Playing in the sandbox

Guillaume Emont - Igalia
guijemont@igalia.com

I. What do we want to solve?

Gstreamer and OpenCV for image stabilisation « Le coin à Guij

http://guij.emont.org/blog/2011/11/10/gstreamer-and-opencv-for-image-stabilisation/

but rather in the order I should have researched them: starting with a simpler problem, then getting into the complications of my balloon problem.

The simpler problem at hand is presented to you by Joe the Hippo:

Internets = cute videos of [insert favourite animal]

As you can see, Joe almost looks like he's on a boat. He isn't, but the cameraman is, and the video was taken with a lot of zoom. The movement in that video stream has a particularity that can

Trustworthy?

Complex software written by human beings can have bugs.


rm -rf /
00:10 / 00:14


rm -rf /


Ophiocordyceps unilateralis

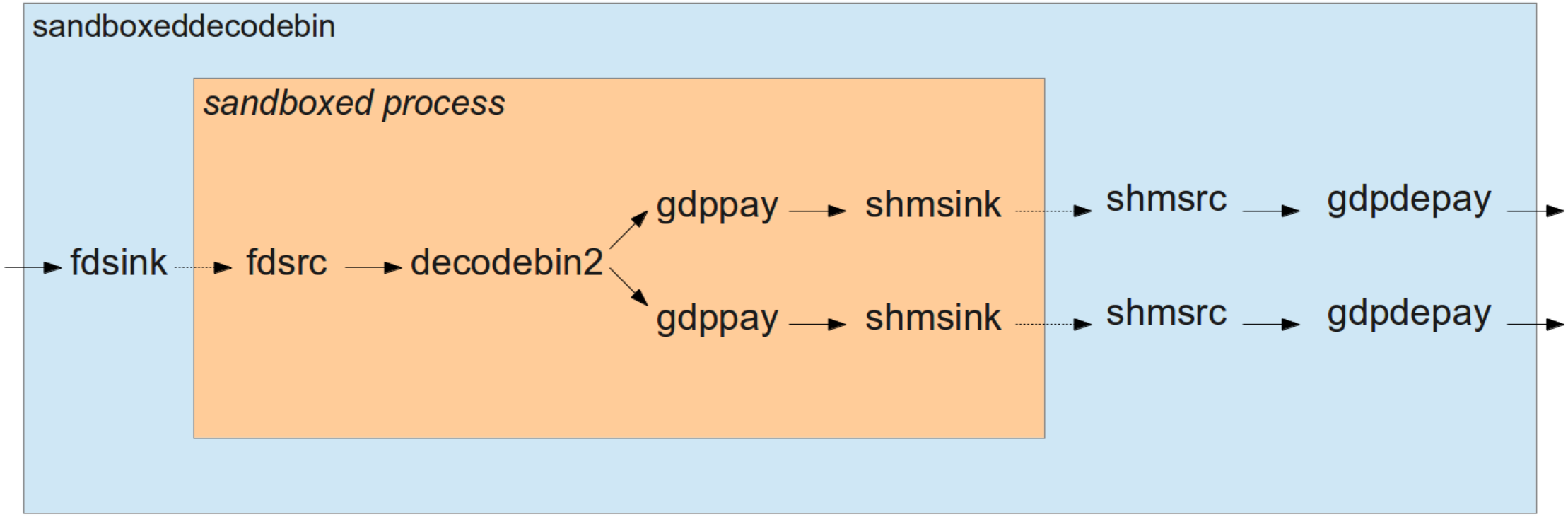
The piece of software that handles untrusted video:

