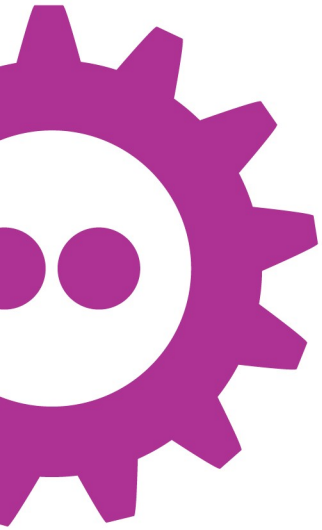
COLLABORA



Introduction to Flatpak

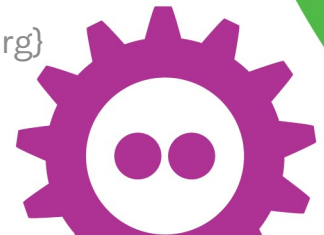
Sandboxed apps for desktop Linux

FOSDEM 18

Simon McVittie

smcv@{collabora.com,debian.org}

2018-02-03



COLLABORA

Introduction to Flatpak

- A sandboxed app framework for desktop Linux
- Formerly xdg-app
- Maintained by Alexander Larsson (Red Hat)
  - Contributors include people from Endless, Collabora, Red Hat, GNOME, Debian, Arch Linux, …
  - No CLA required to participate
- Yes, the name is an IKEA reference

COLLABORA

Sandboxed *app* framework for *desktop* Linux

- Application, as in `/usr/share/applications`
- Application, as in app store
- Platform services and infrastructure out of scope
  - Not for dconf, GNOME Shell, xterm, screensavers
- CLI tools also out of scope
  - Not for gcc, sed, Python, coreutils
- System services are way out of scope

COLLABORA

Sandboxed app framework for desktop Linux

- You trust an app enough to use it
  - This can only be as secure as your kernel
- You shouldn't have to trust an app so much that it can read `~/.gnupg`

COLLABORA

Sandboxed app framework *for desktop Linux*

- No attempt to be portable (sorry *BSD)
- Relies on Linux namespaces
  - Same building blocks as LXC, Docker, rkt, systemd-nspawn
- Expects some sort of desktop environment
  - Not specific to GNOME or KDE
- Does not require LSMs (AppArmor, SELinux)
- Does not require systemd (although it can help)

COLLABORA

Apps and runtimes

Fig.1. Flatpack providing a stable platform

Photo: Simon_sees, 2013. CC-BY-2.0

COLLABORA

The wonderful thing about standards...

- ISVs can't target “desktop Linux” like Windows, or macOS, or Android
- libjpeg 6.2 or libjpeg 8? Turbo or IJG?
- SDL 1 or 2 or both?
- GTK+ 2, 3 or 4? 3.14 or 3.22?
- GNOME or KDE Plasma or Unity or XFCE or LXDE or MATE or Cinnamon or LXQt or UKUI or Enlightenment or fvwm or Openbox?

COLLABORA

Can't we just assume ${ancient_platform}?

- Traditionally some ancient version of Red Hat
- LSB: vendor-neutral Linux baseline
  - Not actually amazingly useful
- More recently, Ubuntu gets used as the reference
- Steam officially requires Ubuntu 12.04, from 2012
  - EOL April 2017
- Disincentive for ISVs to improve the base platform

OK, can we bundle everything?

- Choose a baseline, bundle the rest
- Simplest case: static linking
  - Except for nss plugins
- `-rpath $ORIGIN/../lib`
- `LD_LIBRARY_PATH`
- Often a rather leaky abstraction

COLLABORA

Platform runtimes

- A baseline `/usr` for the sandboxed app
  - Apps bundle anything not in the baseline
  - Host system `/usr` is not visible at all (usually)
- Anyone can publish a runtime
  - Runtime maintainer chooses contents, versions
  - No development/sysadmin tools, package manager, init
- Conventionally `com.example.Platform`

COLLABORA

SDK runtimes

- A Platform, plus what's needed to build against it
  - Compiler and other toolchain packages
  - `gdb`, `strace` and similar debugging tools
  - Header files
  - Static libraries
- Conventionally `com.example.Sdk`

COLLABORA

Runtime versioning

- Platform and SDK runtimes have *branches*
- Branches are whatever makes sense to the runtime maintainer
  - `org.freedesktop.Platform//1.6`
  - `org.gnome.Platform//3.26`
  - `org.fedoraproject.Platform//27`
  - `net.debian.flatpak.Games.Platform//stretch`

COLLABORA

Security?

