strongSwan - Bug #2457

strongSwan Sends Key Info With Update SA Though Disallowed By FreeBSD

02.11.2017 15:48 - Chinh Nguyen

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.6.1		
Affected version:	5.6.0	**Resolution:**	Fixed

Description

With the update SA used to manage MOBIKE address/port change, strongSwan queries for the current SA info and then sends an update SA with new address/port changes. However, if there are key information in the response to the SA query, it will also include that in the SA update.

src/libcharon/plugins/kernel_pfkey/kernel_pfkey_ipsec.c:

```
    if (response.key_encr)
    {
        PFKEY_EXT_COPY(msg, response.key_encr);
    }

    if (response.key_auth)
    {
        PFKEY_EXT_COPY(msg, response.key_auth);
    }
```

But the FreeBSD 11.1 kernel explicitly disallows key updates to established SA and so rejects the pfkey message:

sys/netipsec/key.c:

```
        /*
         * For DYING and MATURE SA we can change only state
         * and lifetimes. Report EINVAL if something else attempted
         * to change.
         */
        if (!SADB_CHECKHDR(mhp, SADB_EXT_KEY_ENCRYPT) ||
            !SADB_CHECKHDR(mhp, SADB_EXT_KEY_AUTH)) {
            key_freesav(&sav);
            return (key_senderror(so, m, EINVAL));
        }
```

Associated revisions

Revision 21a500a0 - 08.11.2017 16:34 - Tobias Brunner

kernel-pfkey: Don't include keys in SADB_UPDATE message to update IPs on FreeBSD

The FreeBSD kernel explicitly rejects messages containing keys for mature SAs.

Fixes #2457.

History

#1 - 03.11.2017 09:39 - Tobias Brunner

- Tracker changed from Issue to Bug

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

- Target version set to 5.6.1

I see. I pushed a fix for this to the *2457-freebsd-sa-update* branch.

#2 - 08.11.2017 16:33 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed