SecBrowser

FREE

SecBrowser ™ is a security-focused browser that provides better protection from exploits, thereby reducing the risk of infection from malicious, arbitrary code. A built-in security slider provides enhanced usability, as website features which increase the attack surface (like JavaScript) can be easily disabled. Since many of the features that are commonly exploited in browsers are disabled by default, SecBrowser ™'s attack surface is greatly reduced. Without any customization, SecBrowser ™'s default configuration offers better security than Firefox, Google Chrome or Microsoft Edge.[1] It also provides better protections from online tracking, fingerprinting and the linkability of activities across different websites.

SecBrowser ™ is a derivative of the Tor Browser Bundle (which itself is a derivative of Mozilla Firefox) but without Tor. This means unlike Tor Browser, SecBrowser ™ does *not* route traffic over the Tor network; in common parlance, this is referred to as "clearnet" traffic. Even without the aid of the Tor network, SecBrowser ™ still benefits from the numerous patches that Tor developers have merged into the code base. Even with developer skills, these enhancements would be arduous and time-consuming to duplicate in other browsers, with the outcome unlikely to match SecBrowser ™'s many security benefits. While browser extensions can be installed to mitigate specific attack vectors, this ad hoc approach is insufficient. SecBrowser ™ leverages the experience and knowledge of skilled Tor Project developers, and the battle-tested Tor Browser.

Table: *SecBrowser ™ Security and Privacy Benefits*

Feature	Description
Default Tor Browser Add-ons	• HTTPS Everywhere: This browser extension encrypts communications with many major websites, making your browsing more secure.[2] • NoScript: NoScript can provide significant protection with the correct configuration.[3] NoScript blocks active (executable) web content and protects against cross-site scripting (XSS). "The add-on also offers specific countermeasures against security exploits".
DNS and Proxy Configuration Obedience	Proxy obedience is achieved through custom patches, Firefox proxy settings, and build flags. Plugins which can bypass proxy setting are disabled.[4]
Reproducible Builds	Build security is achieved through a reproducible build process that enables anyone to produce byte-for-byte identical binaries to the ones the Tor Project releases.[5][6]
Security Slider	Enables improved security by disabling certain web features that can be used as attack vectors.[7] [4]

WebRTC Disabled by Default	WebRTC can compromise the security of VPN tunnels, by exposing the external (real) IP address of a user.[8][9]
Firejail (Linux only) (testers repository only)	... [10]

Research from a pool of 500,000 Internet users has shown that the vast majority (84%) have unique browser configurations and version information which makes them trackable across the Internet. When Java or Flash is installed, this figures rises to 94%.[11] SecBrowser ™ shares the fingerprint with around three million other Tor Browser users, which allows people who use SecBrowser ™ to "blend in" with the larger population and better protect their privacy.

The EFF has found that while most browsers are uniquely fingerprintable, resistance is afforded via four methods:

- Disabling JavaScript with tools like NoScript.
- Use of Torbutton, which is bundled with SecBrowser ™ and enabled by default.
- Use of mobile devices like Android and iPhone.
- Corporate desktop machines which are clones of one another.

With JavaScript disabled, SecBrowser ™ provides significant resistance to browser fingerprinting.[12]

- The User Agent is uniform for all Torbutton users.
- Plugins are blocked.
- The screen resolution is rounded down to 50 pixel multiples.
- The timezone is set to GMT.
- DOM Storage is cleared and disabled.

The EFF's Panopticlick fingerprint test shows that SecBrowser ™ resists fingerprinting.

Note: Because tracking techniques are complex, Panopticlick does not measure all forms of tracking and protection.

- SecBrowser ™ conveys 6.26 bits of identifying information.
- One in 76.46 browsers having the same fingerprint.
- Browser's that convey lower bits of identification are better at resisting fingerprinting.[13]

When Tor Browser's and SecBrowser ™'s HTTP headers are compared using Fingerprint central's test suite the results are near identical.

Table: *Tor Browser vs SecBrowser ™ HTTP headers comparison.*

Percentage (%) out of 1652 with fingerprints tags [Firefox,Windows]:

Name	Value	TorBrowser %	SecBrowser™ %
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101	2.48	2.42

	Firefox/60.0		
Accept	text/html,application /xhtml+xml,application /xml;q=0.9,*/*;q=0.8	97.15	97.15
Host	fpcentral.irisa.fr	90.44	90.43
Content-Length		100.00	100.00
Accepted-Language	en-US,en;q=0.5	32.63	32.95
Referer	https://fpcentral.irisa.fr/	69.37	69.35
Upgrade-Insecure-Requests	1	83.05	83.04
Accepting-Encoding	gzip, deflate, br	82.14	82.13
Content-Type		100.00	100.00
Connection	close	100.00	100.00

SecBrowser ™ is compatible with many popular platforms such as Microsoft Windows, Debian Linux and the highly anticipated Kicksecure, which is a security-hardened, non-anonymous Linux Distribution *(coming soon!)*. This provides convenience for a broad user base due to cross-platform availability:

- SecBrowser ™ in Kicksecure ™ and Debian
- SecBrowser ™ in Qubes OS
- SecBrowser ™ in Microsoft Windows
- SecBrowser ™ in macOS

SecBrowser ™ is a derivative of Tor® Browser, produced independently from the Tor® anonymity software and carries no guarantee from The Tor® Project about quality, suitability or anything else.

No comments for now due to spam. Use Whonix forums instead.

https | (forcing) onion

Follow: Twitter | Facebook | gab.ai | Stay Tuned | Whonix News

Share: Twitter | Facebook

This is a wiki. Want to improve this page? Help is welcome and volunteer contributions are happily considered! Read, understand and agree to Conditions for Contributions to Whonix ™, then Edit! Edits are held for moderation.