- The runtime maintainer is responsible for updating the runtime
  - Choose your runtime maintainer wisely
- The app author is responsible for updating the bundled libraries, if any
  - Be careful what you bundle

COLLABORA

Inside apps and runtimes

Fig.2. Flatpacks ready to be compiled

Photo: Michell Zappa, 2006. CC-BY-SA-2.0

COLLABORA

libostree

- libostree: like git, but for `/usr`
  - `./config`
  - `./refs/heads/master`
  - `./refs/heads/stable`
  - `./refs/remotes/origin/master`
  - `./objects/3b/6f018809252480b740a48ea3cb746a434dd688`
  - `./objects/c0/837b81795498042a3570b792cb2f41da0a0551`

COLLABORA

libostree

- libostree: like git, but for `/usr`
  - `./config`
  - `./refs/heads/app/org.debian.packages.openarena/x86_64/master`
  - `./refs/remotes/flatdeb/runtime/net.debian.flatpak.Games.Platform/x86_64/stretch`
  - `./objects/a1/443a265b155be7d190c5a0a5e99427716a0a1432f6994fbde40aafb23fb11e.file`
  - `./objects/e9/67eda76106efa124b736af20c14b3fea2a254b71927534bd869217e105c532.file`

COLLABORA

libostree deduplication

- Content-addressed storage
- Hardlink-based deployment
- If two runtimes are built from the same base on the same day, and have the same `libc.so.6`, that's a single file
- If one runtime is based on another and they have the same `libc.so.6`, that's still the same file
- For this to work, deployments have to be read-only

COLLABORA

App containers

- Bind-mount the app on `/app`
- Bind-mount the runtime on `/usr`
- Populate selected files in `/var`, `/etc` from host
- Expose host files as required
  - D-Bus socket
  - PulseAudio socket

COLLABORA

bubblewrap (formerly xdg-app-helper)

- Restructuring the mount table needs user namespaces
- Portable code can't rely on unprivileged access to those
  - Scary attack surface (e.g. CVE-2016-3135)
- `bubblewrap` is `setuid` root if it has to be
  - Minimal codebase, minimal dependencies
- `flatpak` is never `setuid`

COLLABORA

Sandboxing desktop apps

- Declarative capabilities
  - “uses X11”
  - “reads and writes ~/Downloads”
- Comparable to Android permissions
- Limitation: like older Android, either you have a capability or you don't

COLLABORA

Sandboxing is hard (work in progress)

- Apps with X11 access can do unwanted things
  - Be a keylogger
  - Take screenshots
- Apps with PulseAudio access can record you
- Apps with dconf access can change **any** configuration
- Among smcv's current work: teaching `dbus-daemon` to sandbox apps without needing `flatpak-dbus-proxy`

COLLABORA

Thinking with portals

Fig.3. Careless use of portals has safety implications

Photo: roninkengo, 2008. CC-BY-2.0

COLLABORA

May I?

- Better than handing out permissions: get user consent when needed
- When done badly, we get browser SSL prompts
  - This site has an obscure problem that you have no basis for understanding. Do you want to continue with what you were already trying to do?
- When done well, it's a lot better
  - Let hangouts.google.com use your microphone?

COLLABORA

Document portal

- Inside the sandbox, the app uses ordinary library APIs
- Outside the sandbox, in a different process, an Open or Save dialog appears
- The portal conspires with the compositor to glue them together
- The selected file magically appears in the sandbox
  - Please pay no attention to the FUSE filesystem behind the curtain

Various other portals

- Compose an email
- Open a URI in its correct handler
- Get user's name and photo/avatar
- Inhibit end-of-session, user-switching, suspend, idle
- Pop up notifications
- Print documents
- Take a screenshot

COLLABORA

How to build a Flatpak

Fig.4. Remember to check the manifest before building

Photo: Duncan Hull, 2013. CC-BY-2.0

Compiling a Flatpak app

- Build it in a runtime of your choice
- Build process usually automated by `flatpak-builder` and described by a JSON manifest
- `./configure –prefix=/app` (or equivalent)
- Does not need to be fully relocatable (always `/app`)

Not compiling a Flatpak app

- To build one the hard way, all you need is to commit:
  - `./files/` (will be mounted at `/app/`)
  - `./metadata` (see `flatpak-metadata(5)`)
  - `./export` (exported entry points, optional)
- If all else fails, hex-editing `/usr/` into `/app/` is ugly but possible

COLLABORA

Introduction to Flatpak

FOSDEM 18

col.la/fosdem18flatpak

Questions?

“*Flatpak and your distribution*”:
Distros devroom, 13:00 tomorrow

We're hiring: col.la/careers