Source: Nokia

Title: Trustworthiness of the next hop (IMS?) network

Document for: Discussion

Agenda Item: 5.4

WI / Topic: IMS-ASEC

Release: Rel-5

1. Introduction

There were discussions about privacy handling in the last CN1 meeting. The only privacy option adopted in Rel-5 by CN1 is the identity privacy. This privacy option allows the calling party to ask the network to remove the P-Asserted-Identity from the request/response. According to RFC 3325, the P-Asserted-Identity header must be removed by the last hop in the trusted network. But for this to be possible, each CSCF must know whether the next hop CSCF is trusted (i.e. it is part of IMS) or not. So it is problematic to define which CSCF shall implement the procedures for the header removal in CN1.

2. Possible solutions

Nokia identified the following solutions for this problem:

1. keep a database at the S-CSCF of the home network, and list there all the known IMS network domain names and IP addresses the home network trusts.

This solution is painful, as a database containing the domain name of the IMS networks and the corresponding IP addresses of the I-CSCFs has to be maintained in a SIP level database.

As SIP requests may contain either domain names or IP addresses in the Request-URI, it is not enough to store the domain names into the database. It is however possible, to make reverse DNS queries whenever an IP address is received instead of a domain name in the R-URI. Thus, the following simplified solution is also possible:

- Keep a database with the domain names of the IMS networks the home network trusts
- If a request with an IP address in R-URI is received, then make reverse DNS query and find out the corresponding domain
- If the domain is in the database, then consider the next hop a trusted domain and apply the corresponding procedures
- If the domain is not in the database, then consider the next hop an untrusted domain, and apply the corresponding procedures

2. keep only a database at the S-CSCF of the home network, and list there all the known IMS network domain names the home network trusts.

If the R-URI contains an IP address instead of a domain name (and thus can not be checked in the database), then simply assume that the next hop is an untrusted domain.

3. Configure the NDS in the security gateways (SPD) in such a way, that an IP packet coming from a CSCF of the domain the gateway is part of, would be sent over a secure connection. If a secure connection towards the destination does not exists, the packet is simply discarded and an ICMP message generated. Thus, the home network always

assumes the next hop is trusted and does not remove the P-Asserted-Identity. If it happens that the next hop is not trusted, then the packet is anyhow discarded, and does not reach the called party.

The consequence of this solution is, that CSCF will only be able to communicate with SIP entities belonging to a trusted domain. But this is actually the aim of Rel-5.

3. Proposal

Nokia proposes alternative 3 to be adopted by 3GPP and standardised by SA3.