
# SpyZilla - fighting root CAs

## To trust, or not to trust?

---

**sachy**

2015-09-03

# Dictionary

- SpyZilla - Mozilla Firefox
  `http://brmlab.cz/user/jenda/spyzilla`
- CA - Certification Authority
- HSTS - HTTP Strict Transport Security
- CertPanel - Shortcut for reference
  *Edit→Preferences→Advanced→Certificates→View Certificates*

# How to get the public key?

- From webserver itself
- From CA repository
- Side way (pidgeon with printed key font size 8)
- DNS (TLSA, DNSSEC, IPSec,...)

# Bundled stuff

On Mozilla's wiki:
`https://wiki.mozilla.org/CA:IncludedCAs`

is a link to **outsourced** list of bundled CAs:
`https://mozillacaprogram.secure.force.com/CA/IncludedCACertificateReport`

Hardcoded list of HSTS sites: `nsSTSPreloadList.inc`

Trust bits stored in `cert8.db`

# Get rid of root CAs

To remove CA go to *CertPanel→Authorities*.

Click *Delete or distrust* and
...wait for it...
**Delete means distrust** and the CA is still in the list!

You have to go one-by-one, no option to distrust all/multiple at once.

# Manual cert exceptions

Go to *CertPanel→Servers* and click *Add Exception*.

The exception does NOT apply recursively for subdomains.

Exceptions have to be added in standard session. If you add it in private window, firefox ignores it.

Exceptions are stored in `cert_override.txt` file in FF profile directory.

# Roadblocks

- 3 more clicks per HTTPS session (Security Exception dialog)
- Since you are lazy to go ^^ all the time, your exceptions will be nice list of frequently visited sites. In plaintext.
- Easier MitM attack - you are used to ignore Security warnings
- HSTS - You are not able to connect without trust to given CA. Issue closed with Won't fix.

# nsSiteSecurityService.cpp.patch #1

Patch to ignore the HSTS preloaded list.

```
842,851c844
<   PRTime currentTime = PR_Now() + (mPreloadListTimeOffset * PR_USEC_PER_SEC);
<   if (mUsePreloadList && currentTime < gPreloadListExpirationTime) {
<     return (const nsSTSPreload *) bsearch(aHost,
<                                           kSTSPreloadList,
<                                           mozilla::ArrayLength(kSTSPreloadList),
<                                           sizeof(nsSTSPreload),
<                                           STSPreloadCompare);
<   }
<
<   return nullptr;
---
>   return nullptr; // Ignore HSTS preloaded sites
```

Download: `http://brmlab.s0c4.net/spyzilla_patch.zip`

# nsSiteSecurityService.cpp.patch #2

Patch to ignore HSTS header.

```
68c768,770
<   SSSLOG(("SSS: processing HSTS header '\%s'", aHeader));
---
>   //SSSLOG(("SSS: processing HSTS header '\%s'", aHeader));
>   SSSLOG(("SSS: ignoring HSTS header"));
>   return NS_OK;
```

Download: `http://brmlab.s0c4.net/spyzilla_patch.zip`

# aboutCertError.xhtml.patch

Patch to display "Add Exception" on the HSTS error page.

```
96c96
<           document.getElementById("badStsCertExplanation").setAttribute("hidden", "true");
---
>           document.getElementById("badStsCertExplanation").setAttribute("hidden", "false");
```

Download: `http://brmlab.s0c4.net/spyzilla_patch.zip`


SPY FOX
in
"DRY CEREAL"

# References


- http://fc07.deviantart.net/fs71/i/2010/325/e/1/spy_fox_dry_cereal___wallpaper_by_editor02-d33cig7.jpg
- http://www.antivirusgratis.com.ar/noticias/fotos/Mozilla-Actualizacion-Alerta-FDG.jpg
- https://archive.mozilla.org/pub/firefox/releases/41.0b6/source/
- https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security