3GPP TSG SA WG3 Security S3-010071

Meeting S3#17

Göteborg, 27 Feb – 2 Mar, 2001

Source: Siemens AG

Title: An analysis of 3G TS 23.228 v170 “IP Multimedia (IM) Subsystem - Stage 2” from a security point of view.

Document for: Discussion / Decision

Work item: Access security for IP-based services

Agenda item: tbd

Abstract

Two alternative proposals for an IM domain security architecture were presented at S3#16 by Ericsson in TD S3-000699 and by Siemens in TDs S3-000689 and S3-000753. A well-founded decision between these proposals must be based on a security analysis of the system to be secured. This system is described in TS 23.228. This contribution concludes that the integrity function should be located in the Proxy CSCF for security reasons. In addition, the contribution identifies the need to protect certain interfaces in the IM network subsystem.

1 Introduction

Any decision on security features and mechanisms and their allocation to network entities should be based on security requirements resulting from an analysis for the system to be secured. In our case, this system is described in 3G TS 23.228 “IP Multimedia (IM) Subsystem - Stage 2”, a document which is under control of 3GPP TSG SA WG 2. Version V1.7.0 (2001-02) is the most recent version on the 3GPP server. This contribution therefore bases its conclusions on an analysis of this version of TS 23.228.

These conclusions are largely based on an analysis of information flows presented in TS 23.228. For the convenience of the reader, some of the relevant information flows are included in this contribution. However, so as not to affect the readability of this contribution, these information flows are included in an appendix.

2 Termination of integrity

There is agreement in S3 that SIP messages sent to and from the UE need to be integrity-protected with a cryptographic key generated during the authentication and key agreement procedure. The question under discussion is whether the P-CSCF or the S-CSCF terminates integrity on the network side. The terminating entity is characterised by being in possession of the integrity key and being able to perform integrity checks of messages sent by the UE and append integrity check values to messages sent to the UE.

This section presents a number of security reasons for terminating integrity in the P-CSCF.

2.1 Procedures for codec negotiations

In section 5.12.3 of TS 23.228, procedures for codec negotiations are described. The corresponding information flows are contained in Appendix 1 of this contribution.

From section 5.12.3.1 of TS 23.228:

> "This section gives information flows for the procedures for determining the set of mutually-supported codecs between the endpoints of a multi-media session, determining the initial codecs to be used for the multi-media session, and the procedures for changing between codecs when multiple ones are supported ...
>
> 1. UE#1 determines the complete set of codecs that it is capable of supporting for this session. It builds a SDP containing bandwidth requirements and characteristics of each, and assigns local port numbers for each possible media flow. Multiple media flows may be offered, and for each media flow (m= line in SDP), there may be multiple codec choices offered.
>
> 2. UE#1 sends the initial INVITE message to P-CSCF#1 containing this SDP
>
> 3. P-CSCF#1 examines the media parameters, and removes any choices that the network operator decides, based on local policy, not to allow on the network."

This implies that the P-CSCF must be able to modify the signalling messages sent by the UE in the procedures for codec negotiations.

It is concluded that these messages must not be integrity-protected between the UE and the S-CSCF. On the other hand, they should be integrity-protected between the UE and the P-CSCF again showing a need for integrity in the P-CSCF.

2.2 Mobile terminal initiated session release

In section 5.11.1 of TS 23.228, the procedure "Mobile terminal initiated session release" is described in the following steps:

> "1. One mobile party hangs up, which generates a message (Bye message in SIP) from the UE to the P-CSCF.
> 2. Steps 2 and 3 may take place before or after Step 1 and in parallel with Step 4. The UE initiates the release of the bearer PDP context. The GPRS subsystem releases the PDP context. The IP network resources that had [?] were reserved for the message receive path to the mobile for this call are now released. This is initiated from the GGSN. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would invoked here.
> 3. The GPRS subsystem responds to the UE.
> 4. The P-CSCF removes the authorisation for resources that had previously been issued for this endpoint for this session. This step also will terminate the media flow if the UE did not properly perform that function in step 2 above.
> 5. The P-CSCF sends a hang-up to the S-CSCF of the releasing party."

