TypeUnitOrDepartmentHere
TypeYourNameHere TypeDateHere

3GPP TSG SA WG3 Security — S3#24 **S3-020375**

9 - 12 July, 2002

Helsinki, Finland

Source: **Nokia**

Title: **Transport layer address in Via header**

Agenda item: **7.1, IMS**

Document for: **DISCUSSION/APPROVAL**

Abstract

This paper corrects a misuse of SIP header, for discovering UE's IP address so as to establish Security Association (SA) properly. It is suggested to use the information in Via header instead of the Contact header according to the SIP grammar.

1. INTRODUCTION

The IP address of UE is used to establish SA in P-CSCF. A potential threat is that source IP address in IP header is not authenticated by MAC therefore apt to be modified by malicious attacker. A couple of contributions have been proposed earlier by Nokia [S3-020108] and Siemens [S3-020234] to tackle on the problem. However the solution based on Contact header in SIP message bears flaw clearly, for it is a misuse of Contact header.

Based on SIP grammar, it is proposed in this paper to utilize the 'sent-by' field in Via header for acquiring UE's proper IP address. The attached CR reflecting the changes against TS 33.203 v 5.2.0, is proposed to be endorsed by this meeting.

2. ANALYSIS

When the UAC creates a request such as REGISTER, it MUST insert a Via header into that request. [IETF_SIP] states, "The Via header indicates the *transport* path taken by the request and indicates the path that should be followed in routing responses." It means the client's host name or network address, and possibly the port number at which it wishes to receive responses, are inserted, precisely in the 'sent-by' field of the Via header.

In contrast, the Contact header provides a SIP or SIPS URI at which the UA would like to receive *subsequent* requests, i.e. at which user can be contacted. That address may contain the address of any other device than the UE's, because the person wishes to be reached only by that address in Contact header. So it is seen an impropriate means looking for UE's IP address from the Contact address.

3. PROPOSAL

The SIP grammar tells that using Contact header is impropriate to obtain UE's IP address. Instead the sent-by in Via header contains either direct an IP address or a symbolic name of UE that may be resolved to establish SA. It's suggested to apply the latter one in TS 33.203.

4. REFERENCE

[IETF_SIP] J. Rosenberg et al., SIP. RFC 3261, IETF. June 2002.
[S3-020108] Nokia, Uniqueness of IP address/port number checking in the P-CSCF. S3#22.
[S3-020234] Siemens, Justification for proposed changes to text on SIP integrity in TS 33.203 v510. S3#23.

TypeUnitOrDepartmentHere
TypeYourNameHere TypeDateHere

(CR attached)

TypeUnitOrDepartmentHere
TypeYourNameHere TypeDateHere

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: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Correction of IP address acquisition in P-CSCF
Source:	⌘	Nokia
Work item code:	⌘	IMS-ASEC
Date:	⌘	4 July 2002
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)*
Rel-6	*(Release 6)*

Reason for change:	⌘	It is improper to utilize Contact header according to SIP grammar. The contact address is used for terminated call delivery and may contain the address of any device other than the UE's.
Summary of change:	⌘	The Via header, in particular the 'sent-by' field in Via header should be used to obtain the information.
Consequences if not approved:	⌘	The P-CSCF may not get the proper IP address of UE.

Clauses affected:	⌘	7.1
Other specs affected:	⌘	Y / X: TS 24.228, 24.229 ⌘
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.

TypeUnitOrDepartmentHere
TypeYourNameHere TypeDateHere

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

**********omitted**********

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~~ inserted in the ~~contact~~ Via header of the protected REGISTER message. If the ~~contact~~ Via 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.

**********omitted**********