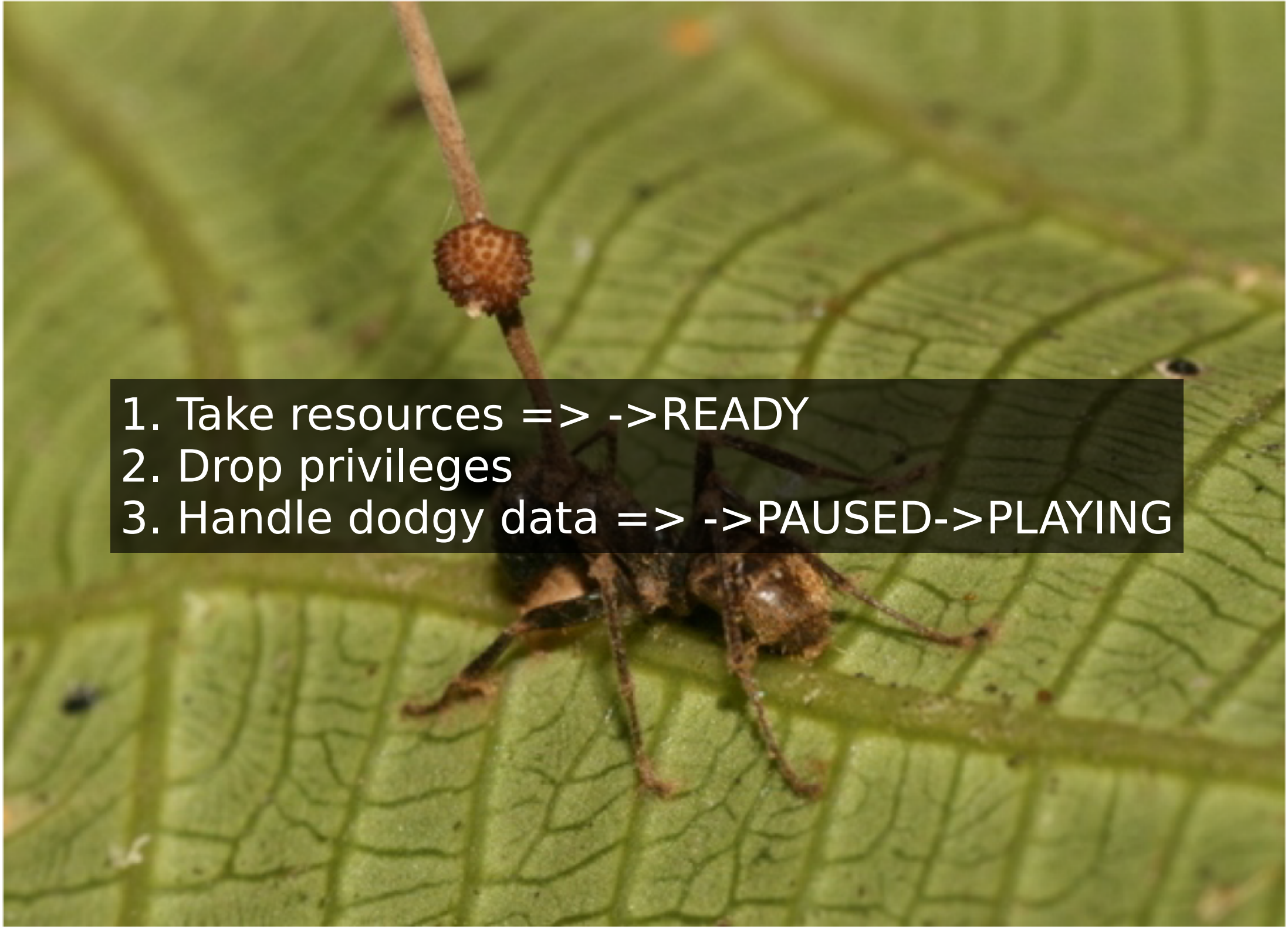
- is not evil in itself
- should be considered evil when it starts to handle untrusted data

1. Take resources
2. Drop privileges
3. Handle dodgy data

II. Experimentations

sandboxeddecodebin


sandboxeddecodebin
sandboxed process
fdsink
fdsrc
decodebin2
gdppay
shmsink
gdppay
shmsink
shmsrc
gdpdepay
shmsrc
gdpdepay



1. Take resources => ->READY
2. Drop privileges
3. Handle dodgy data => ->PAUSED->PLAYING

Issues:

- resources acquired when going to PAUSED
- clean up

Potential solutions:

- finer grained sandbox
- modify elements to acquire everything at ->READY?
- add an all-resources-acquired signal?
- have a controlling process do the clean up

Other big limitations:

- no upstream communication => no seeking
- overhead: 720p ogg/theora on my i5: 20-30% -> 30-40% cpu

III. Usable sandbox implementations on Linux

Setuid-sandbox (CLONE_NEWPID + separate uid/gid + chroot)

- prevents access to data outside of chroot
- in kernel since 2.6.24
- ideally needs a pool of UIDs/GIDs
- not very granular

Seccomp

- only read(), write(), exit(), sigreturn()
- applied to a thread
- in kernel since 2.6.10

Seccomp + BPF

- filters on syscalls and their arguments
- libseccomp to make it easier
- in kernel since 3.5

SELinux

- by process
- quite fine grained
- rules set by administrator/distribution, developers
- not standard

IV. Going Forward

Better IPC: GstPadProxy, GstElementProxy & friends
=> control over a remote pipeline

Put the whole pipeline process in the sandbox
=> shouldn't be complicated with a granular sandbox

Architecture that is agnostic
to the sandboxing system used

Performances: profile, optimise

Thank You

guijemont@igalia.com
http://guij.emont.org/blog/
https://github.com/guijemont/Sandboxed-Player