3GPP TSG SA WG3 Security — S3#21 **S3-010636**

27 - 30 November, 2001

Sophia Antipolis, France

Source: Siemens

Title: SIP application required to check IP address

Document for: Discussion / Decision

Agenda item: IMS security

Abstract

This contribution proposes to add some text to the IPsec-specific Annex of 33.203 v0.7.0 regarding the processing of incoming messages. The rule specified in this text is important because a failure to take it into account may result in a security gap. The rule states that the SIP applications in both the P-CSCF and the UE have to verify that for an incoming SIP message the correct security association (the one bound to the public ID in the SIP message) has been used. As it is assumed to be difficult for the application to access the SPI that was used by IPsec processing the source IP address and source port that were used to transmit the message shall be checked.

The affected section of annex D of TS 33.203, v0.7.0 is given below, the changes are added as revision marks.

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 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. The only parameter that shall be negotiated, is a 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.