COLLABORA

Containers and Steam

Putting games under pressure

FOSDEM'20

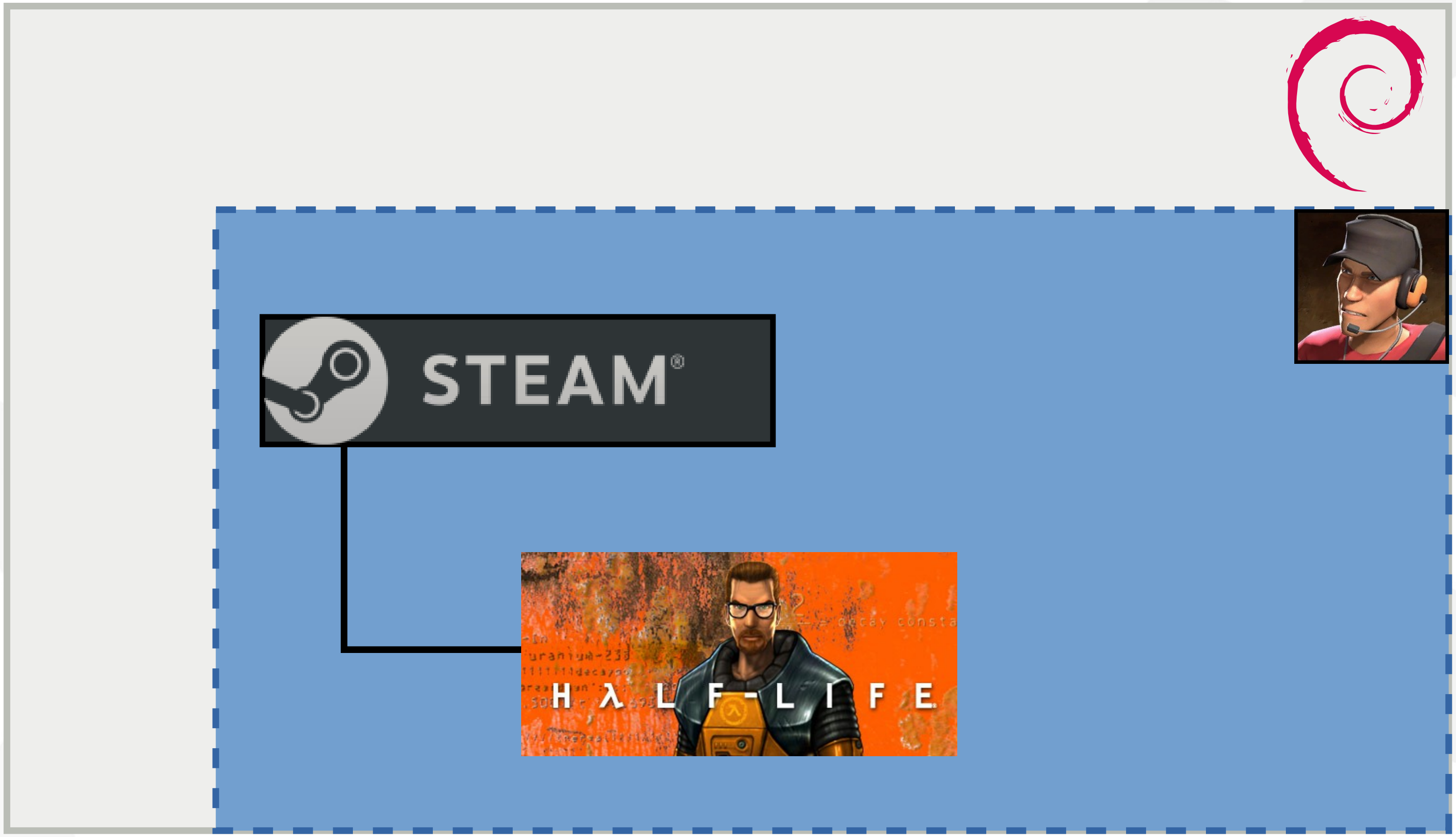
Simon McVittie
smcv@collabora.com
smcv@debian.org
2020-02-01

Introduction

- Steam is Valve's app-store for games on Windows, Mac, SteamOS and generic Linux
- I'm a consultant at Collabora, helping Valve with the Steam Runtime
- People who have bought a game expect it to work
- There's no useful ABI baseline for how we make it work
  - except maybe the LSB, but nobody actually uses that

The Steam Runtime, circa 2013

- Steam Runtime 1 'scout', based on Ubuntu 12.04 LTS 'precise'



