3GPP TSG SA WG3 Security — S3#22 **S3-020108**

25 - 28 February 2002

Bristol, UK

Source: **Nokia**

Title: **Uniqueness of IP address/port number checking in the P-CSCF**

Document for: **Discussion and decision**

Agenda Item: **7.3, IP Multimedia Subnetwork (IMS)**

1. Scope and objectives

TS 33.203 keeps IPsec solution during SA set-up procedure in Annex D. The scope of this document is to analyse concerns related to UE's source IP address and port number.

The analysis draws the conclusion that during the registration to IMS, the P-CSCF shall check whether the IP address of the UE is already bound to some one registered before hand. Additionally, the P-CSCF shall check whether the IP address in IP header equals to the one stored in Contact header of SIP REGISTER. For further releases, the IP address uniqueness may be expanded to that of an IP address and port number pair. A CR to TS 33.203 is provided to reflect the concern.

2. Discussion

2.1 Attack description

An attacker takes first step. He finds out of a victim's source IP address. Then he tries to register to the IMS with the same IP address but with his own identities (i.e. IMPI and IMPU). Suppose the attacker is a valid subscriber of IMS, he can negotiate a SA based on his own IMPI. This leads to a situation, where two registered IMPIs have the same source IP address (Also the associated port numbers can be equal.).

In future release when other access technologies to the IMS than 3G/GPRS are deployed, this attack scenario is rather permitted, because the address allocation is out of 3G/GPRS network control.

Now IPsec is for the first hop integrity protection, the attacker has a possibility to abuse the victim. As the second step, he sends an INVITE message with target's IMPU. In P-CSCF, integrity checking is passed without problem, next, the SIP level queries the source IP address of that INVITE from the IP level. Because the same IP address is bound to both identities, P-CSCF can not detect the identity is spoofed.

The same problem does not exist for SIP level integrity solution. P-CSCF firstly finds out the associated SA for that IMPU, then use the corresponding key to check the message integrity. If the attacker using somebody else's IMPU, he can not pass the integrity checking with his own key. Or, suppose P-CSCF does not get all implicit IMPUs, it would find corresponding key with uniqueness of SA_ID, insert the corresponding IMPI to SIP message and forward it to the S-CSCF. S-CSCF can verify whether that IMPI/IMPU association is valid.

Current working assumption is to send all implicitly registered IMPUs to P-CSCF and detect Identity Spoofing in the P-CSCF [S3z010673, S3z020041].

2.2 *Prevention of the attack in IPsec level*

The attack can be prevented, if during every registration the P-CSCF checks the IP address does not repeat with any other IMS subscribers successfully registered before hand. This is not a problem if attacker succeeds to register via another P-CSCF with victim's source IP address, since the second P-CSCF has no record of victim to mix them up. Any methods described in [S3z010673] will prevent the identity spoofing attack.

Furthermore, we need to ensure that the source IP address is correctly recorded in Security Policy Database (SPD) during registration. In IPsec ESP, MAC does not cover source IP address, but the data payload, so P-CSCF must check that the source IP address in IP header equals to the one in Contact header of SIP message (SM1 and SM7, see Figure 3 in [33.203 v1.0.0]), after integrity is sucessfully checked. The Contact header is in data payload of ESP, so it is integrity protected.

2.3 *Future aspect*

In the future there might be a situation, where several "well behaving" IMPIs use the same source address. In this case IMPIs must be separated using different port numbers. If IPsec is used between the UEs and P-CSCF, the identities of all UEs must be bound to the selector pair , namely, source IP address and source port number, to prevent identity spoofing attack.

3. IP address allocation

The RFC3041 specifies IPv6 dynamic address usage. The terminal shall be assigned a fixed network-prefix in address space, usually the first 64 bits. And the terminal freely concatenates any host suffix to the network prefix, and uses the concatenation as tempory IP address. Since every MS shall be assigned an unique network prefix, P-CSCF can still route properly. We see that this kind of IPv6 address allocation does not conflict with IPsec usage. For inbound traffic processing in P-CSCF, the SPD records the agreed network prefix as selector, and associates the corresponding SA to the prefix rather than to the whole address.

This is in line with [RFC2401].

The deployment detail of dynamic IPv6 address is yet unstable in 3GPP at the moment. We propose not to reflect the latest developments in TS 33.203 until it is confirmed.

4. Conclusions

Based on the analysis, it is concluded that for IPsec solution, the P-CSCF must guarantee the uniqueness of IP address of each subscriber. For future releases it is the uniqueness of source IP address and source port number. Put it into pieces,

- for every REGISTER message the P-CSCF must check the source IP address is not used by any other registered subscriber (or the same source IP address prefix).
- the P-CSCF must make sure that the same source IP address in IP/UDP datagram equals to the one in Contact header of REGISTER message.

