Firefox and Security Add-ons

by Andy Pepperdine

Introduction

With recent revelations, there is much more interest in matters of security. This paper contains a quick review of some relevant add-ons to the Firefox browser which may of interest or use.

This paper looks at some of the additional features that can be added to Firefox to help private browsing. It does not look at the settings that you may wish to use to keep your browsing relatively private.

What are add-ons?

Add-ons are little applications that are added to the Firefox browser that extend its function in some way. They are typically not written by the Mozilla foundation, which supplies Firefox, but most are available from them through the normal channels.

To see what add-ons you already have, in Firefox, go to Tools → Add-ons to open the Add-on Manager in a new tab. By selecting the Extensions header on the left, you will see the add-ons that are currently installed. Depending on where you obtained your Firefox from, there may be some already there. These you can generally leave as they are.

Installing more

To get more add-ons, the Get Add-ons heading in the Add-on Manager will bring up a page containing, among other things, a search bar at the top right. Putting the name of the add-on, or some relevant keyword, will bring up the list of associated add-ons that are available in the Mozilla repository of add-ons.

Against each entry in the list is an Install button on the right hand side. In addition, many of them have a link to a more expansive description of the add-on through the word More.

Changing settings

Many of the add-ons can be tailored to suit your actual use.

If you go to look at the list under the Add-on Manager, at the Extensions heading, you will see for each add-on some buttons that can control each one separately. Depending on where your Firefox came form, most of the add-ons will have a Remove button to allow you to uninstall it and remove it from your Firefox.

Most also allow you to Disable it. Occasionally, you may wish to temporarily disable an add-on in order to see what effect it was having on a particular site.

Many have a Preferences button which will open a dialog where you can see the various configuration options for that add-on. This is where you can make it do what you want.

The Add-on Toolbar

In Firefox, under View → Toolbars , setting a tick mark against against Add-on Bar will show a tool bar along the very bottom of the window where the icons associated with each add-on may appear. Most appear on the right, but some can be seen on the left. Depending on each add-on, hovering the mouse over the icon, or clicking on it, may show you a menu of actions that this add-on controls. For each of the add-ons it is worthwhile spending a little time trying left, middle and right clicks on these icons to see what they do.

When you look at the menu from an icon, almost always, the Escape key will clear the menu away cleanly.

HTTPS Everywhere – or why not encrypt where we can?

This add-on is the only one mentioned here that is produced by an external agency, and so is not available in the usual add-on manner. To obtain it, go to the site:

https://www.eff.org/https-everywhere

where you will see the appropriate versions of the add-ons for your Firefox.

The intention of this add-on is to provide, as far as is possible, access to sites via the more secure https protocol, instead of the normal plain text http. It attempts to convert links into secure links if the site allows such access. If you see a link in one webpage to a site with a simple http prefix, but the site will allow https access, then this add-on will attempt to transfer you to the more secure protocol automatically.

Currently, the safe browsing protocols are rather little employed. They are spreading, but slowly, and still a lot of the Internet is open and insecure.

If you are concerned about how safe your browsing is, then this is the add-on to start with.

Settings

When HTTPS Everywhere is enabled, it puts a little blue circle with arrows at the top right, after the search input bar. A small triangle next to it will open a short menu to allow you to disable, see what sites it has set to https for this page, and gives options to change the settings, one of which is to tell the Electronic Frontier Foundation what certificates are being checked so they can improve their security checks.

Flagfox – or where is the host for this site?

This is a fun little add-on that slips a small flag at the end of the url bar to show which country contains the server that you got the page from.

If you mouse over the flag, it shows you the name of the domain you are reading from, the actual IP address for the page, and the country (in case your knowledge of flags is deficient).

A left click on the flag brings up a map locating it precisely.

If you use a middle click on the flag, it will transfer you to a site that looks up the ownership credentials of the site, so you can verify it is where you want to be.

A right click will enable you to reach other sites to get even more information.

NoRedirect – or where does that abbreviated link really go?

You might have seen during your browsing, short link names, and when you click on them they actually take you somewhere else entirely. These abbreviated names are useful to include in messages, like Twitter, and to put into print to reduce errors when typing them in. But you never know from the name of such a link, where it will actually go.

This add-on will intercept these re-directs so that you can see where they will take you before you go there. That way you can check it is where you want to go before you get there.

However, as set up initially, it does not contain any of the usual suspects for these abbreviated names, and so may appear to have no effect. But by going into the Preferences, you will see what it does allow and disallow. Anything not in the list will be ignored and Firefox will do what it always did.

My list of extras that I've stumbled across while browsing includes these:

```
^http://bit\.ly
^http://goo\.gl
^http://j\.mp
^http://dlvr\.it
^http://gu\.com
^http://usat\.ly
^http://slate\.me
^http://huff\.to
^http://tinyurl\.com
^http://wrd\.cm
^http://read\.bi
```

There are probably others that you will come across. To enter these, hit the Add button in the Preferences dialog, and then type these expressions in, adding each one in turn. For every one fo these, the Source column should be checked for them to be examined and intercepted.

Note the backslashes before the dots. This is important, as in the format used, a dot on its own means any character in that position. The backslash prevents this interpretation and forces \. to mean an explicit dot. Also, the hat character at the beginning means the start of the string being matched.

Share Me Not – or why should Facebook track me?

How Facebook et al know you have visited a particular site? The apparently ubiquitous little icons you see for FB, G+ and other social sites, are fetched from their servers, and so the mere fact that you have displayed the icon is enough to tell them you've been there.

This little add-on intercepts these fetches for the pictures, and substitutes its own versions. Only when you actually click on one of the icons, will they get the message you've been there. But if you are doing that, you are telling them explicitly anyway, and presumably you want to “like” something or other etc.

The Preferences give some small control over what is being tracked.

Certificate Patrol – or are the secure certificates up to date?

The secure https protocol relies on up to date certificates being in place at the certificate agencies. The site you are visiting is responsible for ensuring these are all current for their site. This add-on keeps track of the certificates you have seen, and alerts you when it finds an out of date one,(which in my experience is a rare occurrence).

But it also tells you when they are about to become outdated, or when they were apparently replaced long before time. This latter condition is a warning that perhaps the site has been compromised (or they thought so) and have replaced their certificates early. Or it might mean that an alien has intercepted the traffic and so had to insert their own for the real one.

If you are concerned about the integrity of sites you visit this add-on may be worthwhile. However, be aware that there are several places that are implementing an aggressive form of secure protocol that will be replacing these certificates frequently. In these cases, the alerts come frequently and may hide any real message you should be looking for.

Flashblock – or why should I watch that flashy stuff?

Adobe’s Flash is a means of encoding video stream for you to watch. It has a history of security holes in it, and is best avoided if possible.

This add-on enables you to block all flash unless you explicitly click on the screen to start it.

A side-effect is that a number of adverts that use flash become quiet and still, enabling you to read the page instead of suffering the annoying moving images.

The Preferences for this add-on provide a way of adding sites to a “white list” which will be allowed in any case. Note that it requires Javascript to work, so it has interactions with the NoScript add-on.

Adblock Plus – or why do I want to buy that?

This add-on does what it says in the title. It works off a list of known servers that provide adverts for other sites, so that when they are asked for, this add-on blocks them. The default list seems to work well in my experience. Your habits may means trying another one, which you can find from the Preferences by clicking the Filter Preferences button.

No Script – or why do I have to wait just for your benefit?

This is a very popular add-on that will suppress all scripts on a site unless you explicitly enable it. In that way, it can save a lot of time loading up and executing unnecessary advertisements and other non-essential dross associated with many sites.

Under the Preferences of the add-on, under the General tab, you can set it to always allow the upper level of a site. This I’ve found very useful, as typically you find you need scripts at that level to run many pages. But it still suppresses all fetched scripts from elsewhere, which normally suppresses all the irrelevant stuff.

The default settings are fine for normal use, but it is still worth looking at them all to see whether there is anything else you want to tweak.

When on a page, if you click on the icon (blue S with or without a No Entry sign), you will see what sites are being blocked. These can be allowed temporarily, or permanently. Allowing a site always to deliver scripts will place it on a “white list” by NoScript and that site will always execute scripts for you. You may find this is necessary for some financial sites and other shopping sites.

The general rule for the sites listed is that if you do not recognise the name, it is probably rubbish and best ignored. Only try those if there seems to be something missing or not working.

Self-destructing Cookies – or why should I keep your litter?

Cookies are those little bits of data that a website will drop onto your machine to keep track of what it is doing. The way the web works, it is not possible to avoid all use of cookies. But you can considerably reduce the time taken when they are present and active.

That is what this add-on does. When you leave a site, it checks the cookies and deletes any that are not needed by any active pages. This will prevent other sites from seeing them as a hint that you have visited those sites as well. There is collusion between some sites, and this is one way of thwarting them.

For more information, it is worth reading the description and the FAQ you can find at the Preferences to the add-on, and then scroll up to the top of that page.

Lightbeam – or who has heard about me, and from whom?

With everyone determined to know where you are, where you’ve been, and what you are doing, this add-on keeps track of who has been told about what and can display the results in a graph of list form. You might be surprised how everything gets connected together over time as you browse. The add-on keeps it across sessions, so you can accumulate all the history and see who knows what about you (theoretically).

It puts a little grey icon in the add-on bar. Clicking on it brings up a new tab and it shows you what is has found. There are a number of buttons available to customise what it does and how it shows it to you.

I found it quite educational as to how things are connected.

You can also clear out the information so you can start afresh to see what can be gleaned from a given time onwards.