strongSwan - Bug #547

key passphrase lost between network manager gui and charon-nm

14.03.2014 12:22 - Harald Dunkel

Status:	Closed	**Start date:**	14.03.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	networkmanager (charon-nm)		
Target version:	5.1.3		
Affected version:	5.1.1	**Resolution:**	Fixed

Description

Using Debian Jessie (network-manager-strongswan 1.3.0 and strongswan 5.1.1) I am asked for the key passphrase, but it seems that it is lost on its way to charon-nm. daemon.log shows 3 lines like

```
charon-nm: 02[LIB] building CRED_PRIVATE_KEY - RSA failed, tried 8 builders
```

See the attached log file. There is also a popup complaining about no valid VPN secrets (not shown here).

If I use openssl to remove the passphrase (just for testing), then the unprotected key works.

Associated revisions

Revision c489c588 - 18.03.2014 14:53 - Tobias Brunner

charon-nm: No additional secrets are required once a password has been entered

Recent versions of NM will call need_secrets() as long as it returns TRUE,
but then fail as the number of calls is limited by an assert.

Fixes #547.

History

#1 - 17.03.2014 08:13 - Harald Dunkel

PS: I would like to migrate about 30 laptops from openVPN to Strongswan, but I am stuck due to this problem.

#2 - 17.03.2014 19:12 - Tobias Brunner

- Tracker changed from Issue to Bug

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

> I am asked for the key passphrase, but it seems that it is lost on its way to charon-nm.

It's not actually lost. What happens is this: The NeedSecrets callback is called multiple times by NetworkManager. If the method returns TRUE NM will invoke the registered auth-dialog. The first time without interaction, to load cached secrets, the second time with interaction, to show a dialog and request a secret from the user. The problem is that the NeedSecret implementation in source:src/charon-nm/nm/nm_service.c#L623 always will return TRUE for public key authentication ("key"). This is because the entered password is not yet made available to the decoding routines. After this happens the second time NM's internal state machine breaks because it does not expect additional secrets to be required after the user has already been asked for one. I'm not sure why it worked before. It's possible that earlier versions of NM called NeedSecrets just once.

Something like this should fix it:

```
--- a/src/charon-nm/nm/nm_service.c
+++ b/src/charon-nm/nm/nm_service.c
@@ -660,6 +660,10 @@ static gboolean need_secrets(NMVPNPlugin *plugin, NMConnection *connection,
                                        key->destroy(key);
                                        return FALSE;
                                }
+                               else if (nm_setting_vpn_get_secret(settings, "password"))
+                               {
```

```
+                                       return FALSE;
+                                   }
                                }
                            }
                            else if (streq(method, "smartcard"))
```

#3 - 18.03.2014 12:17 - Harald Dunkel

- File daemon1.log added

I tried your patch on top of 5.1.2, but it seems that the key still cannot be decoded. Log file is attached. Please note the "no private key found for ...". If I use the key without passphrase, then there is no such message.

Do you think this is something to be fixed in NetworkManager or network-manager-strongswan?

#4 - 18.03.2014 13:10 - Tobias Brunner

> I tried your patch on top of 5.1.2, but it seems that the key still cannot be decoded. Log file is attached. Please note the "no private key found for ...". If I use the key without passphrase, then there is no such message.

Are you sure the private key is the same in the two files you are using? Because if decrypting the key had failed, NM would already have aborted the initiation with an error message ("Loading private key failed."). Since that is not the case I suspect the encrypted key does not actually match your client certificate, whereas the unencrypted key does.

#5 - 18.03.2014 14:14 - Harald Dunkel

You are right, I used the wrong key. Sorry. Tests are still in progress, but AFAICS the "no private key found" message is gone, even though the key is protected by a passphrase.

Do you think your patch could be added to the official sources?

Thanx
Harri

#6 - 18.03.2014 14:56 - Tobias Brunner

- Category set to networkmanager (charon-nm)

- Status changed from Feedback to Closed

- Target version set to 5.1.3

- Resolution set to Fixed

> Do you think your patch could be added to the official sources?

Done with the associated commit.

#7 - 09.02.2015 16:17 - Harald Dunkel

Is it possible that this problem is back? I didn't check for quite some time (I had to move back to Wheezy), but using Strongswan 5.2.2 on a freshly installed laptop running Jessie I see the error message on every second run again.

#8 - 01.03.2016 09:16 - Harald Dunkel

Any news about this? Its a pretty annoying problem.

I would have reopened this bug report, but obviously I am not allowed.

Files

daemon.log	2.45 KB	14.03.2014	Harald Dunkel
daemon1.log	3.88 KB	18.03.2014	Harald Dunkel