, cf. section 7.2.~~The most significant bit of any SPI allocated by the P-CSCF shall be "0" and the most significant bit of any SPI allocated by the UE shall be "1".~~

NOTE 4: This allocation of SPIs ensures that protected messages in the uplink always differ from protected messages in the downlink in, at least, the SPI field. This thwarts reflection attacks. When several applications use IPsec on the same physical interface the SIP application should be allocated a separate range of SPIs.

The following SA parameters are not negotiated:

- Life type: the life type is always seconds;
- SA duration: the SA duration has a fixed length of 2^{32}-1;

NOTE 5: The SA duration is a network layer concept. From a practical point of view, the value chosen for "SA duration" does not impose any limit on the lifetime of an SA at the network layer. The SA lifetime is controlled by the SIP application as specified in clause 7.4.

- Mode: transport mode;
- Key length: the length of the integrity key IK_{ESP} depends on the integrity algorithm. It is 128 bits for HMAC-MD5-96 and 160 bits for HMAC-SHA-1-96.

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. source and destination IP addresses, transport protocol, and source and destination ports.

- IP addresses are bound to a pair of SAs, as in clause 6.3, as follows:

- inbound SA at the P-CSCF:
  The source and destination IP addresses associated with the SA are identical to those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

- outbound SA at the P-CSCF:
  the source IP address bound to the outbound SA equals the destination IP address bound to the inbound SA; the destination IP address bound to the outbound SA equals the source IP address bound to the inbound SA.

NOTE 6: This implies that the source and destination IP addresses in the header of the IP packet in which the protected SIP REGISTER message was received by the P-CSCF need to be the same as those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

- The transport protocol is either TCP or UDP.

- Ports:

1. The P-CSCF receives messages protected with ESP from any UE on one fixed port (the"protected port") different from the standard SIP port 5060. The number of the protected port is communicated to the UE during the security mode set-up procedure, cf. clause 7.2. No unprotected messages shall be sent to or received on this port. From a security point of view, the P-CSCF may receive unprotected messages from any UE on any port which is different from the protected port.

NOTE 7: The protected port is fixed for a particular P-CSCF, but may be different for different P-CSCFs.

2. For protected or unprotected outbound messages from the P-CSCF (inbound for the UE) any port number may be used at the P-CSCF from a security point of view.

3. For each security association, the UE assigns a port to send or receive protected messages to and from the P-CSCF ("protected port"). No unprotected messages shall be sent to or received on this port. The UE may use different protected port numbers for TCP and UDP. The numbers of these ports are communicated to the P-CSCF during the security mode set-up procedure, cf. clause 7.2. From a security point of view, the UE may send or receive unprotected messages to or from the P-CSCF on any ports which are not protected ports.

Editor’s note: The condition that the UE sends and receives protected messages on the same port is not necessary from a security point of view. These ports could be made different, at the expense of one more parameter to be negotiated in the security mode set-up procedure, but they have to be fixed in the registration procedure.

4. The P-CSCF is allowed to receive only REGISTER messages on unprotected ports. All other messages not arriving on the protected port shall be discarded by the P-CSCF.

5. The UE is allowed to receive only the following messages on an unprotected port:

   - responses to unprotected REGISTER messages;

   - error messages.

   All other messages not arriving on a protected port shall be discarded by the UE.

The following rules apply:

1. For each SA which has been established and has not expired, the SIP application at the P-CSCF stores at least the following data: (UE_IP_address, UE_protected_port, transport protocol, SPI, IMPI, IMPU1, ... , IMPUn, lifetime) in an "SA_table".

NOTE 8: The SPI is only required when initiating and deleting SAs in the P-CSCF. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

2. The SIP application at the P-CSCF shall check upon receipt of a protected REGISTER message that the source IP address in the packet header coincides with the UE’s IP address given in the contact header of the protected REGISTER message. If the contact header does not explicitly contain the UE’s IP address, but rather a symbolic name then the P-CSCF shall first resolve the symbolic name by suitable means to obtain an IP address.

3. The SIP application at the P-CSCF shall check upon receipt of an initial REGISTER message that, for each transport protocol, the triple (UE_IP_address, UE_protected_port, transport protocol), where the UE_IP_address is the source IP address in the packet header and the protected port is sent as part of the security mode set-up

procedure (cf. clause 7.2), has not yet been associated with entries in the "SA_table". Furthermore, the P-CSCF shall check that, for any one IMPI, no more than three SAs per direction and per transport protocol are stored at any one time. If these checks are unsuccessful the registration is aborted and a suitable error message is sent to the UE.