The Steam Runtime, circa 2013

- Bundle all the things!
  - Except for glibc and the graphics driver
- Steam Runtime 1 'scout', based on Ubuntu 12.04 LTS 'precise'
- LD_LIBRARY_PATH=/path/to/lib
- It worked!
  - But not for long

Graphics drivers are hard

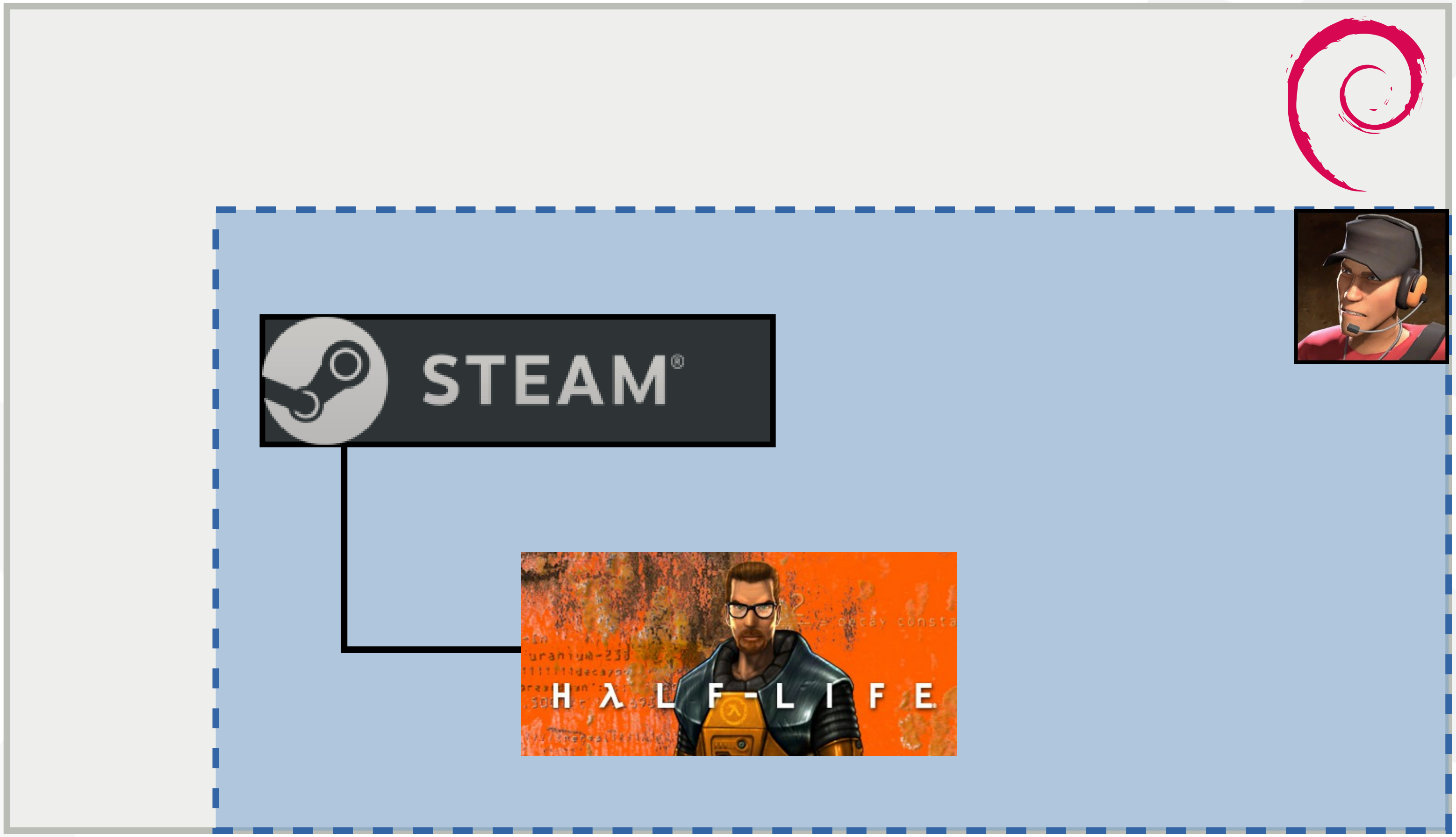
- Open-source drivers (Mesa)
  - We need to use dependencies at least as new as the distribution
  - New GPUs need a new Mesa
  - New kernels work best with a new Mesa
- Proprietary NVIDIA drivers, and historically others
  - Must be in lockstep with the kernel module

glibc is also hard

- /lib/ld-linux.so.2 is hard-coded into every i386 dynamic binary
- /lib64/ld-linux-x86-64.so.2 is hard-coded into every x86_64 dynamic binary
- If ld.so doesn't match libdl.so.2, bad things happen
- If libdl.so.2 doesn't match libc.so.6, bad things happen
- If libc.so.6 doesn't match libpthread.so.0, you get the idea
- So the Steam Runtime cannot include glibc

The Steam Runtime, circa 2018

- What if we use more host-system libraries in the container?

