Packages - Packaging Request #874

Packaging Request # 2165 (open): [Iceweasel-UXP] and other potential iceweasel replacements

[tor-browser] add package for PCR

2015-11-24 09:15 PM - totalchaos

Status:	open	**% Done:**	0%
Priority:	wish		
Assignee:			
Category:			

Description

Tor Browser Bundle: Anonymous browsing using Firefox and Tor
I guess it will be a crucial part of Parabola's nonprism suite, thus making Parabola the logical choice for users, that value their privacy.
https://www.torproject.org/projects/torbrowser.html.en

History

#1 - 2015-11-24 09:41 PM - GNUtoo

There are several issues to handle here:

- Is tor-browser suggesting non-free software with "get add-ons"?
  - The tor-browser and Tor project suggest not to install any add-ons (reference needed), this is to prevent the user's browser from looking different and unique
  - We should probably try to disable that feature instead. But we should be very careful at not changing how the modified tor-browser looks on the internet, else it becomes dangerous and useless (you will be uniquely identified). We probably need to check that with tor-browser developers, and make them review the change.
- Since there is this add-on issue, we can't use stock tor-browser for now, which is really problematic, we loose:
  - Reproducible builds
  - The possibility not to make a tor-browser-libre package but instead a tor-browser installer. This would have been desirable because it has a nice auto-update feature. You also would get a reproducible build.

#2 - 2015-11-24 11:39 PM - pizzaiolo

I think your first point could be suggested upstream at the Tor Project, that would be a very good idea.

#3 - 2016-01-18 08:10 PM - Anonymous

- Subject changed from tor-browser to [tor-browser] add package for PCR

#4 - 2016-09-26 08:32 PM - GNUtoo

I've made some research but forgot to report back:
The add-on page can be changed in about:config.

However extra care must be taken not to make a tor-browser-libre distinguishable from the tor-browser.
Some information about plugins updates can be found in the following (fixed) security bug: http://seclists.org/dailydave/2016/q3/51

#5 - 2018-06-01 02:01 PM - GNUtoo

See also the same bug for another FSDG compliant distribution: https://tracker.pureos.net/T343

#6 - 2018-07-19 03:00 AM - ovruni

- Priority changed from bug to wish

#7 - 2019-12-11 11:36 PM - GNUtoo

Here are some pointers to the status of this issue:

- The following wiki page has information on the status of the tor-browser port to other architectures (arm and ppc64le)
- The following bug report has information on getting rid of the add-on repository.

Thanks to Jeremy Rand for working on both.

#8 - 2019-12-12 04:11 AM - bill-auger

the auto-update feature makes this program not well fit for any distro - every program that i know of, which has such a feature, has it disabled in parabola builds - this is effectively a "back-door" feature, which is explicitly prohibited by the FSDG; and i beleive that is why parabola has always removed it from all applications

there is hardly any reason to package any program with with an auto-update feature - anyone who installs the package would only be using the packaged build until the next auto-update (like maybe the very next day in this case); and then will be using the upstream binary from then on - one really may just as well get the upstream binary in the first place, saving us the trouble of maintaining yet another mozilla beast

#9 - 2022-04-13 05:28 PM - gap

GNUtoo

Please may I submit my wish for this? Since torbrowser-launcher was blacklisted today I no longer have a web browser which is safe to use over Tor.
Needless to say, I never utilised the Mozilla repo with nonfree addons in it.

Would the existing Iceweasel patchset be helpful to liberate the Tor Browser?

#10 - 2022-04-21 04:01 AM - bill-auger

gap - read my last comment above - i think you are better off using the ones that tor people build

OTOH, you could install tor on your computer and 'torify' any program

i can add that there is one other huge factor impeding the progress of this ticket - that is, all of the same arguments against #2165 - mozilla software is a huge maintenance burden

#11 - 2022-05-05 11:52 PM - gap

The issue with Torification is that not everything is safe to Torify, IIRC, without modifying it to act in a less identifiable way.
The Tor Browser and Torifiable programs have been designed to work safely over Tor.
In this way, merely Torifying Iceweasel (or any other browser) wouldn't be as safe as the Tor Browser.

I wouldn't want to use the binary directly from the Tor Project for several reasons:
1. Self-updating programs are a nightmare and all updating should be handled by the system package manager.
2. It is not compliant with the GNU FSDG.
3. The build environment of the Tor Project is almost certainly different to that of the Parabola build server, so dependencies and libraries might be different, potentially incompatible versions.
4. There are all these redundant faux-universal package formats to deal with (eg. AppImage) and I don't want to have to deal with a TPPM, so I'd probably end up waiting hours for it to compile from a sourceball.

I lived with issues 1, 2, and 3, whilst using torbrowser-launcher, and a native package would be much better.
The AUR package has issues 1 and 2, assuming the user builds it locally, so it could be a starting point for a -libre package.

At the moment I am relatively busy and have enough time only to submit issue reports and discuss issues, but I might volunteer to maintain a tor-browser package, if the patch set from Iceweasel is manageable.
I'd be willing to learn how to package such complex software and Parabola's policies regarding packaging, but I would probably start off contributing to smaller bugfixes in the blacklist first.

