strongSwan - Bug #1198

Early IKEv1 Quick Mode exchange packets are ignored

09.11.2015 02:36 - Mark McKinstry

Status:	Closed	**Start date:**	09.11.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.4		
Affected version:	5.3.1	**Resolution:**	Fixed

Description

We are finding that very occasionally during a Quick Mode exchange the responder receives the final packet very early, before it has finished processing the previous packet, and it generates a log entry like "ignoring request with ID 3584557445, already processing".

It appears to be falsely determining that this final Quick Mode packet is the same as the packet it is still processing and so ignores it. The problem appears to be in get_message_id_or_hash() (in src/libcharon/sa/ike_sa_manager.c), which for IKEv1 and non-zero message-ID, returns message ID, but all Quick Mode messages have the same message ID!

The fix that worked for us was to modify get_message_id_or_hash() to make it return message hash, rather than message ID, for Quick Mode exchange messages - see attached patch.

Associated revisions

Revision 7b5dcc9f - 11.11.2015 11:01 - Tobias Brunner

ikev1: Also use message hashes for Quick Mode for the early retransmission check

We already did so during Phase 1 but because all three Quick Mode
message have the same message ID we occasionally dropped the third
message as retransmit, so we do it there too. For INFORMATIONAL
and TRANSACTION exchanges we don't expect more than one inbound message
with the same message ID so we still use them there.

Fixes #1198.

History

#1 - 09.11.2015 17:30 - Tobias Brunner

- Tracker changed from Issue to Bug

- Status changed from New to Feedback

> We are finding that very occasionally during a Quick Mode exchange the responder receives the final packet very early, before it has finished processing the previous packet, and it generates a log entry like "ignoring request with ID 3584557445, already processing".

Yes, makes sense. This is a race condition between the thread that sent the second QM message and is cleaning up and the thread that processes the third QM message. Since resetting the IKE_SA entry's processing member to 0 is pretty much the last step for the first thread, it's possible that the second thread finds that value still set to the QM's message ID.

> The fix that worked for us was to modify get_message_id_or_hash() to make it return message hash, rather than message ID, for Quick Mode exchange messages - see attached patch.

I guess we could change that generally for IKEv1 and just use hashes there. Only for INFORMATIONAL exchanges we don't expect more than one message with the same MID, or even retransmits, so we could still use MIDs there. I pushed such a change to the *1198-ikev1-mid-hash* branch. Let me know if that works for you.

#2 - 10.11.2015 21:20 - Mark McKinstry

Tobias Brunner wrote:

> I pushed such a change to the 1198-ikev1-mid-hash branch. Let me know if that works for you.

Thanks for your patch. I can confirm that it would serve our needs - and it does test out OK on our setup.

#3 - 11.11.2015 11:02 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.3.4

- Resolution set to Fixed

Thanks for testing. The patch I now merged is actually more like the one you posted because for TRANSACTION exchanges the MID is also still usable (and probably slightly quicker).

Files

0001-Fix-IKEv1-Quick-Mode-exchange-pkts-being-se.patch	1.98 KB	09.11.2015	Mark McKinstry