Generic reporting and exception configuration for bad SSL server certificates

Author:
Kai Engert
kaie@redhat.com
August 2009

The error page reporting and exception creating mechanism for bad SSL server certificates introduced in Firefox 3.x is insufficient for other Mozilla applications like Thunderbird.

The motivation of this document is to extend the existing solution (used by Firefox) in a way that works with SSL connections in any Mozilla application.

Introduction

The design described here is based on another document titled „Better SSL Client Authentication for Mozilla applications“. While working on the SSL client authentication topic, it became clear the same mechanism may also be appropriate to implement a general solution for reporting and management of problems around SSL server authentication.

Before reading this document, please make sure you have read the mentioned base document.

The document about SSL client authentication showed how to manage a specific property of an SSL connection and associated configuration choices.

Another property of an SSL connection is the state of the server authentication. The authentication may be broken (bad certificate) but the user may decide to proceed anyway.

In Firefox 3.x the concept of „certificate exceptions“ got introduced and the classic prompts got disabled, because they invited the user to take risks and simply proceed.

However, the support to manage such exceptions in applications other than Firefox has been insufficient. While Firefox can use its content area to display an „error page“ and provide guided assistance to work around it, other applications like Thunderbird don't have support yet that works equally well.

A general mechanism is required, a general solution to report bad SSL certificates, not using prompts, not inviting users to click through. A solution that requires users to deliberately decide to work around it, but on the other hand be readily available.

This document has already proposed to introduce a status bar area for SSL client state.

The next sections will propose a similar status bar area to visualize the state of bad server certificates and to provide access to the exception mechanism, similar to what's being provided by Firefox.

General SSL status for any SSL connection

Browser applications (like Firefox) use a status bar padlock icon when an SSL connection is active. This icon can be accessed to learn details about the SSL connection like cipher strength or to view the certificate used by the server.

Other applications use SSL connections, too, for example connections to mail servers. Unfortunately, access to SSL status information for those connection is often not available, although users would benefit from the same information and have expressed a desire to be able to view this information.

The proposal is to allow any application to include space for an SSL server status icon in their user interface, preferably in the status bar.

This document already talked about SSL connections either being tied to a specific window or be running independently in the background. It described a solution where SSL client authentication status may be shown for both groups of connections. The same strategy could be used to report the SSL server authentication status.

The SSL server status icon (e.g. Padlock) may offer a dropdown list of active (or recently closed) SSL connections (globally or associated to the current window) and allow to view an informational dialog, similar to the security portion of the „page info“ dialog provided by Firefox.

Bad certificate notifications outside of Firefox

When the server side of an SSL connection uses a „bad certificate“ (e.g. expired, can not be authenticated, has a hostname mismatch), and the connection happened outside a browser window, then no error page can be shown.

(There may be scenarios where it's possible, for example the mail application could display an error page in the same area where it usually shows the contents of an email message. But there are clearly scenarios where it seems impossible or inappropriate, for example in the message compose window, or when performing a background SSL/LDAP address book lookup while typing a name into the compose window.)

The proposal is to use the SSL server status area to contain (a list of) the current and recent problematic SSL sites using a „Server Auth Control“ (SAC). Accessing SAC shall open a dialog with information equivalent to what's being provided on error pages by Firefox.

When a bad cert is encountered, the termination will stop (as usual) and an error message may be shown, but the error message will give no hint how to fix it.

Instead, SAC will show an icon that visualizes such a „terminated“ connection. (Icon idea: Use two radio masts and a broken network line between them?)

When a user clicks SAC, a list of the problematic sites (with port number) will be shown.

When a user clicks an hostname[:port] entry, a dialog will open that shows contents equivalent to the

„bad cert error page“ used by Firefox.

That dialog shall behave in the same way as the error page, give explanations, provide guidance, and allow to jump to the „add exception“ dialog, prefilled with the hostname[:port] selected by the user.

Implementation thoughts

CliAC and SerAC may exist and need to be registered independently, in order to give applications full control over their desired features. The application shall include any combination of them in their chrome and register them with PSM at application start.