NOTE 9: According to clause 7.4 on SA handling, at most three SAs per direction and per transport protocol need to exist at a P-CSCF for one user at any one time.

4. For each incoming protected message the SIP application at the P-CSCF shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the triple (UE_IP_address, UE_protected_port, transport protocol) in the "SA_table". The SIP application at the P-CSCF shall further check that the IMPU associated with the SA in the "SA_table" and the IMPU in the received SIP message coincide. If this is not the case the message shall be discarded.

5. For each SA which has been established and has not expired, the SIP application at the UE stores at least the following data: (UE_protected_port, transport protocol, SPI, lifetime) in an "SA_table".

NOTE 10: The SPI is only required to initiate and delete SAs in the UE. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

6. When establishing two new pairs of SAs (cf. clause 6.3) the SIP application at the UE shall ensure that, for each transport protocol, the selected number for the protected port does not correspond to an entry in the "SA_table".

NOTE 11: Regarding the selection of the number of the protected port at the UE it is generally recommended that the UE randomly selects the number of the protected port from a sufficiently large set of numbers not yet allocated at the UE. This is to thwart a limited form of a Denial of Service attack. UMTS PS access link security also helps to thwart this attack.

7. For each incoming protected message the SIP application at the UE shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the pair (UE_protected_port, transport protocol) in the "SA table".

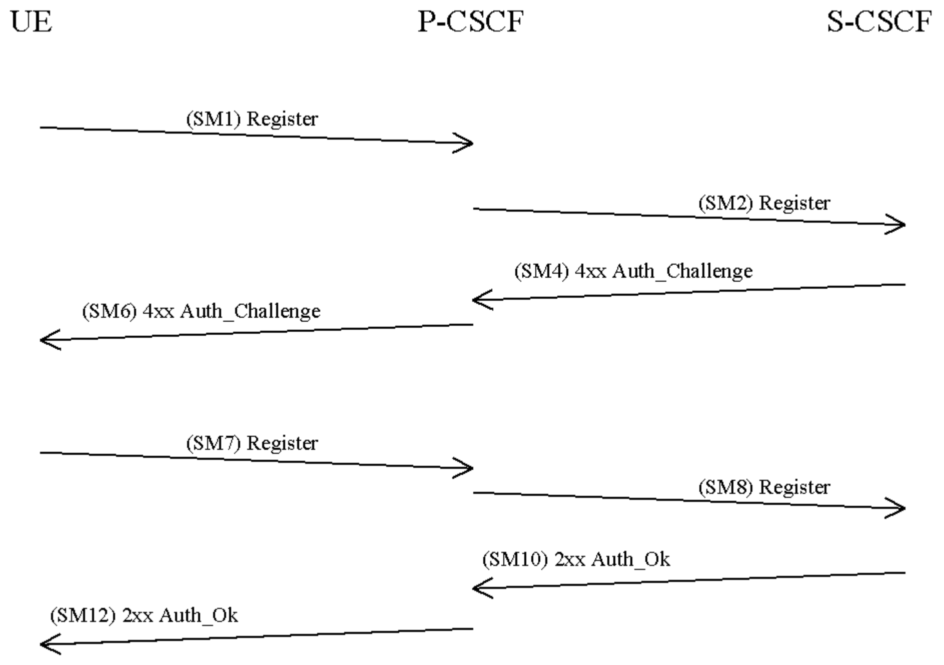
NOTE 12: If the integrity check of a received packet fails then IPsec will automatically discard the packet.

8. The lifetime of an SA at the application layer between the UE and the P-CSCF shall equal the registration period.

7.2 Set-up of security associations (successful case)

The set-up of security associations is based on [draft-IETF-sip-sec-agree]. Annex H 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. clause 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. The P-CSCF shall define the SPIs such that they are unique and different from any SPIs as received in the *Security-setup-line* from the UE. Note that this rule is needed since the UE and the P-CSCF use the same key for inbound and outbound traffic.

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.

SM6:
4xx Auth_Challenge(Security-setup = *SPI_P_TCP, SPI_P_UDP, Port_P*, *P-CSCF integrity algorithms list)*

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 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 setup (i.e. a Security-setup line), but with sending SM12 not indicating an error the P-CSCF confirms that security mode setup has been successful. After receiving SM12 not indicating an error, the UE can assume the successful completion of the security-mode setup.