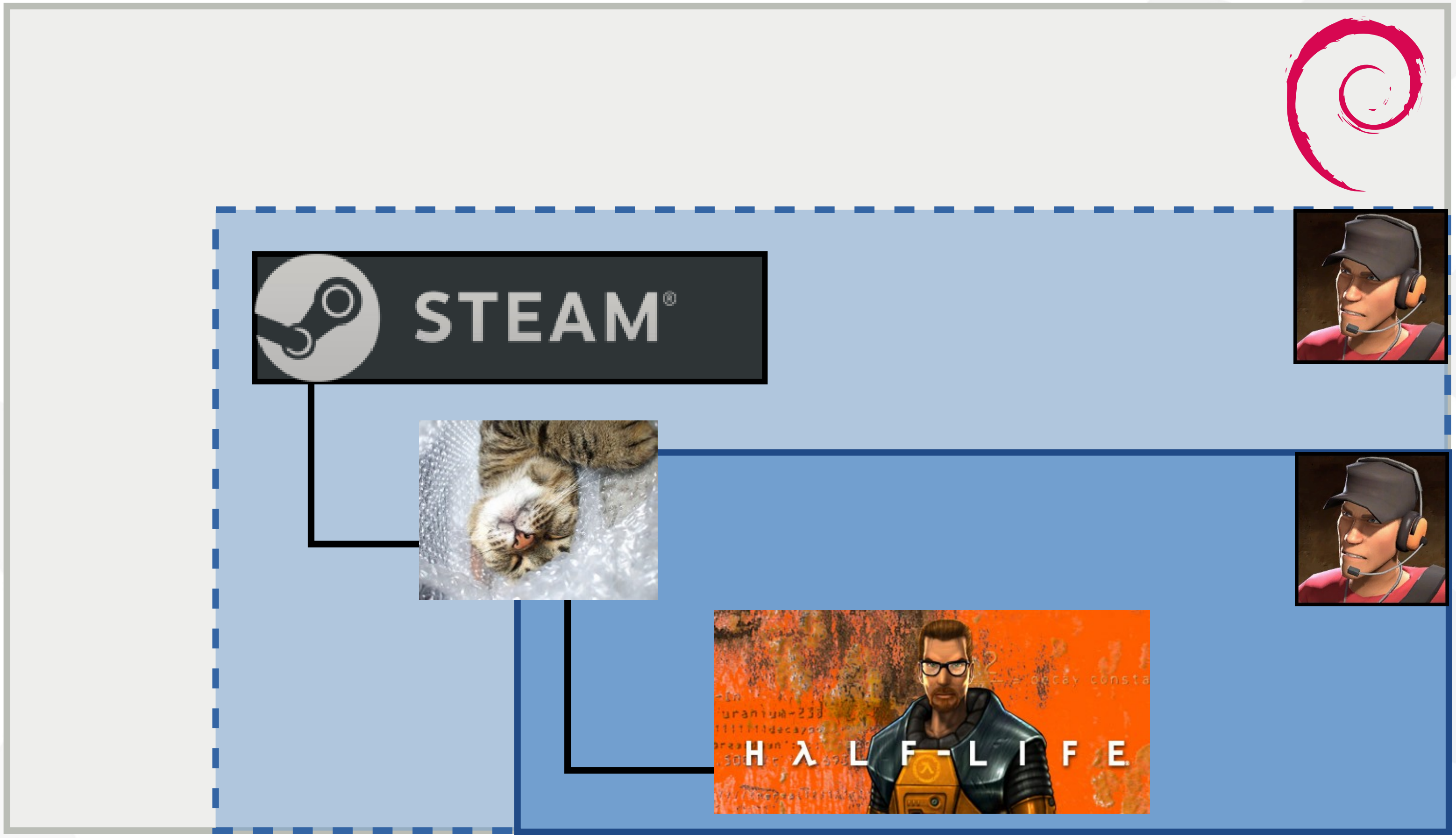


The Steam Runtime, circa 2018

- Still bundle all the things!
  - Except for glibc and the graphics driver
- Steam Runtime 1 'scout', based on Ubuntu 12.04 LTS 'precise'
- LD_LIBRARY_PATH again
- Find all the system libraries that are newer than ours and put them first
- It works, except when it doesn't
  - Comparing versions is not as obvious as you might think
  - libcurl.so.4 has a different ABI in different distributions
  - OpenSSL is always troublesome
- Game vendors accidentally add dependencies from outside the Runtime

