Packages - Housekeeping #2626

Privacy Issue # 2619 (in progress): Refactor [nonprism]

Create a consice requirement specification for packages in "your-privacy"

2020-02-07 03:17 PM - theova

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

Description

Freemor wrote on the mailing list:

> One thing that is needed [...] create a clear, concise, idea of what should be in
> "privacy-enhanced". By which I'm not meaning actual package but a set of
> guidelines. a la "Things that remove tracking/dialing home". And also what
> kinds of things should not be included because they fall under the umbrella of
> security (we should probably think about a "Security-enhanced" down the road),
> or should be in libre, etc.

As a comparison [1]:

> The [libre] repository contains four things
> - Replacements for packages in Arch's [core] that were blacklisted
> - Replacements for packages in Arch's [extra] that were blacklisted
> - Replacements for packages in Arch's [community] that were blacklisted
> - Packages produced entirely by Parabola that are deemed to be core packages (and their build dependencies)

Today, [nonprism] contains:
- Replacments for packages which need geolocation (see #2621)
- Replacments for packages which need libgdata (see #2622)
- Replacemts for packages which provide the us of "privacy-unfriendly" services (see #2623)
- Replacement for packages which I am not quite sure, what is patched (see #2624)
- Hardened packages (see #2625)

[1]: https://wiki.parabola.nu/Official_Repositories#.5Blibre.5D

Subtasks:

Privacy Issue # 2622: Reevaluate libgdata and/or its dependents	**info needed**
Privacy Issue # 2623: Re-evaluate nonprism-packages which remove addon or access to non...	**confirmed**
Privacy Issue # 2624: Re-evaluate packages in nonprism with unkown problems	**confirmed**
Privacy Issue # 2625: Re-evaluate [nonprism] hardened packages	**confirmed**

History

#1 - 2020-02-13 10:38 AM - theova

Starting a first trial:
[Privacy enhanced] contains:

1. Packages with hardened settings which changes the use of the programm fundamentally
2. Packages which blacklist privacy-unfriendly packages (e.g. your-privacy)
3. Replacement for packages blacklisted in "your-privacy".

To the first point: I think, that changing e.g. the search engine of a browser should be done for all users and therefore in the package should be in libre/pcr. This does not change the use of the programm. By having it in libre/pcr we can reduce the maintanence work load.
But a patched geolocation service changes the use of the programm fundamentally and therefore it should be in [privacy enhanced].

I think the question is: what should be blacklisted?
Blacklisting all packages which have the *possibility* to connect to a surveillance service (google, ...) targets on a simple user who don't have an idea which services are bad.
Replacing such packages (eg. gnome-online-accounts) increases the maintanence workload without adding to much functionality. Having no google account is a simple, individual countermeasurement.

To address the "simple user", we could have an additional blacklist ("no-surveillance-services", or a better name?) which blacklists all package which *could* connect to surveillance services.

your-privacy should blacklist:

- Packages with anti-privacy-features which are needed to use the package.
- Packages with anti-privacy-features which are hidden to use the package.

#2 - 2020-02-13 12:46 PM - freemor

I like the direction of your thinking.. "Blacklist 'em All". But creating a meaningful blacklist that catches all "Evil" applications is a Sisyphean task. As Amazon is know to be part of Prism/etc this would require blacklisting anything that uses AWS or EC as a back end. Also any program who's backed is behind CloudFlare. (Even if CloudFlare isn't actively part of such spying you have to believe that they have been "downstreamed" as they are the largest MiTM on the Internet.). The we have FB (annd all of its part), Yahoo (and all of its part) Anything backed by Microsoft Cloud services, and on and on.

The easiest way to do this would be blacklist everything net enabled and then start unblacklisting things proven safe.

The above is one of the reasons I wanted to move away from the whole nonprism thing. Because realistically we'd have to replace all major browsers and webengines with ones with the JS engines completely removed as almost every site has tracking JS bits often but not always tied back to GAFAM. Getting out from under surveillance these days requires a huge, constant, educated, shift in user behaviour. Without that all the blaclisting and tweaking in the world wont help because people will convince themselves that undoing just a few of the protections is OK, because they gotta have their Vids, or Social thing, or cause site X is broken without JS or because 60% of the internet disappears if you block CloudFlare. etc.

