Tails - Bug #11812

tails-security-check's CA pinning is not effective on sid

09/19/2016 09:00 AM - intrigeri

<table>
<thead>
<tr>
<th>Status:</th>
<th>Resolved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Elevated</td>
</tr>
<tr>
<td>Assignee:</td>
<td>intrigeri</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>Tails_3.0</td>
</tr>
<tr>
<td>Feature Branch:</td>
<td></td>
</tr>
<tr>
<td>Type of work:</td>
<td>Code</td>
</tr>
<tr>
<td>Blueprint:</td>
<td></td>
</tr>
<tr>
<td>Start date:</td>
<td>09/19/2016</td>
</tr>
<tr>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>% Done:</td>
<td>100%</td>
</tr>
<tr>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Spent time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>intrigeri</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
</tbody>
</table>

Description
I guess it's the same on Stretch. The BEGIN block does not work as it used to. This instead seems to work:

```perl
$ua->ssl_opts(verify_hostname => 1);
$ua->ssl_opts(SSL_ca_file => $cafile);
```

To be verified: do we also need to empty SSL_ca_path to avoid the system's /etc/ssl/certs/ from being used?

Note that we might wish to change the way tails-security-check does HTTPS requests entirely (#11810#note-1) so let's hold on a bit here.

Related issues:
Blocked by Tails - Feature #11810: Have our website CA bundle trust Let's Enc...

Resolved 09/19/2016

History

#1 - 09/20/2016 02:33 AM - intrigeri
- Description updated

#2 - 09/20/2016 02:40 AM - intrigeri
- Description updated

(Tested on Jessie, and there the CA pinning works fine.)

#3 - 09/20/2016 02:57 AM - intrigeri
- Related to Feature #11810: Have our website CA bundle trust Let's Encrypt CA added

#4 - 09/20/2016 02:58 AM - intrigeri
- Description updated

#5 - 09/20/2016 08:28 AM - intrigeri
- Status changed from Confirmed to In Progress
- % Done changed from 0 to 50

Fixed by my pull request on #11810.

#6 - 09/20/2016 08:28 AM - intrigeri
- Related to deleted (Feature #11810: Have our website CA bundle trust Let's Encrypt CA)
#7 - 09/20/2016 08:28 AM - intrigeri
- Blocked by Feature #11810: Have our website CA bundle trust Let's Encrypt CA added

#8 - 11/15/2016 10:44 AM - intrigeri
- QA Check set to Ready for QA

Next step is to do the tests documented on #11810#note-4 in a current feature/stretch.

#9 - 11/15/2016 07:39 PM - intrigeri
- Status changed from In Progress to Resolved
- % Done changed from 50 to 100
- QA Check changed from Ready for QA to Pass

- **OK** tails-security-check should work
- **OK** tails-security-check https://labs.riseup.net/test/tails.boum.org/security/ should work
- **OK** HTTPS_CA_FILE=/etc/ssl/certs/DST_Root_CA_X3.pem tails-security-check should fail
- **OK** HTTPS_CA_FILE=/etc/ssl/certs/AddTrust_External_Root.pem tails-security-check https://labs.riseup.net/test/tails.boum.org/security/ should fail