pressure-vessel

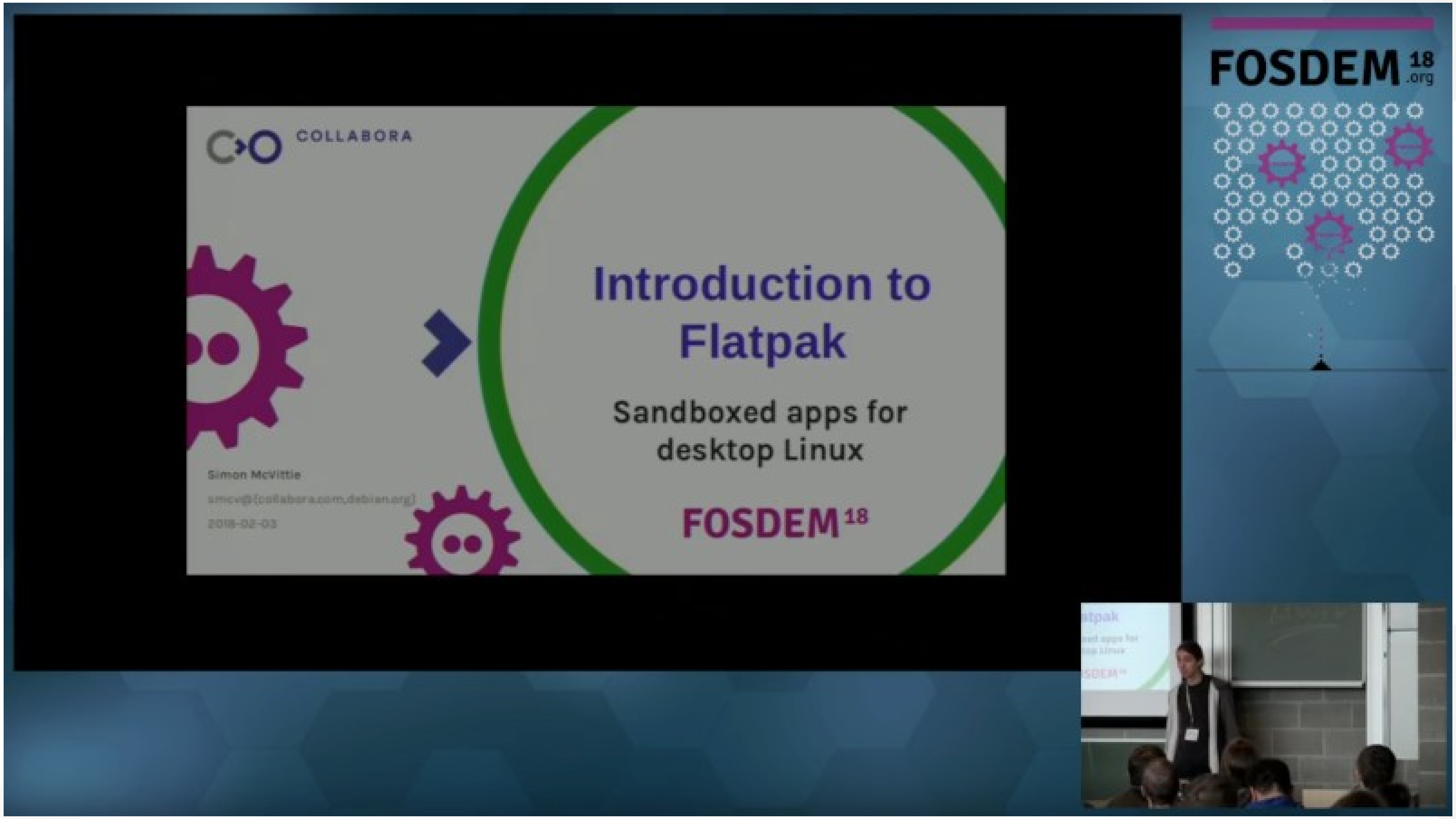
- Put each game in a container, using bubblewrap



pressure-vessel

- Put each game in a container, using bubblewrap
  - Lots of code recycled from Flatpak
- Graphics drivers (and maybe dependencies) from the host system
  - We wish we didn't have to
- Container's /usr is a very strict 'scout' environment
  - Good for QA: if it works here, it should work anywhere
  - But: dependencies outside the runtime? No game for you
- Experimental side-benefit: separate $HOME per-game
  - Currently breaks Cloud Auto-Sync and Steam Workshop
- Not a security boundary
  - Would be nice, but not a priority right now

Meanwhile, in the community…



COLLABORA

Introduction to Flatpak

Sandboxed apps for desktop Linux

FOSDEM 18

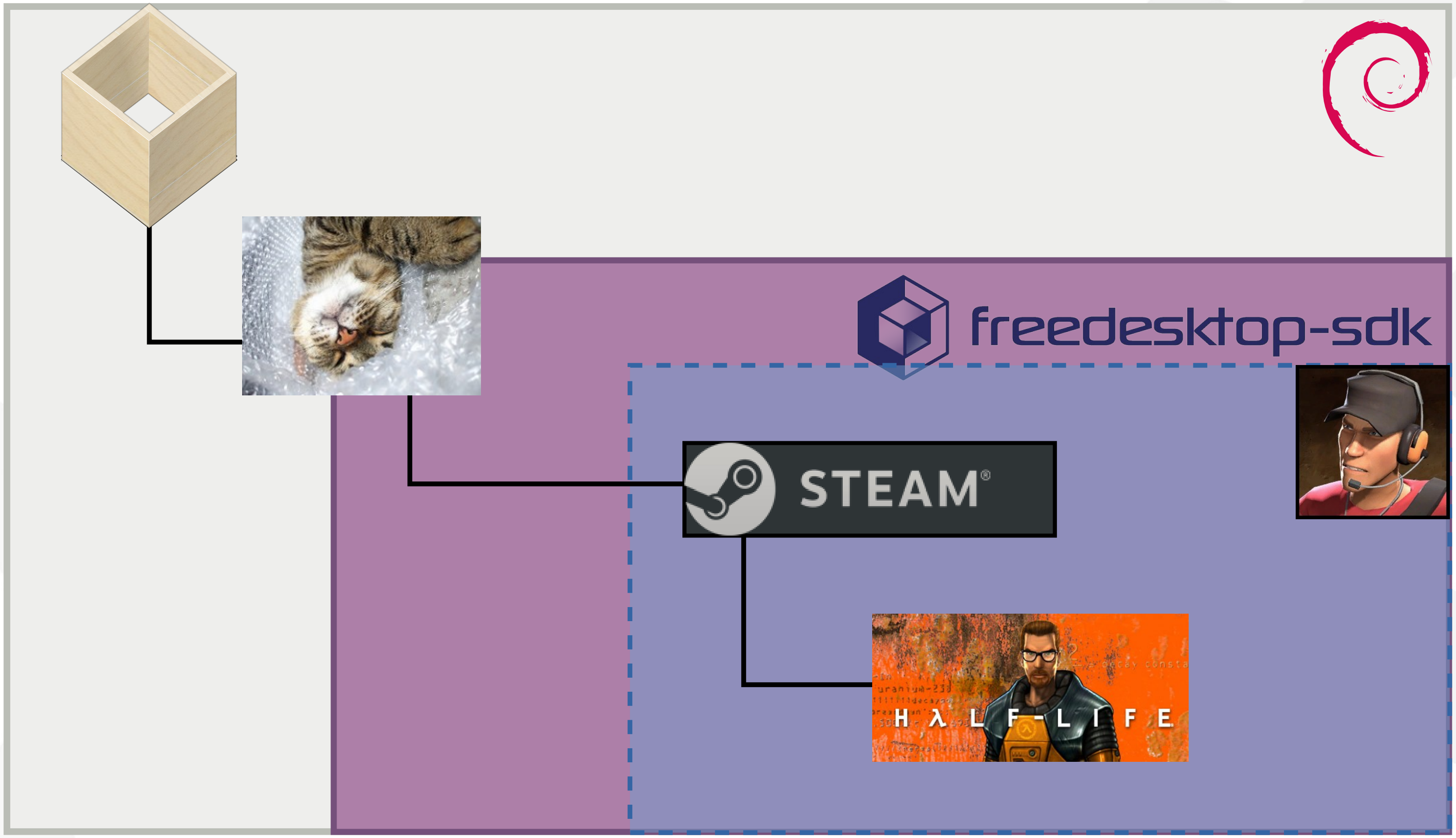
Simon McVittie

smcv@{collabora.com,debian.org}

2018-02-03

Steam, as an unofficial Flatpak app

- Put the entire Steam client in a container, along with all games



Steam, the unofficial Flatpak app

- Put the entire Steam client in a container
- Container's /usr is the freedesktop.org Flatpak runtime
- Games are in the same container
  - ... inside the (2018 edition) Steam Runtime
- Is a security boundary
  - At least, a weak one – X11 is hard to sandbox
- Graphics drivers and glibc from the Flatpak runtime
- Libraries from the Flatpak runtime or the Steam Runtime, whichever is newer
- Goes to heroic efforts to work around broken games

Flatpak with pressure-vessel inside?

