strongSwan - Issue #3148

Control flow to OpenSSL

14.08.2019 22:00 - amritha rao

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.8.0	**Resolution:**	No feedback

Description

Hi,

I could not find this info in the README section or in the Strongswan forum which is why I'm posting it here.
Suppose I'm using the OpenSSL engine to perform IKEv1 and IKEv2, then how does the control flow to OpenSSL?
Code for IKE I see is in libcharon. So I'm interested in understanding how does control from libstrongswan and libcharon and OpenSSL plugin.

Thanks in advance!

History

#1 - 15.08.2019 09:51 - Tobias Brunner

- Status changed from New to Feedback

What exactly do you want to know?

#2 - 16.08.2019 14:59 - Noel Kuntze

OpenSSL is only used for cryptographic primitives, third party lib dependencies and certificate authentication (if no other plugin provides the functionality). OpenSSL never takes part in the IKE negotiation as part of the control flow of the protocol or the parsing of packets. Only its primitives are used for cryptographic operations (and certificate parsing and authentication).

#3 - 19.08.2019 21:18 - amritha rao

Thanks for the response.
Where is the code that performs the key derivation?
What OpenSSL calls does it use?

#4 - 20.08.2019 13:21 - Noel Kuntze

Check the openssl plugin's source code in the repository (git.strongswan.org or Github.

#5 - 26.08.2019 21:21 - amritha rao

Thanks for the response.
I've already looked into the openssl plugin. What I want to know is, how OpenSSL gets used to perform Key derivation of IKE keys.

#6 - 27.08.2019 09:05 - Tobias Brunner

source:src/libcharon/sa/ikev2/keymat_v2.c#L301

#7 - 09.10.2019 11:09 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to No feedback