#12 - 2022-10-10 09:22 PM - bill-auger

- Parent task set to #2165

#13 - 2023-12-29 11:38 PM - GNUtoo

Guix now has a package for the tor-browser and also patched it along the way to use gnuzilla.gnu.org for the addons search. So the way to go is probably to somehow do something similar in Parabola.

#14 - 2023-12-30 01:52 AM - bill-auger

i am still against this - there are several reasons why this program should not be in any distro - i believe they were already discussed on this ticket and the related ones; but i will reiterate

the program is designed to replace it's own binary automatically upon launch; and that is the recommended way to use it - among its primary privacy features is to thwart fingerprinting, which depends on every user of that program using the identical build at all times - every user using a stray version forfeits anti-fingerprinting - that is why for this program (and i can think of no other), auto-upgrade is an important feature and it should always be done immediately upon each upstream release, otherwise the user is misusing the tool - distros would need to compile and publish new packages immediately upon each upstream release, in order to retain its anti-fingerprinting properties (and i mean *immediately*, within a few hours)

however, from the perspective of a distro, auto-upgrade behavior is a back-door vulnerability - not only should distros avoid giving back-doors to their users, the auto-upgrade mechanism inherently defeats the purpose of why distros exist in the first place

any distro package of an automatic self-updating binary, may as well be exactly this:

```
$!/bin/bash
curl upstream.com/download/replacement-for-this-script > $0
$0 &
```

ignoring that it is a back-door, anyone who would be happy with that package, clearly did not need the distro package in the first place

"back-doors" are explicitly forbidden by the FSDG - if guix did not disable that feature, then their package is FSDG-unfit - if they did disable it, but they do not publish a new package within a few hours of each and every upstream release, then they are giving their users a version of that tool which is prone to fail in its primary "value-added" fork characteristic, that which is the only reason why anyone would want to use it instead of firefox or any other web browser

aside from that, even one of the necessary FSDG treatments (disable EME) decreases its anonymity by many orders of magnitude - just to illustrate, i read just today, that only 3% of web browsers in use today are derived from mozilla - tor-browser is a minuscule fraction of those; and tor-browser with EME disabled would be a minuscule fraction of tor-browsers - in fact, *any* web browser without EME is relatively fingerprintable - that literally implies that no FSDG distro can distribute a web browser which offers a high degree of non-fingerprint-ablity - we should not fool ourselves nor our users about that fact

myself, i must decline to maintain this program for parabola; and i would not like to see it in parabola if done half-assed, even if someone else volunteers - i believe that it is naiive to even try to maintain this properly to the FSDG standards; and that is presuming that it would need no extra patches in [nonprism] - if the version becomes even one day behind, it betrays the users' trust by by putting them at risk, the very same risk against which the software exists to protect, and the only reason why people use it in the first place - i would not want to automate it either; because then users would be using something that is never tested - at the very least, parabola's privacy respecting channel [nonprism] would need to block it's installation, quite ironically given this application's reputation and "raison d'être"

in short, it is not worth the effort for anyone other than the upstream to maintain tor-browser properly - and it is also risky - even if you try to rebuild it on the same day as the upstream release, there is no guarantee that it will actually compile that day on a rolling distro (or on any distro, other than the precise environment that the upstream used) - if that happens even once (and it surely will happen some day), all users are fingerprinting targets until it does compile again and is published, then some time later, the package finally propagates across the mirror network

#15 - 2023-12-30 08:03 PM - bill-auger

another serious point came to mind today, which is very relevant

note that GNU icecat is also maintained by guix - icecat has been presented as 'beta' for four years (for as long as guix has been maintaining it), because according to the maintainer, it is not maintained well enough to meet GNU standards - more importantly for tor-browser, icecat typically lags several months behind upstream - months, not hours

seeing how sluggishly icecat is maintained, how could anyone believe that guix can maintain another mozilla browser in addition to icecat, one which would need most or all of icecat's FSDG treatments, yet maintain it well enough to get releases out on the same day as the upstream - i would not daresay to suggest this to parabola's iceweasel maintainer; as the suggestion would be ridiculous - tor-browser is the only software which i would suggest (and i would suggest it strongly) that people should use only the upstream binary build - ie: people really should *not* modify this software, if they expect to trust the result for its intended use-case; but FSDG distros *must* modify it, else reject it entirely

my every intuition tells me that they can not possibly maintain tor-browser adequately, even if icecat were abandoned and all effort on icecat were shifted to tor-browser - i dont believe that any distro could; unless the build was fully-automated, such that they do not ever inspect the changes before releasing, nor patch it in any way, and it is built in the identical environment as the upstream

lastly, as built-in tor support has recently been removed from icecat, if guix were sincere about this, they should propose that it *becomes* "GNU icecat", that is, an official GNU fork of tor-browser which would replace icecat entirely - tor-browser *must* be maintained better than icecat is now; and as a GNU project, guix should not want to maintain *any* web browser better than GNU's flagship web browser: icecat is maintained - but then, under the light of scrutiny, it would be more obvious to people, that it would need *far* more effort than GNU/guix is currently allocating to icecat, even if it were feasible to get releases out quickly enough to preserve the tor-browser application's primary value, which i contend is not feasible - icecat in its current form, can endure a sluggish release cycle; because the application's primary value does not depend on such a tight release schedule - the time-window within which to inspect the changes and ensure that releases meet the same standards that icecat is admittedly failing to meet now, is prohibitively small for tor-browser