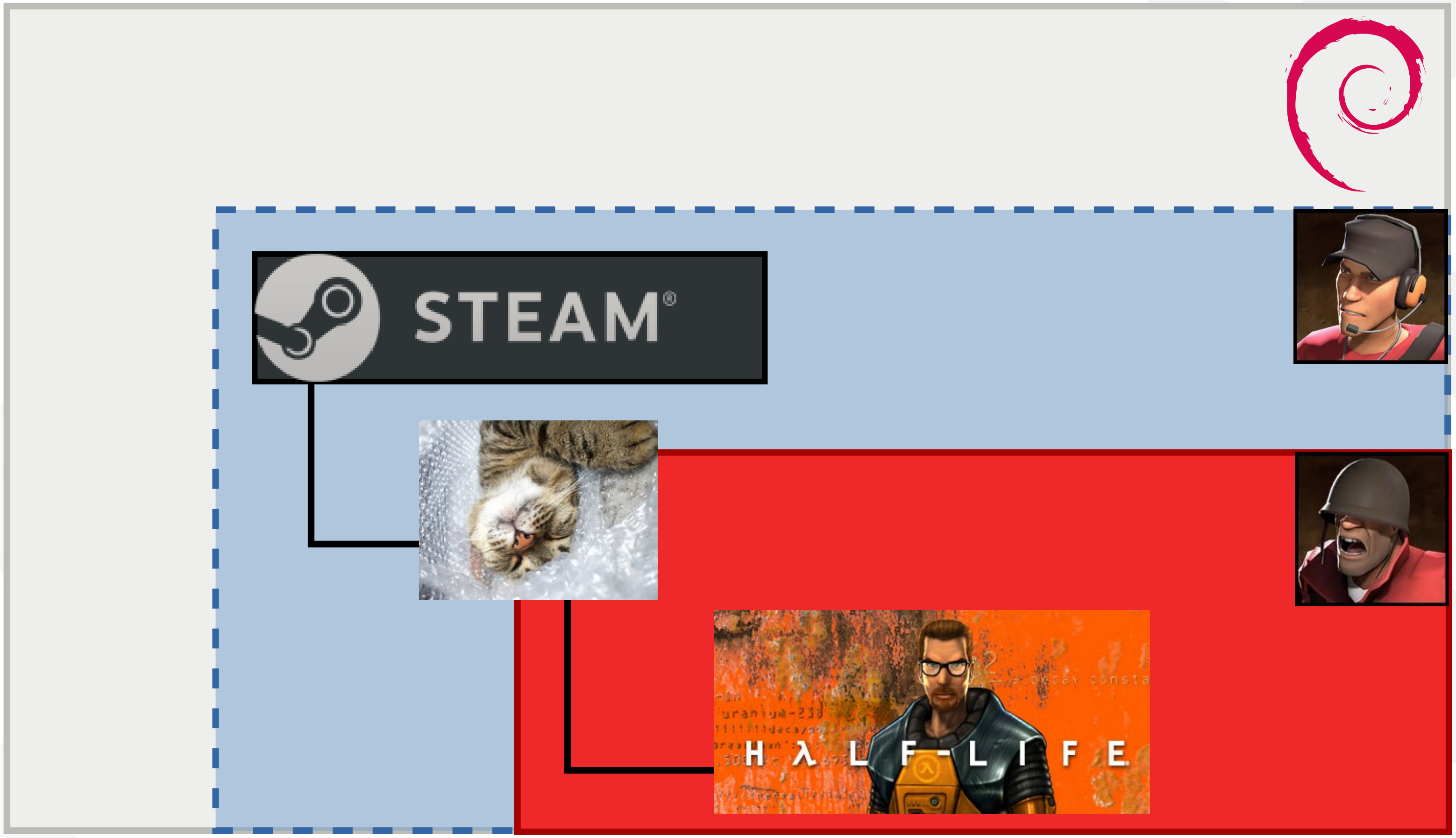
- Sadly, not possible for technical and security reasons
  - If unprivileged users can't create a userns (e.g. Debian), to make setuid bubblewrap safe, it has to relinquish privileges
  - Flatpak doesn't want apps to be able to make arbitrary containers anyway, so that portals can identify sandboxed processes by /proc/PID/root/.flatpak-info

The future?

