strongSwan - Bug #2347

AH proposals can be mangled in some valid and invalid configurations

30.05.2017 17:18 - Paul Wouters

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	ikev1		
Target version:	5.6.0		
Affected version:	5.5.1	**Resolution:**	Fixed

Description

IKEv1 AH support, working in 5.4.4, broken in 5.5.2 (versions in between not tested)

http://testing.libreswan.org/results/testing/v3.20-482-gfed7ad3-master/interop-ikev1-strongswan-11-ah-initiator-sha512/

This test case used to work, and now fails with:

| PROTO AH: we should check registration of attrs->transattrs.integ_hash=5
"westnet-eastnet-ikev1" #2: AUTH_ALGORITHM_HMAC_SHA2_256 attribute inappropriate in AH_AES_XCBC_MAC Transform | complete v1 state transition with BAD_PROPOSAL_SYNTAX

Another test case failure:

http://testing.libreswan.org/results/testing/v3.20-482-gfed7ad3-master/interop-ikev1-strongswan-10-ah-initiator-sha256/description.txt

Seems what we receive is badly formed:

| ***parse ISAKMP Transform Payload (AH): | next payload type: ISAKMP_NEXT_NONE (0x0) | length: 28 (0x1c) | AH transform number: 1 (0x1) | AH transform ID: AH_AES_XCBC_MAC (0x9) | ****parse ISAKMP IPsec DOI attribute: | af+type: AUTH_ALGORITHM (0x8005) | length/value: 5 (0x5) | [5 is AUTH_ALGORITHM_HMAC_SHA2_256] | ****parse ISAKMP IPsec DOI attribute: | af+type: GROUP_DESCRIPTION (0x8003) | length/value: 5 (0x5) | [5 is OAKLEY_GROUP_MODP1536]

Configurations and pluto/charon logs can be found at the above link.

There are more issues with bad configurations, such as specifying ah=sha2-modp2048

Associated revisions

Revision 5d580ae0 - 05.07.2017 10:08 - Tobias Brunner

ikev1: Determine transform ID before mapping integrity algorithm ID

Due to the lookup based on the mapped algorithm ID the resulting AH
proposals were invalid.

Fixes #2347.

Fixes: 8456d6f5a8e9 ("ikev1: Don't require AH mapping for integrity algorithm when generating proposal")

Revision a3bcbb4c - 05.07.2017 10:08 - Tobias Brunner

stroke: Don't load configs with invalid proposals

References #2347.

History

#1 - 30.05.2017 17:20 - Paul Wouters

config files can be seen in the libreswan git repo, eg:

https://github.com/libreswan/libreswan/tree/master/testing/pluto/interop-ikev1-strongswan-10-ah-initiator-sha256/

#2 - 30.05.2017 18:29 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to ikev1

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

- Target version set to 5.6.0

- Affected version changed from 5.5.3 to 5.5.1

- Resolution set to Fixed

> IKEv1 AH support, working in 5.4.4, broken in 5.5.2 (versions in between not tested)

Thanks for the report. I pushed a fix to the *2347-ah-proposal* branch. Was broken since 5.5.1.

> There are more issues with bad configurations, such as specifying ah=sha2-modp2048

Unless you configure that with an ! at the end there shouldn't really be a problem (a default is added). In strict mode, however, this results in an empty proposal (but at least you get two messages in the log, in either case):

```
[CFG] algorithm 'sha2' not recognized
[CFG] skipped invalid proposal string: sha2-modp2048
```

With swanctl.conf the complete config would be rejected, but that's currently not the case with ipsec.conf. There is another commit in the branch above that changes that.

#3 - 05.07.2017 10:10 - Tobias Brunner

- Status changed from Feedback to Closed