It would have to be a blacklist and educate approach.

Also the surveillance blacklist should probably be split into Surveillance-Capitalism and Surveillance-Gov. Tho the Venn diagram of those two has a large intersection.

And if we are worried about Surveillance-Gov. How do we protect from things like Great Firewall of China, GCHQ, All the crap going on in Australia with spying on and blocking the internet, etc. Makes no sense just to worry about one or two as at lest 5 of them share info to dance around domestic spying laws I.e. GCHQ will gladly spy on US citizens and then share the data with NSA (so their hands are clean).

In the end probably the best we can aim for is to reduce the amount of data leaked. But as I said in the initial refactoring post. Stopping Surveillance-Gov
is outside the range of what we can do. Tho it'd be interesting to create the blacklist (no JS enabled browsers, Nothing with GAFAM back end, an iptables
blocklist of GAFAM services and CloudFlare, nothing geolocating, nothing with telemetry, etc.) and see just what we are actually left with as a starting point.

Realistically this is the domain of Heads/Tails etc where the entire focus of the distro is reducing exposure. And even they caved and turned JS on by default
as too much of the web is so badly written as to require it. (side note: I really wish people would remember that it is Hyper TEXT Transfer Protocol and not
Javascript Transfer Protocol).

That all came out more negative sounding then I intended. Please hear it as "Great idea!", "Dammmmn! thats gonna be a harsh blacklist."

#3 - 2020-02-15 09:27 AM - bill-auger

it is easy to evolve into absurdity, when addressing privacy concerns with technical solutions - by default, every program running on the system could "potentially" access the network; naturally, they all could "potentially" make unsupervised connections - there are standard tools to observe and control access to the network, and which hosts are allowed - the privacy repo offers some one-size-fits-all configurations, as a matter of convenience; but those are necessarily very narrow in scope - it can not possibly cover everything

i propose this as the following is the most precise explanation for the what the privacy repo should address

- the FSDG prohibits malware or anti-features - that is, anything which some program does unsupervised, which the user has no particular use for, and has no obvious way to detect, observe, or control it

- everything in the [nonprism/privacy] repo is either a privacy-enhanced build of, or a privacy-enhanced configuration for, some package that is in some other repo

- so nothing in the [privacy] repo should remove malware from some package that is in another parabola repo - doing so, would imply that the counterpart does not meet the FSDG

geo-location is the clearest example of why a privacy-enhanced repo exists - it has privacy implications, and we want to identify those; but it is not malware, because some people have an intentional use for it - for that reason, we would not want to remove all possibility of geo-location functionality from the entire system - IMHO, everything in the privacy-enhanced repo should be of that sort: extra privacy, beyond the FSDG requirements

the only reason that geo-location needs to be handled in [privacy], is because programs that use it, do not provide a simple on/off switch for it's network access - probably, those devs blindly assume that it is a universally valuable feature, which no one would want to disable; and most likely because too few people bothered to complain about it - the parabola privacy repo is merely recognizing that malware is a subjective distinction, according to the use-cases of each user, and offering the options for each user to decide

iceweasel for example, has many easily installable and user-friendly add-ons for blocking unwanted connections; so that concern does not need to be handled in [privacy] - the [privacy] repo only needs to address privacy-related features which are FSDG-fit, but which the standard build does not have a simple way to control it, and therefore a special and separate build is required

i.e. if we made a tool to easily control network access by the geo-location libraries, then only that tool would need to be in [privacy] - the main programs could be built only once per arch in [libre] (or less than once for non-blacklisted packages) - if every privacy concern could be solved in a similar way, then there would be no need for any special privacy repo - all of those config helpers could be available by default in [pcr]

conversely, we could eliminate the [privacy] repo by enabling all of its magic globally, essentially removing FSDG-fit functionality from the distro - that is the same as if we built icecat, such that it ware incapable of executing javascript - we would not want remove the geo-location libraries globally, nor any other any features which are within the FSDG - maybe ive gone too long-winded about this; but that seems to be what this discussion is suggesting, as a way to reduce the workload - if reducing the workload were the primary factor, that could be achieved to a greater degree by deleting everything in [nonprism] and doing nothing more than what the FSDG requires

the very reason that the [nopnrism] repo is separate and not the default, and why a separate build is required in some cases, is to provide some privacy-enhancements, while retaining maximal user-choice, within the FSDG - it is the same reason for maintaining multiple init-systems - the FSDG does not require "init freedom" - these things do increase the workload; but we dont want to be removing functionality from the distro or impeding configurability, if only to reduce the workload, or to impose subjective ethical criteria upon all parabola users

we are not trying to make a pre-configured system like heads/tails - parabola is primarily a DIY system - we really would rather spend time teaching people to how to fish, rather than concocting and peddling our own brand of free frozen fish-sticks - anything like: "here, let me do that for you" or "trust us, we know whats best for you", pretty much disqualifies an arch-like distro from being arch-like, doesnt it? - i make an exception for the user-friendly installer; because that eases new people onto the boat - from then on though, we do hope that they are willing to learn how to fish

that was just a flowery way of agreeing with freemor - people with wise networking habits, need to be far less concerned about privacy than others; and distros can do relatively little of practical significance, which would suit any one user perfectly, and avoid constraining others

the real solutions are learning to observe and control ones
network and exercising self-discipline over ones networked
computer habits - it is quite analogous to learning to watch
ones weight and to exercise self-discipline over ones eating
habits, for a person who wants to lose weight - everyone's
situation is unique; and all the nutrition experts and yoga
instructors in the world can be no more than guides - in
the same way, managing ones computer privacy depends
predominantly on the active discipline of each computer user

#4 - 2020-02-19 08:17 PM - theova

I totally agree with you.

I was wondering what other FSF endorsed OS do. So I asked the purism about what PureOS (focused on privacy) is doing.
Here is the reply: https://forums.puri.sm/t/privacy-on-package-level/8599/1

In short: They patch the browser and remove non-free packages.

#5 - 2020-02-19 09:59 PM - freemor

I think we are getting close.

I wanted something simple and consice as the guiding principal(s) of [privacy-enhanced]

So I'm thinking something like this:

privacy-enhanced is a repo containing sofware that is tweaked beyond the requirements of FSDG (as those would all live in Libre).
They are seperate because these packages will break/remove things which many users would consider standard or desirable.

What we do:

- Remove leaks that more privacy conscious users would see a a bane rather then a boon. (geolocation, etc.)
- Hardened preferences, where hardening breaks users assumptions. (disabling JS, Forcing email to text only, etc)
- Provide a clear text document explaining what we changed and why. (Because you need to be informed to protect your privacy.)

What we don't do:

- Focus on protecting from Corporate or Government (NSA, CIA, CES) spying (beyond our scope and ability)

Thoughts?

Fixed the formatting (sorry about that)

#6 - 2020-03-09 02:37 PM - bill-auger

i would word it a bit differently; but the essential ideas are
complete and sound

im a bit out of touch with this one - this ticket is on the
"Packages" tracker; but the discussion seems to be more about
documentation

#7 - 2020-03-09 07:43 PM - theova

freemor wrote:

> So I'm thinking something like this:
> ...

For me this reflects quite good the discussion we had.

freemor wrote:

> What we don't do:
>
> - Focus on protecting from Corporate or Government (NSA, CIA, CES) spying (beyond our scope and ability)

... and thus not blacklist/patch packages which provide services like google & co. Right?

#8 - 2020-03-09 08:48 PM - freemor

<quote>

... and thus not blacklist/patch packages which provide services like google & co. Right?
</quote>

I think I get wat you are getting at here. I'b be fine blacklisting and patching.... If we stood a chance of making a difference.

I doubt people are willing to have us break their systems that badly.
Such as:

- Remove all JS engines from all browsers (Google anaylitics/Firebase/Double click/Etc.)
- Write hosts file /IPtables rules to block all things Google)
- Refuse to talk to their Android based Tablet or smartphone unless it is running Replicant

Then We'd have to add all the Facebook/Amazon/Microsoft/etc protections.
guess the quick way would be: ifdown <*>   :)

This isn't all or nothing thinking. this is not wanting to give people a false sense of "Oh I'm safe now" when really they are not.
Keeping people save from Corporate and/or Government spying requires a huge shift on the users part. If they aren't willing to make the shift to disengage themselves as much as possible. Then we really can't do it for them.