- Old games need to keep working
  - Even with new distributions, GPUs, graphics drivers
  - Even though old runtimes can't compile new graphics drivers
- New games need new runtimes
  - Ubuntu 12.04 is many things but new is not one of them
- New games need to keep working too
  - Games that work on Debian 10 won't necessarily work on Debian 15

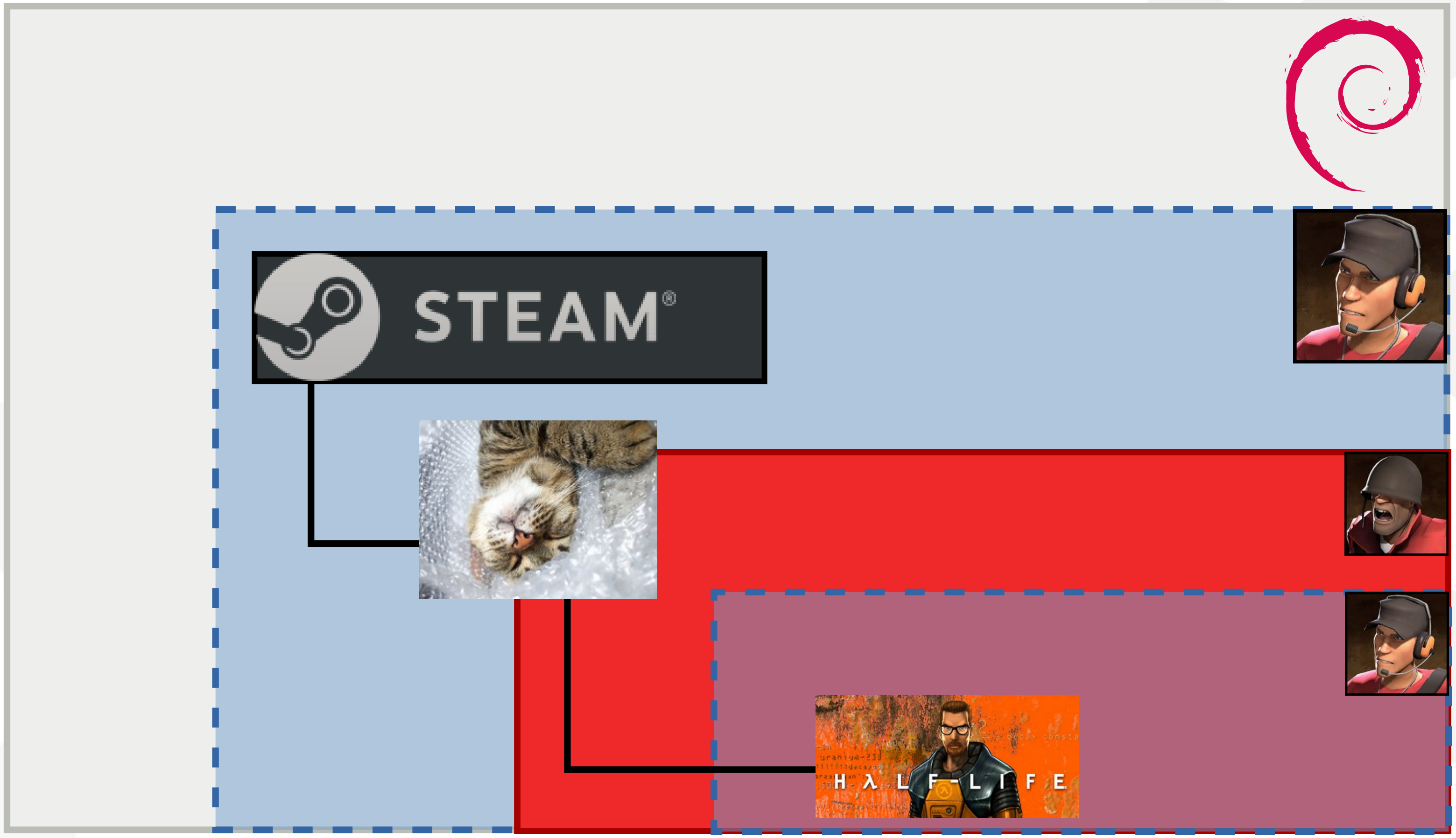
Future: games in newer runtimes?

