strongSwan - Feature #2946

Support for ChaCha20-Poly1305 via OpenSSL

03.03.2019 07:28 - Glen Huang

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.8.0		
Resolution:	Fixed		

Description

From the cipher suites doc it seems curve25519 support is only provided with the curve25519 plugin. But from the source code it seems openssl can also provide support if a recent enough version is used. Is the doc not up-to-date in this case?

Another question is that openssl provides ChaCha20-Poly1305 support since version 1.1.0. And it seems strongswan never makes use of that. Is there any plan to be able to leverage openssl's ChaCha20 implementation?

Associated revisions

Revision 34766542 - 08.03.2019 15:56 - Tobias Brunner

Merge branch 'openssl-chapoly'

Adds support for ChaCha20-Poly1305 via OpenSSL.

Fixes #2946.

History

#1 - 04.03.2019 09:50 - Tobias Brunner

- Category set to libstrongswan

- Status changed from New to Feedback

> Is the doc not up-to-date in this case?

Yep (see 5.7.2).

> Another question is that openssl provides ChaCha20-Poly1305 support since version 1.1.0. And it seems strongswan never makes use of that. Is there any plan to be able to leverage openssl's ChaCha20 implementation?

No, currently not.

#2 - 04.03.2019 17:58 - Tobias Brunner

- Tracker changed from Issue to Feature

- Subject changed from Openssl cipher support to Support for ChaCha20-Poly1305 via OpenSSL

- Target version set to 5.8.0

- Affected version deleted (5.7.2)

> > Another question is that openssl provides ChaCha20-Poly1305 support since version 1.1.0. And it seems strongswan never makes use of that. Is there any plan to be able to leverage openssl's ChaCha20 implementation?
>
> No, currently not.

I quickly put together a patch, see the *2946-openssl-chapoly* branch.

#3 - 06.03.2019 06:43 - Glen Huang

Tobias Brunner wrote:

> > Another question is that openssl provides ChaCha20-Poly1305 support since version 1.1.0. And it seems strongswan never makes use of that. Is there any plan to be able to leverage openssl's ChaCha20 implementation?
>
> No, currently not.

I quickly put together a patch, see the *2946-openssl-chapoly* branch.

Great stuff. Looking forward to it being merged.

#4 - 08.03.2019 15:57 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed