Locking Down Firefox

Caging the Beast

Version 0.11

Abstract

With Firefox's popularity rising on a day-by-day basis, many corporate environments are starting to employ the power of Firefox as their default browser. But without sufficient restrictions or lock-downs Firefox becomes a powerful client controlled web browser that a sophisticated user can manipulate for their own benefits.

Firefox can be locked down similar to Internet Explorer, and this guide will give you the relevant information that is needed to create a secure, locked-down configuration, to restrict knowledgeable users actions into manipulating Firefox for their own needs.

Contents

Introduction

First you need to find out what the names are of the preferences you wish to lock. The best way to do this is by entering `about:config' in the Firefox URL address bar. You may then have to click the box "I'll be careful, I promise!" every preference that is in use will appear in the resulting window. You can use the filter field to search for preferences that contain certain words. For instance, if you're looking for the homepage URL setting, just type homepage in the filter field.
For more info on preference names, and `about:config' see http://kb.mozillazine.org/About:config

Creating A Lockdown Configuration File

Create a new file called lockdown.txt. Open lockdown.txt in a text editor (Notepad/Text Editor), and begin the first line with two forward slashes. The following lines will contain the preferences you want to lock, and their values. They should be in the same form as you see them in your profile's prefs.js file, with one exception:

- Instead of using user_pref, use lockPref.

For instance, if you want to lock the homepage at http://www.portcullis-security.com, the contents of your lockdown.txt file would look like this:

```
//
lockPref("browser.startup.homepage", "http://www.portcullis-security.com/");
```

The file must be encoded, and renamed. The encoding is a simple method known as `byte-shifting' with an offset of 13. You can use the attached Perl program moz-byteshift.pl (see Appendix A), or use an online encoder (http://www.alain.knaff.lu/~aknaff/howto/MozillaCustomization/cgi/byteshf.cgi).

The output should be saved in a file called lockdown.cfg. Copy the file to the same directory as firefox.exe.

Finally edit the following file

- C:\Program Files\Mozilla Firefox\greprefs\all.js.

At the end of the file add the following line:

```
pref("general.config.filename", "lockdown.cfg");
```

Save and close, your changes will then be in effect the next time Firefox is launched.

At the end of this guide is a list of categories with suggested keys and values, which should be used to secure Firefox.

Remove the Tools & Help Menu Items

Open "C:\Program Files\Mozilla Firefox\defaults\profile\chrome\userChrome-example.css" in a text editor.

Add (at the end):

```
/* Remove the Edit and Help menus
Id's for all top-level menus:
file-menu, edit-menu, view-menu, go-menu, bookmarks-menu, tools-menu, helpMenu */
helpMenu, tools-menu {    display: none !important; }
```

This will remove the `Help and Tool' menus.

Save the file as `userChrome.css'.

Removing Search Engines

Open `C:\Program Files\Mozilla Firefox\Searchplugins\'. Delete the .xml for the engines you do not want

E.g.

```
eBay.xml
amazondotcom.xml
```

Restricting Access to Local Drives

Open `C:\Program Files\Mozilla Firefox\Chrome\Browser.jar' in a zip program.

- Browse to `content\browser' and extract `Browser.js';
- Open `Browser.js' in a text editor.

NB: *Notepad loses the formatting, so open `Browser.js' in WordPad*

Locate the lines:

```
var location = aLocationURI ? aLocationURI.spec : "";
this._hostChanged = true;
```

Add (below the above lines):

```
if (location.match(/^file:/) ||
location.match(/^\//) ||
location.match(/^resource:/) ||
(!location.match(/^about:blank/) &&
location.match(/^about:/))) {
loadURI("about:blank");
}
```

Save `Browser.js' and copy back into `Browser.jar' in the zip program and save `Browser.jar'.

This should now load a blank page when you try to go to a `about:*' page, try opening `file:/ / /C:/' and also `C:'.

Lockdown Categories, Keys And Suggested Values

Browser.*

browser. chrome. favicons	Boolean	False: Prevent loading of favicons. *Note: This should be set to the same value as browser.chrome.site_icons for legacy reasons.*
browser. chrome. site_icons	Boolean	False *Note: This should be set to the same value as browser.chrome.favicons for legacy reasons.*
browser. download. hide_plugins_without_extensions	Boolean	True (default): In the Download Actions dialog, remove entries where no file extensions are associated with a plugin.
browser. download. manager. scanWhenDone	Boolean	True (default): Scan files for viruses when they finish downloading
browser. download. manager. skipWinSecurityPolicyChecks	Boolean	False: (default) Use Windows' security setting for executable file downloads ("Launching applications and unsafe files" setting in Internet Options). This blocks executable file downloads if the Windows setting is set to "Disable".
browser. fixup. alternate. prefix	String	The prefix to prepend when attempting to fix an entered URL. Default is "www." (includes full stop). Requires browser.fixup.alternate.enabled be true.
browser. fixup. alternate. suffix	String	The suffix to append when attempting to fix an entered URL. Default is ".com". Requires browser.fixup.alternate.enabled be true.
browser. fixup. hide_user_pass	Boolean	True (default): When attempting to fix an entered URL, do not fix an entered password along with it (i.e. do not turn http://user:password@foo into http://user:password@(prefix)foo(suffix) but instead http://user@(prefix)foo(suffix))
browser.fixup.alternate.enabled	Boolean	TRUE
browser. formfill. enable	Boolean	False : Stop data being stored in web page forms and search bar
browser. frames. enabled	Boolean	False : Disable frames.
browser. goBrowsing. enabled	Boolean	False: Stop google.com acting as DNS Server
browser. safebrowsing. enabled	Boolean	Whether to determine if a site is a web forgery or not. True (default)

DOM.*

dom. disable_image_src_set	Boolean	False : Prevent scripts changing images
dom. allow_scripts_to_close_windows	Boolean	False(default): Prevent scripts closing windows
dom. disable_open_during_load	Boolean	Determines popup blocker behaviour True (default in Firefox): Block popup windows created while the page is loading

Extensions.*

extensions. disabledObsolete	Boolean	True : Disable plugins no longer used.
extensions. dss. enabled	Boolean	False(default) : Prevent browser theme switching
extensions. update. autoUpdate	Boolean	True: Automatically update extensions

General.*

general. useragent. security	String	U (default): Strong security

Network.*

network. security. ports. banned	String	A comma-separated list of port numbers to disable in addition to the ports already disabled by default.
network. standard-url. escape-utf8	String	Determines whether URLs with UTF-8 characters are escaped per the spec True (default): Escape UTF-8 characters
network. dns. disableIPv6	Boolean	False (default) : Prevent Ipv6 name lookups
network. dns. ipv4OnlyDomains	String	A comma delimited list of valid DNS Servers
network. enablePad	Boolean	True: enable Proxy auto-Discovery
network. ftp. anonymous_password	String	Hardset the anonymous ftp password
network. http. accept-encoding	String	Comma delimited list of accepted encodings
network. http. accept. default	String	Comma delimited list of accepted MIME encodings
network. http. redirection-limit	Integer	5 : limit the number of consecutive redirects
network. http. sendRefererHeader	Integer	0 : Never send referer header over HTTP
network. image. imageBehavior	Integer	1: Load images from same (originating) server only
network. ntlm. send-lm-response	Boolean	Determines whether or not the LM hash will be included in response to a NTLM challenge. Servers should almost never need the LM hash, and the LM hash is what makes NTLM authentication less secure. False (default)
network. prefetch-next	Boolean	Determines whether to use link prefetching. False
network. automatic-ntlm-auth. allow-proxies	Boolean	Enable automatic use of the operating system's NTLM implementation to silently authenticate the user with their Windows domain logon with proxy servers. False: Prompt for authentication
network. automatic-ntlm-auth. trusted-uris	String	A comma-and-space-delimited list of URIs with which to automatically authenticate via NTLM (Windows domain logon). Default value is an empty string.
network. proxy. autoconfig_url	String	The automatic proxy configuration URL used by the browser to determine a proxy server. Used when network.proxy.type is 2. Default value is an empty string.
network. proxy. failover_timeout	Integer	Determines how long to wait until re-contacting an unresponsive

		proxy server. Default value is 1800 (30 minutes).
network. proxy. (protocol)	String	A manually configured proxy for the given protocol. Default value is an empty string.
network. proxy. (protocol)_port	Integer	The port for the manually configured proxy for the given protocol. Used when network.proxy.type is 1.
network. proxy. no_proxies_on	String	A comma-and-space-delimited list of hosts for which the specified proxies should not be used.
network. proxy. share_proxy_settings	Boolean	Determines whether to use the same proxy server for all protocols. False (Default)
network. proxy. socks_remote_dns	Boolean	False (default): Perform all DNS lookups client-side
network. proxy. socks_version	Integer	Determines which version of SOCKS to use with the server specified in network.proxy.socks. Default value is 5. (The only other valid version is 4.)
network. proxy. type	Integer	Determines how the browser uses proxies. 0 (default): Direct connection to the Internet (no proxy used) 1: Manual proxy configuration (use values in network.proxy.*) 2: Auto-configuration by URL (use value in network.proxy.autoconfig_url) 4: Auto-detect proxy settings for this network

Privacy.*

privacy. popups. policy	Integer	Determines the popup blocker behaviour. 2: Reject popups

Plugins.*

plugin. default_plugin_disabled	Boolean	False: Don't prompt the user to install needed plugins

Security.*

security. enable_java	Boolean	False : Java is disabled
security. enable_ssl2	Boolean	False : SSL version 2 is disabled
security. checkloaduri	Boolean	Determines how to handle access across schemes (e.g., loading file: URLs from http: URLs) True (default): Perform security checks and block access for insecure access
security.fileuri.strict_origin_policy	Boolean	True : Local documents have access to other local documents in the same directory and in subdirectories, but not directory listings. (Default)
security. ssl2.(cipher suite)	Boolean	False : Disable weak ciphers
security. xpconnect. plugin. unrestricted	Boolean	Allow scripting of plugins by untrusted scripts False

Signon.*

signon. prefillForms	Boolean	False : Prevent auto filling web forms

Startup.*

Startup.homepage_override_url	String	Enter your homepage.
Startup.homepage_welcome_url	String	Enter your homepage.

Update.*

update. severity	Integer	2: High severity updates available (new version of Firefox/security patch)

View_Source.*

view_source. editor. external	Boolean	False : Use internal viewer

XPInstall.*

xpinstall. enabled	Boolean	False : Prevent plugins being installed
xpinstall. whitelist. add	String	A comma-separated list of sites to automatically add to the extensions whitelist. Default value is update.mozilla.org,addons.mozilla.org but is cleared as soon as the values are added to the whitelist
xpinstall. whitelist. required	Boolean	True (default): When installing extensions from remote hosts, remote host must be on the whitelist

Miscellaneous

application. use_ns_plugin_finder	Boolean	False (default): Clicking on the puzzle piece will send the user to that plugin's page on plugins.netscape.com which will have a link to that plugin's installation page.
clipboard. autocopy	Boolean	False : Prevent auto-copying contents to clipboard

Appendix A

moz-byteshift.pl

```
#!/usr/bin/perl

# Byteshifting program for mozilla's *.cfg files

# Mozilla uses a byteshift of 13
#   To decode: moz-byteshift.pl -s -13 <netscape.cfg >netscape.cfg.txt
#   To encode: moz-byteshift.pl -s  13 <netscape.cfg.txt >netscape.cfg

# To activate the netscape.cfg file, place the encoded netscape.cfg file
# into your C:\Program Files\Mozilla Firefox directory.
# Then add the following line to your
# C:\Program FilesMozilla Firefox\defaults\greprefs\all.js file :
# pref("general.config.filename", "mozilla.cfg");

use encoding 'latin1';
use strict;
use Getopt::Std;

use vars qw/$opt_s/;

getopts("s:");
if(!defined $opt_s) {
        die "Missing shift\n";
}

my $buffer;
while(1) {
        binmode(STDIN, ":raw");
        my $n=sysread STDIN, $buffer, 1;
        if($n == 0) {
                last;
        }
        my $byte = unpack("c", $buffer);
        $byte += 512 + $opt_s;
        $buffer = pack("c", $byte);
        binmode(STDOUT, ":raw");
        syswrite STDOUT, $buffer, 1;
}
#End Of File
```