For the corresponding information flow see Appendix 2.

This means that the resources for the call are released before the S-CSCF even knows about it. If the P-CSCF is unable to verify the origin of the "Bye" message sent by the UE then also a bogus "Bye" message could cause the release of the call. In other words, anyone able to send IP packets to the P-CSCF could release anybody else's call. This could be used to selectively target users or to cripple the system completely.

Of course, the procedure as described in TS 23.228 could be modified so that the P-CSCF releases resources only after receiving confirmation from the S-CSCF. However, this would be at the cost of a higher network signalling load and a higher delay in releasing the resources.

It is concluded that the P-CSCF should be able to check the integrity of release messages.

3 Need for integrity protection of messages between P-CSCF and S-CSCF

In section 5.11.3.1 of TS 23.228, procedures for a network initiated session release - P-CSCF initiated are described:

> “1. The bearer for the session is terminated, for example, by a mobile power down or loss of signal, etc. This is noted by the GPRS subsystem.
>
> 2. The GPRS subsystem may send a release indication to the P-CSCF for the disconnected mobile. The P-CSCF might also note the release due to a SIP Session Timeout.
>
> Editor's Note: Which mechanism is used to report or detect release in this case is FFS.
>
> 3. The P-CSCF removes the authorisation for resources that had previously been issued for this endpoint for this session.
>
> 4. The P-CSCF generates a Hang-up (Bye message in SIP) to the S-CSCF of the releasing party. It is noted that this message should be able to carry a cause value to indicate the reason for the generation of the hangup.”

The Hang-up message is an example of a message sent by the P-CSCF to the S-CSCF which does not originate from the UE. The S-CSCF must be able to check the integrity of this message so as to prevent fake session releases. Without protection the attacks would be the same as described for mobile terminal initiated session release, cf. section 2.1 of this contribution.

It is concluded that there is a need for the integrity protection of messages between P-CSCF and S-CSCF independent of any potential integrity protection between UE and S-CSCF.

Note: The integrity protection of messages between P-CSCF and S-CSCF is not user-specific and may be provided by an IPSec tunnel in accordance with the principles laid down in TS 33.200 “Network Domain Security”. This section shows that extending integrity protection from the UE to the S-CSCF does not remove the requirement for NDS at this point.

4 Need for integrity protection of messages between P-CSCF and GGSN

In section 5.11.3 of TS 23.228, procedures for a network initiated session release are described:

> “In case of a break in the radio connection for a real-time PDP context which is related to an IM session, the corresponding session should be terminated in order to avoid billing for session inactivity time. . . .
>
> 4. If a request state was created in the PCF [comment: Policy Control Function, located in P-CSCF] at PDP context activation, the GGSN sends the Release indication message to the PCF. The message indicates that the corresponding PDP context has been deactivated.
>
> 5. The proxy CSCF performs session termination, which is FFS.“

This implies that anyone impersonating a GGSN towards a P-CSCF could terminate any session, cf. attacks in sections 2.1 and 3.

It is concluded that there is a need for the integrity protection of messages between GGSN and P-CSCF.

Note: The integrity protection of messages between P-CSCF and GGSN is not user-specific and may be provided by an IPSec tunnel in accordance with the principles laid down in TS 33.200 “Network Domain Security”.