- pressure-vessel decouples the Steam client's runtime from the game's



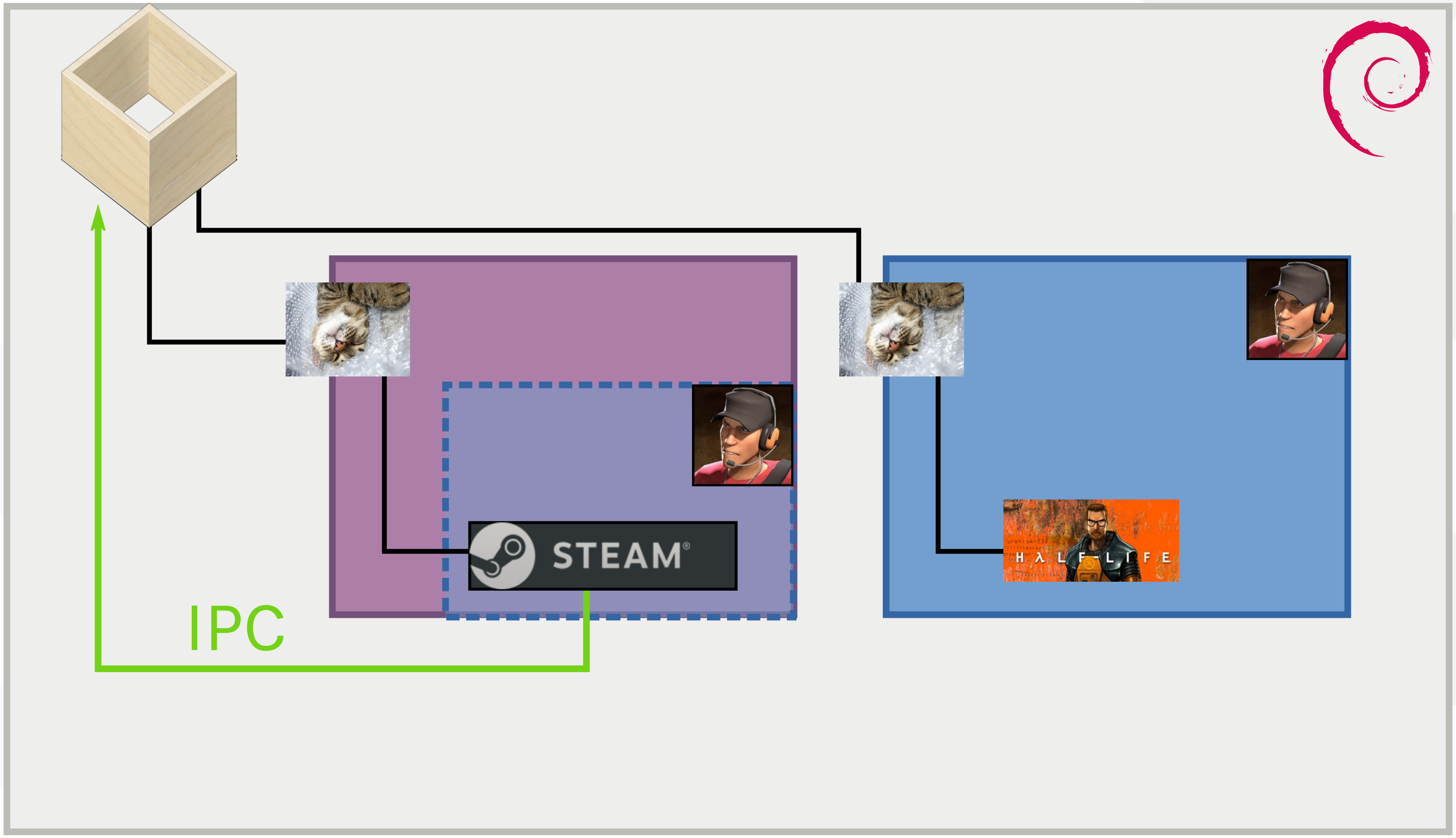
Future: scout inside a newer container runtime?

- For older games that accidentally depend on post-2012 libraries



Flatpak with a parallel scout container?

- Requires Flatpak and bubblewrap feature development
- PID namespace currently breaks Steam's tracking of running games



FOSDEM'20

Containers and Steam

Any questions?

https://github.com/ValveSoftware/steam-runtime
https://repo.steampowered.com/
https://www.collabora.com/

Psst...
We're hiring!