3GPP TSG-SA3 Meeting #24 ***Tdoc S3-020418***
Helsinki, Finland 9-12 July 2002

Title: Bye and Response attacks in IMS
Source: SA3
To: CN1
Cc: -

Contact Person:
Name: Krister Boman
Tel. Number: +46 313446055
E-mail Address: krister.boman@erv.ericsson.se

Attachments: S3-020381

---

1. Overall Description:

SA3 has discussed two new potential attacks:

1. An attacker can send responses to INVITEs intended for other entities. This attack is possible if an attacker already has an SA with the P-CSCF. The attacker eavesdrops the channel and takes the required information from e.g. a SIP INVITE and creates a response and sends it through the SA of the attacker. This attack has to be performed in 'real time'.
2. Another more severe attack is that an attacker can send requests at any time to other people dialogs such as a BYE request, which does not have to be performed in real time.

The attached CR aims to update the requirement such that the P-CSCF verifies that the message received from a genuine user is tied to a dialog in which the sender is involved. This CR was tentatively approved at SA3#24 given that CN1 cannot identify any other better solution.

SA3 also discussed a similar attack "Identity Spoofing in IMS" which was solved by CN1 in S3-020029 (=N1-020155) that seemed to solve the attack described above. However it seems that the problem with e.g. BYE is that it may contain only dialog ID but not the IMPU, according to SIP. If that is correct then one potential solution is to verify the dialog ID against an SA.

SA3 also would like to note that if this new requirement is necessary that it would impose increased complexity in the P-CSCF.

2. Actions To CN1:

CN1 is kindly asked to identify if a solution to the above mentioned attacks are already implemented in the CN1 specifications. If CN1 cannot confirm that a solution already exists SA3 would like CN1 to identify if the proposed solution by SA3 is the optimal solution or not.

3. Date of Next CN1 Meetings:

SA3_25	October 8-11 2002	Munich, Germany
SA3_26	November 19-22 2002	ETSI, Sophia Antipolis (Tentative)

3GPP TSG-SA3 Meeting #24 ***S3-020381***
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 **X**

Title:	⌘	Attacker sends responses to requests intended for other parties
Source:	⌘	Ericsson, Nokia
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:	⌘	According to the current requirements in TS33.203 an attacker can send responses to INVITEs intended for other entitites. This attack is possible if an attacker has already an SA with the P-CSCF. The attacker eavesdrop the channel and takes the required information from e.g. a SIP INVITE and creates a response and sends it through the SA of the attacker. This is not acceptable from a security point of view. Another more severe attack is that an attacker can send requests at any time to other people dialog such as a BYE request which does not have to be performed in real time.
Summary of change:	⌘	Update the requirement such that the P-CSCF verifies that the message received from a genuine user is tied to a dialog in which the sender is involved.
Consequences if not approved:	⌘	Necessary requirements are missing.

Clauses affected:	⌘	7.1		
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 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. ~~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". Once the UE gets involved in dialogs, the dialog IDs need to be associated with the SA as well.

NOTE 8: The "SA_table" represents only a logical term showing that SIP application maintains the association between the- inbound SA from the UE and other UE's parameters.

NOTE ~~8~~9: 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~~10: 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. This verification shall be performed for both SIP Requests and Responses and in particular the P-CSCF shall verify that the messages are sent ~~over~~on a dialog in which the sender is involved. 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 in the received SIP message coincides with ~~the~~ any IMPU associated with the SA in the "SA_table" ~~and the IMPU in the received SIP message coincide~~. The SIP application at the P-CSCF shall further check that the Dialog ID in the received SIP message coincides with any Dialog ID associated with the SA in the "SA_table". If ~~this is not the case~~either checking fails 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~~11: 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~~12: 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~~13: 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.