Conclusions

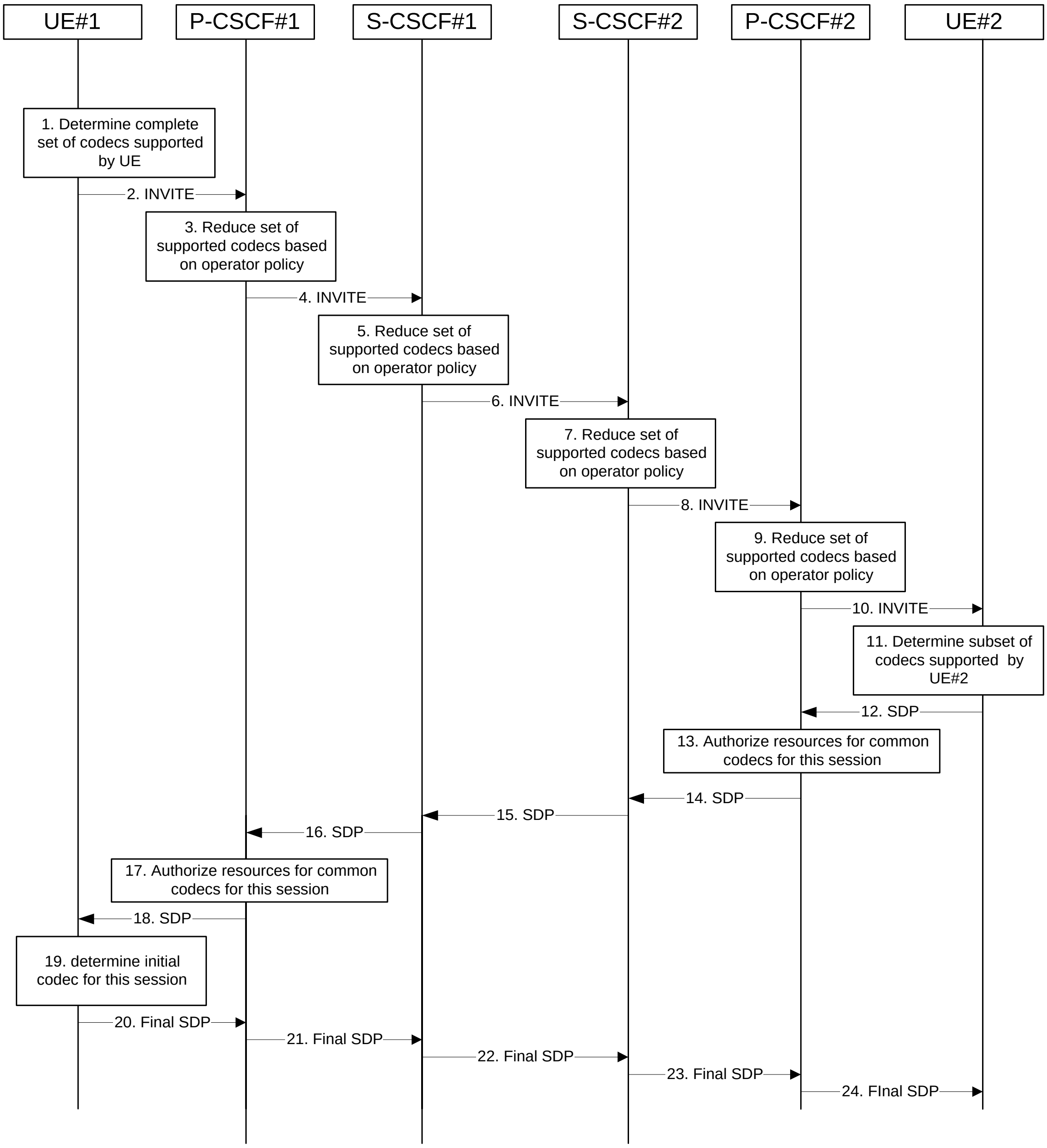
This contribution showed that the P-CSCF must be able to check the integrity of messages sent by the UE. It also showed that the integrity-protection of all messages is not possible between the UE and the S-CSCF as the P-CSCF needs to modify some of them. The contribution further showed the need for network domain protection between GGSN and P-CSCF and between P-CSCF and S-CSCF.

As a general remark, it seems to be a good idea, quite apart from the security considerations above, to perform the integrity check of messages originating from the UE as early as possible so as to prevent bogus messages from creating additional load in the signalling network.

