ChiliProject - Bug # 618: Add TLS support to ldap connection

Status:	Open	**Priority:**	Normal
Author:	Igor GaliÄ‡	**Category:**	
Created:	2011-09-13	**Assignee:**	
Updated:	2011-09-17	**Due date:**	
Remote issue URL:			
Affected version:			
Description:	This patch (to redmine) has been residing in their issue tracker for.. 3? Years. I applied it on every update, now I'm doing the same ChiliProject. I think it would be enormously helpful if guys added this standard feature		

History

2011-09-13 11:17 am - Alexander PÃ¡nek

+1 !

2011-09-13 12:35 pm - Holger Just

- Status changed from Ready for review to Open

Igor, Welcome to ChiliProject.

Unfortunately, we can't accept your patch as it is now. You patch mixed many different things which are mostly unrelated to TLS into one big mess.

Apart from the unrelated changes to the Gemfile (where you actually forgot to include the @ruby-ldap@ gem), most of the code is for switching from @Net::LDAP@ to "ruby-ldap":https://github.com/alexey-chebotar/ruby-ldap which is covered in #258. So the core of the patch are the three lines with the switch to use either @LDAP::SSLConn@ or @LDAP::Conn@ which seems necessary for @ruby-ldap@.

Finally, I want to note that ChiliProject and Redmine already support TLS now which is exactly what is enabled if you check the TLS box. The only feature we (or better @net-ldap@) don't support is SSL via @STARTSSL@. But from my understanding, this is also not added by your library.

What is also missing is a way to check certificates. Without this feature, SSL/TLS is about useless as most of the time, once an attacker is able to observe traffic, she is also able to spoof it and thus take over the connection with a spoofed certificate which - unless properly checked effectivly disables the perceived security of SSL/TLS. However, having this feature is rather complex to do as a web app, as it involves a couple of steps to initially trust an potentially unknown certificate. It might be easier to do it by configuration. But I guess, this is out of scope for this issue for now.

So finally, I have to ask the question, what does this patch add â€” feature-wise â€” what we don't have now? could you also please reference the Redmine issue, as I wasn't able to find it now...

2011-09-17 09:24 am - Igor GaliÄ‡

I would close the ticket as Invalid.

The problem I have with reverting the change back is that the configurations are stored in the database. This is quite fatal with configuration changes needed for authentication. You need a working application to make changes to authentication system..
..back then when I put this patch into place I needed StartTLS --- now I need the patch, because I patched the system back then.

Files

chili_tls_ldap.patch	3.2 kB	2011-09-13	Igor GaliÄ‡