strongSwan - Bug #771

strongswan ike phase 2 exchange with ikev1 involving AH algorithm does not work when communicating with non-strongswan ike daemon

21.11.2014 17:21 - bettina ko

Status:	Closed	**Start date:**	21.11.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.2.2		
Affected version:	5.1.1	**Resolution:**	Fixed

Description

I had problem when setting ah to either sha1 and md5 when communicating to a non-strongswan ike daemon. It appears that ah algorithm passed in ike phase2 exchange is off. For example, when I did ah=sha1 I see the value 3 on the other end when it suppose to be 2. According to IKE attributes definition, the mapping is MD5=1, SHA=2, Tiger=3, SHA2-256=4, etc.. After looking at strongswan source code for clue, I believe the bug is in proposal_substructure.c in which it gets/sets the attributes as transform id instead of integrity algorithm. set_from_proposal_v1 should have done the get_ikev1_transid_from_alg only for transform_substructure_create_type call , not the following add_transform_attribute call in the following section code.

```
enumerator = proposal->create_enumerator(proposal, INTEGRITY_ALGORITHM);
     if (enumerator->enumerate(enumerator, &alg, &key_size))
{

alg = get_ikev1_transid_from_alg(proto, INTEGRITY_ALGORITHM, alg);
          if (alg)
{
                if (!transform)
     {
                     transform = transform_substructure_create_type(
                                              PLV1_TRANSFORM_SUBSTRUCTURE, number, alg);
                }
                transform->add_transform_attribute(transform,
                     transform_attribute_create_value(PLV1_TRANSFORM_ATTRIBUTE,
                                              TATTR_PH2_AUTH_ALGORITHM, alg));
          }
     }
```

Furthermore, add_to_proposal_v1 should not call get_alg_from_ikev1_transid for TATTR_PH2_AUTH_ALGORITHM when the correct value is set.

History

#1 - 24.11.2014 17:39 - Tobias Brunner

- Category set to libcharon

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

- Target version set to 5.2.2

Thanks for the report and your analysis.

There are two sets of identifiers, the AH Transform Identifiers and the Authentication Algorithms. The latter are sent in the *Authentication Algorithm* attributes contained in the AH transforms (and also the ESP transforms if authentication is used). The two sets of identifiers only partially match (starting with 5).

I pushed a fix to the *ikev1-ah-proposal* branch of our repository (2c6fe299f8). Let me know if that works for you.

#2 - 11.12.2014 13:56 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed

Merged to master with 728f529c42.