Quassel IRC - Feature #489

Provide validation of and feedback about the core/client SSL cert

01/17/2009 01:08 AM - Sputnick

Status:	Confirmed	**Start date:**	01/17/2009
Priority:	Normal	**Due date:**	
Assignee:	EgS	**% Done:**	80%
Category:	General / Unspecified	**Estimated time:**	0.00 hour
Target version:			
OS:	Any		

Description

It would be nice to show a different icon ("security-medium" exists for that purpose) in the statusbar in case there were problems with the cert, and maybe a way (tooltip? popup?) to display the warnings generated by cert validation. Core output on the console will rarely be seen by people.

Also we should at least warn or outright refuse connection if the core cert's fingerprint has changed; similar to what SSL does. This prevents MITM attacks after the initial connection.

We also need to find a way to make SSL connections the default. Right now, if the core doesn't support SSL, we fail and tell the user to uncheck the box manually. This is OK, but it would be smoother to just change that directly if the user accepts rather than requiring extra clicks. Need to make sure it works with the mono client too.

History

#1 - 01/29/2009 01:19 AM - EgS

- Assignee set to EgS

- % Done changed from 0 to 80

Sputnick wrote:

> It would be nice to show a different icon ("security-medium" exists for that purpose) in the statusbar in case there were problems with the cert, and maybe a way (tooltip? popup?) to display the warnings generated by cert validation. Core output on the console will rarely be seen by people.

Mostly done. You will be informed on connect (before you're able to login) about any issues with the core's ssl certificate. You also have the ability to inspect that certificate. And add the core to the "known hosts" which will basically store a pair of hostaddress and certificate digest. (see below).

TBD:
- icons + tooltips
- we should also drop that lock icon from the connect to core dialog in favor of the security icons we already use in the statusbar.

> Also we should at least warn or outright refuse connection if the core cert's fingerprint has changed; similar to what SSL does. This prevents MITM attacks after the initial connection.

If the digest of the core's ssl certificate changes you will be warned about it in the same manner as described above.

> We also need to find a way to make SSL connections the default. Right now, if the core doesn't support SSL, we fail and tell the user to uncheck the box manually. This is OK, but it would be smoother to just change that directly if the user accepts rather than requiring extra clicks. Need to make sure it works with the mono client too.

This has not been done yet. I don't see any possible problems with the mono client here.

#2 - 02/18/2009 12:03 AM - Sputnick

- Status changed from New to Confirmed

- Target version deleted (0.4.0)

- OS set to Any