5. References

[33.203 v1.0.0]	TS 33.203,
[RFC2401]	Security Architecture for the Internet Protocol.
[S3-010673]	Prevention of identity spoofing in the IMS (S3#21)
[S3z020041]	Registrations without user authentication and Identity Spoofing (S3#21bis)

CR-Form-v4

CHANGE REQUEST

⌘ **33.203 CR** ⌘ ev **1** ⌘ Current version: **1.0.0** ⌘

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:	⌘	IPsec selector bundle checking when registering to IMS		
Source:	⌘	Nokia		
Work item code:	⌘	IMS	***Date:*** ⌘	19 February 2002
Category:	⌘	**F**	***Release:*** ⌘	R5

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 to provide integrity protection defined in 33.203 does not mandate P-CSCF to verify that user provided selector pair is unique, namely IP address and port number. This is essential to IPsec solution, that every entry in SPD should not overlap by same selectors. This CR addresses the verification complement in Annex D.1 "Security Association Parameters". The principle is well known and specified in RFC2401.
Summary of change:	⌘	The user IP address and UE specified port number should be checked to be unique in P-CSCF when UE registering to IMS.
Consequences if not approved:	⌘	Skip verification of selector pair will permit User ID spoofing attack.

Clauses affected:	⌘	Annex D.1
Other specs affected:	⌘	□ Other core specifications ⌘ □ Test specifications □ O&M Specifications
Other comments:	⌘	IPv6 address allocation should not affect to 33.203, until the mechanism is stable in 3GPP.

-- START of CR---

Annex D (Informative): Set-up procedures for IPSec based solution

[Editors Note: If the IPSec solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

This chapter is based on chapter 7 and provides additional specification for the support of IPsec ESP.

D.1 *Security association parameters*

The SA parameters, identifiers and attributes that shall be negotiated between UE and P-CSCF, are:

- - ESP transform identifier
- - Authentication (integrity) algorithm
- - SPI

Further parameters:

- - Life type: the life type is always seconds
- - SA duration: the SA duration has a fixed length of 2^{32}-1.
- - Key length: the length of encryption and authentication (integrity) keys is 128 bits.

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. IP addresses and ports. Both sides have to use the same policy here, but since the required selectors will be known from the SIP messages, there is no need to negotiate them. However, it is critical to keep the source IP address and source port number, the selector pair unique in P-CSCF. The P-CSCF must reject any REGISTER message sent from a valid SA's selector pair yet bear a different user ID than the previously registered one. Furthermore, the P-CSCF must check if source IP address/source port number of the inbound IP datagram equals to that in Contact header of every SIP REGISTER. The only parameter that shall be negotiated, is a fixed port for specific unprotected SIP messages at the P-CSCF:

- 1. For the inbound SA at the P-CSCF (outbound for the UE) the P-CSCF shall use a fixed port. This may be port 5060 as the standard SIP port, or any other fixed port where the server accepts SIP messages from the UE. In addition, another port for specific unprotected SIP messages from the UE to the server is fixed.
  For the outbound SA at the P-CSCF (inbound for the UE) ANY port number shall be allowed at the P-CSCF.
- 2. On the UE side, the SIP UAs shall use the same port for both sending and receiving SIP signalling to the P-CSCF.
- 3. If there are multiple SIP UAs belonging to different ISIMs in one UE they shall use different SAs and bind them to different ports on the UE side.
- 4. The UE may send only the following messages to the fixed port for unprotected messages:
  - - initial REGISTER message
  - - REGISTER message with network authentication failure indication
  - - REGISTER message with synchronization failure indication

All other messages incoming on this port must be discarded by the SIP application on the P-CSCF.

[Note: It is ffs whether case 3 can actually occur.]

For each incoming message the SIP application must verify that the correct inbound SA associated with the public ID (IMPU) given in the SIP message has been used. This shall be done by verifying that the correct source IP address and source port bound to the public ID (IMPU) of the SIP message have been used for sending the message.

D.2 Security mode setup for IPsec ESP

This section describes how the security mode setup described in chapter 7 shall be used for negotiating ESP as protection mechanism and setting up the parameters required by ESP.

D.2.1 General procedures specific to the ESP protection mechanism

The integrity and encryption mechanisms both have the value "esp". The fields SA_ID_U and SA_ID_P carry the SPI values to be exchanged, to identify the ESP SAs.

The P-CSCF shall use an unprotected port to be able to receive specific unprotected messages. This unprotected port has to be communicated to the UE, by using the *info* field of message SM4. This unprotected port is required, when an IPsec SA is already in place at the P-CSCF, but the UE due to any reason is not able to use this SA. In this case, the UE shall send error messages or a new REGISTER message in the clear to the P-CSCF port received in the *info* field within SM4. Otherwise at the P-CSCF side, ESP would simply drop all IP packets from the UE that fail the integrity check.

The error messages that shall be sent in the clear from the UE to the P-CSCF are these for network authentication failures (sections 7.3.1.2) and synchronization failures (section 7.3.1.3).

D.2.2 Handling of user authentication failure

(This extends the content of chapter 7.3.1.1 and 7.3.3.3 for IPsec ESP)

In the case of a user authentication failure, the user will usually not be able to use a security association with the correct key material. Therefore, when using ESP for integrity protection and encryption, this will cause SM5 to be dropped at the P-CSCF IP(sec) layer due to a failed integrity check within ESP processing.

As SM5 will not reach the P-CSCF IMS application, the P-CSCF shall implement a timer for the authentication process. When a message is received that passes the integrity-check and successfully completes the authentication, it is immediately processed. However, if during the registration timer the P-CSCF receives packets that cannot be verified, it discards them. At the end of the registration timer, it reports an authentication failure back to the home network.

D.2.3 Authenticated re-registration procedures specific to the ESP protection mechanism

The new security associations SA11 and SA12 shall be bound to a new port on the UE side. This new port shall be communicated by the UE in the *info* field of the first REGISTER message SM1.