As soon as a user gets frustrated and turns JS back on just "Just a few sites" then are back to being tracked.

I'd rather we spend time and effort on places where we can actually make a difference. Like the neutered geoclue2
perhaps a config that ran all networked things under firejail to limit leakage of information from the system.

Now, I'm open to being persuaded that we can help useres be more safe (patch out GAFAM). If there is some why I'm not considering to
Change the "false sense of safe" part of it. Sadly, I've been around tech support too long and know that people will gladly disable
safety a,b,c because they just got use that one shiney webby thing.

Basically I guess I'm saying that if Cambridge Analytics and Snowden Revelations didn't change user behaviour in meaningful ways. Us patching this and that
it's gonna make a difference to their privacy.

#9 - 2020-03-09 08:57 PM - theova

I am fine with this. I just think it is important to get consense on this point.

#10 - 2020-03-10 10:27 AM - bill-auger

- Status changed from confirmed to open

- Tracker changed from Privacy Issue to Housekeeping

#11 - 2020-03-10 10:31 AM - bill-auger

also, i dont know if anything in the [nonprism] repo currently does attempt to globally block certain domains - im not sure if that ever was promised explicitly - i think freemor's main concern, and the reason for this discussion, was only that the repo name and documentation could be naively interpreted as such a magic solution to what is an unreasonably vague and broad perceived problem - such a global block is not even feasible - for starters, addressing that at the DNS level is insufficient - there would need to be a constantly maintained list of all IPs operated by foo-corp, goo-corp, and evil.gov; and that is assuming that all such IPs are known or knowable - it would be an undeliverable promise at best

even if that were feasible, as freemor pointed out, most people would not actually want it, even if they know they should; just as with librejs - even if it were feasible and people wanted it, simply enabling [nonprism] and installing 'your-privacy' would not accomplish it anyways, without a complete security audit of every program in the system; and/or a custom hosts file - not to mention that 99% of privacy leaks, happen when people download javascript in their web browser, and execute it without reading it first - to guard against that would be a very large, hosts file indeed, and a woefully unmaintainable one

there are legitimate reasons for a program to connect to third-party services (namely: those known by and potentially valuable to the user) - geo-location, weather reports, time sync are among those, as is every web browser - any other connections to third-parties could be considered as an anti-feature according to the FSDG; and those would need to be patched out in [libre] anyways

if some network service is the intended use-case for some program, then it is not a "leak" - it is a feature, which some people may value and others may not - the privacy-enhancing repo only needs to address unintended leakage from programs which use third-party services as a legitimate feature; such that if someone does not want geo-location, weather reports, or time sync, we could ensure that none of the installers install any programs which use those services by default, and only patched builds would be available, when the [privacy] repo is enabled, and none would be available when the 'your-privacy' package is installed to conflict with those which can not be patched

that arrangement would be more reasonably maintainable; and in full disclosure, that is probably what the [nonprism] actually is now in practice - for example, LXDE comes with a weather widget for the panel - the installers will install lxpanel by default; but the weather widget is not enabled by default - it is pre-installed however, and is available in the panel config GUI - though one could argue that enabling it is not unintentional; for the sake of example, there could be a privacy/lxpanel package which has the weather.so deleted; so that the privacy repo could be selected in the installer GUI at install time - i dont think we can reasonably do much more than that; and again, i dont think that the [nonprism] repo has ever accomplished any more than that practically, or was ever intended to

in conclusion, my point is that i dont see any drastic technical or policy change in this discussion - it is mainly about presenting, in the documentation, a more responsible disclosure regarding the scope of the promises that are made - if this discussion is not about a new package, or a change to an existing package, or a correction to the documentation, then it would be better on the mailing list, where more opinions could be accumulated, instead of buried on the packaging tracker where only a small few are discussing it

im being so verbose about this, not so much as information to those few of us who are reading this thread; but because the real solution is a thorough wiki article explaining what is practical for any distro to manage, and that knowledge and self-discipline must do the rest - so maybe some of this discussion can be distilled into a 'your-privacy' wiki article

side note: ill add this just so that it is not overlooked, in addition to the wiki documentation, the 'your-privacy' install hook has a user-facing message also

https://git.parabola.nu/abslibre.git/tree/nonprism/your-privacy/your-privacy.install