Appendix 1

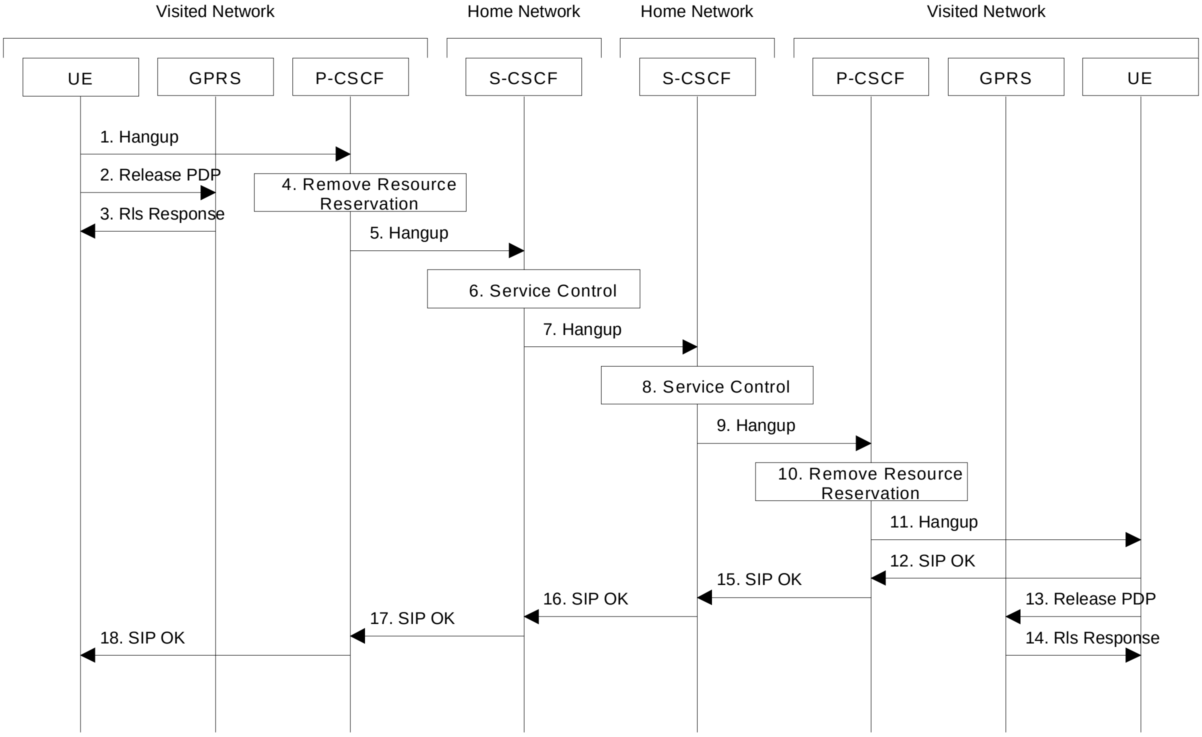
From section 5.12.3 of TS 23.228, procedures for codec negotiations

5.12.3.1 Codec negotiation during initial session establishment


UE#1
P-CSCF#1
S-CSCF#1
S-CSCF#2
P-CSCF#2
UE#2
1. Determine complete set of codecs supported by UE
2. INVITE
3. Reduce set of supported codecs based on operator policy
4. INVITE
5. Reduce set of supported codecs based on operator policy
6. INVITE
7. Reduce set of supported codecs based on operator policy
8. INVITE
9. Reduce set of supported codecs based on operator policy
10. INVITE
11. Determine subset of codecs supported by UE#2
12. SDP
13. Authorize resources for common codecs for this session
14. SDP
15. SDP
16. SDP
17. Authorize resources for common codecs for this session
18. SDP
19. determine initial codec for this session
20. Final SDP
21. Final SDP
22. Final SDP
23. Final SDP
24. FInal SDP

Appendix 2

From section 5.11.1 of TS 23.228, V1.7.0 “Mobile terminal initiated session release”



Visited Network
Home Network
Home Network
Visited Network
UE
GPRS
P-CSCF
S-CSCF
S-CSCF
P-CSCF
GPRS
UE
1. Hangup
2. Release PDP
4. Remove Resource Reservation
3. Rls Response
5. Hangup
6. Service Control
7. Hangup
8. Service Control
9. Hangup
10. Remove Resource Reservation
11. Hangup
12. SIP OK
15. SIP OK
16. SIP OK
13. Release PDP
17. SIP OK
18. SIP OK
14. Rls Response