3GPP TSG SA WG3 Security **S3-020387**

9th – 12th July, 2002

Helsinki, Finland

Agenda Item:	TBD
Source:	Ericsson
Title:	MitM attack for TCP Security Association negotiation
Document for:	Discussion/Decision

1. Introduction

This paper documents an attack for Security Association (SA) negotiation between UA and P-CSCF. More specifically, it is possible for a MitM to forge the SA parameters needed for P-CSCF to send messages to UA using TCP. The attack is possible due to the fact that different SAs are required for TCP and UDP together with the design of SIP Security Agreement.

A CR from Ericsson aims to update TS33.203 such that this attack is alleviated.

2. Attack description

The current working assumption in SA3 about SA negotiation is as follows:

- The negotiation will use UDP.
- SAs needed for TCP are also negotiated at the same time as the SAs needed for UDP.
- The negotiation will use SIP Security Agreement procedure in which the Security-Client and Security-Server headers are sent unprotected, and Security-Verify header is sent protected.

There is a possible attack in which the SA negotiated for messages from P-CSCF to UA using TCP will not work. The attack is as follows:

- UA sends the first unprotected REGISTER message with Security-Client header. This header includes SPIs for UDP and TCP.
- An attacker modifies the SPI value related to TCP in the Security-Client header.
- P-CSCF will open an outbound SA for TCP using the wrong SPI value.
- UA will send the inbound SA for TCP using the correct SPI value.

IPsec in UA will discard all the messages from P-CSCF to UA using TCP.

3 Analysing the attack

This attack is possible since different SAs are required for TCP and UDP. If the same SA could be used the attack would no longer be possible. Secondly the attack is also made possible due to the design of the SIP security agreement procedure. This procedure relies in part on the use of the negotiated SAs as a means to assure that the negotiation has succeeded:

- The server's parameters have to be repeated over the SA to ensure that they have not been modified. (This is sufficient to ensure the right selection between mechanisms has been made, since the client knows its own list, and the servers list is secured in this manner.)
- Any modification of the servers list may in some cases result in a situation where the established SAs do not matche, i.e. a Denial-Of-Service attack is created.
- Any modification of the clients list may also result in a situation where the established SAs do not match

The above works well when the Denial-Of-Service attacks can be immediately detected. In the simple case of a single transport protocol this is ensured as the servers list modification is detected by either the inability to communicate or by the differences in the servers list. The clients list modification is detected by the inability to communicate. Since the UE is performing the registration procedure it will notice that it has not received an answer.

However when there are two transport protocols, we may find out the problem with the other transport protocol much later e.g. at the time we make an INVITE which is too large to fit comfortably to a single packet. So the real problem with the attack is not that it can happen but rather that we cannot detect it early enough.

The attack affects only some parameters in the negotiation as follows:

- Those parameters that are always shared between the UDP and TCP SAs will not be affected, because they will be tested immediately with the UDP SAs. These parameters include all the algorithm and protocol parameters and the base for the keys for the SAs.
- Those parameters that necessarily have to be different between UDP and TCP. The SPI values have to be different as otherwise there would be a single SA for both protocols. This is not possible as typical SPD entries and selectors only allow a specific protocol not a list of protocols
- Those parameters that we might arrange to be the same between TCP and UDP but which may be implementation wise hard. Port numbers belong to this category

In conclusion the problem affects only the SPI and port number parameters.

4. Known solutions

There are at least two known solutions to the problem:

1. Including the TCP SPI and port number from the client to the Security-Server header can solve the problem. In this case, the UA must check that the TCP SPI and port number in the Security-Server header is the same as sent by itself. Otherwise, the UA must abort the registration. The advantage with this solution is that it represents a fairly small modification to the current technical specification. Note that the UE will in SM7 repeat the values as it received in SM6 from the P-CSCF according to the sip security agreement draft.
2. Another solution is that the SIP Security Agreement mechanism is only used to negotiate the SAs for the transport protocol currently used. In other words, if UDP is used, SIP Security Agreement will only cover SAs for UDP. The SAs for TCP can be negotiated later, for example, when there is a need to use TCP. SIP Security Agreement mechanism is not limited to REGISTER messages, and if UA and P-CSCF have a local policy that Security Agreement must always be used, they will be able to negotiate security later. For example, the first terminating INVITE, which is sent from P-CSCF to UA unprotected using TCP, could initiate the security agreement. This would require, however, that the UA must take the role of the server in SIP Security Agreement. The advantage with this solution is that it would eliminate the complexity from the security mode setup procedure by having it negotiate only a single set of SAs. On the other hand, it is not clear if another authenticatin is needed for the second security mode set-up run.

4. Conclusions

MitM is able to modify the SA parameters sent by the UA to P-CSCF. If MitM will only modify parameters related to TCP, the attack will be noticed only when TCP is used at the first time. The reason for this attack is that the negotiation is done using UDP, and SAs related to TCP are not tested during the registration.

Ericsson proposes that SA3 adopts solution 1 mainly since this solution will have the least impact on the current security framework and reduces the work effort to solve the attack.