

IMS R5 profile of RFC 3329

Vesa Torvinen
Ericsson Research
Finland

Background

- RFC 3329 was developed for IMS in order to enable secure development of security mechanisms
- Mitigation of bidding down attack was one of the main requirements
 - E.g. the attacker should not be able to shut the encryption down
- No real use cases for “normal” IETF SIP
 - TLS is “negotiated” via DNS – or just used in the well-known port

Summary of recent changes

- Changes in parameters
 - Motivation: SA handling has been changed
 - One new parameter (spi)
 - Change of the semantics for three parameters (spi and ports)
- Changes in procedure
 - Motivation: had to solve the man-in-the-middle problem caused by the changes in parameters
 - “3gpp-ipsec” mechanism has been extended to repeat the client side parameters in the protected message

Changes in parameters

- Spi-c: Defines the SPI number of the inbound SA at the protected client port.
- Spi-s: Defines the SPI number of the inbound SA at the protected server port.
- Port-c: Defines the protected client port.
- Port-s: Defines the protected server port.

Changes in procedure; motivation

- Because the UDP and TCP will use different port numbers, need to mitigate the related man-in-the-middle attack
- MitM attack:
 - REGISTER message is sent using UDP
 - MitM modifies TCP parameters in Security-Client header
 - IPsec will reject all TCP messages; UDP will work

Changes in procedure; agreed solution

- A new procedure for “3GPP-ipsec” mechanism to repeat the Security-Client header in the protected REGISTER message
 - Competing solution used contiguous port and spi values
- No influence to other security mechanisms in RFC 3329
 - If you end-up using TLS or Digest, you don’t need to repeat the Security-Client header
- Modification of IPsec parameters is noticed during registration