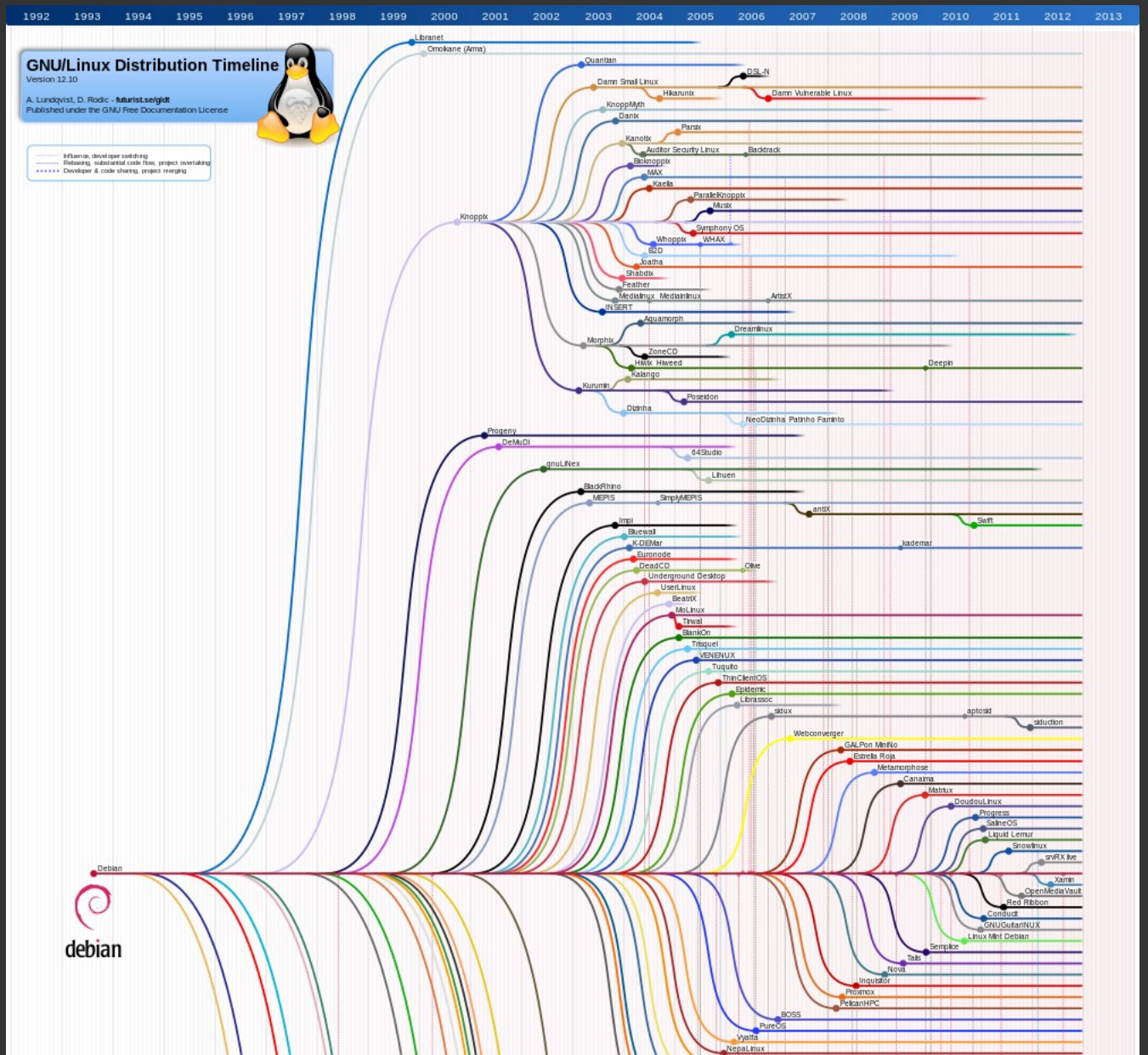
fedora
WORKSTATION

Sandboxed Desktop Applications

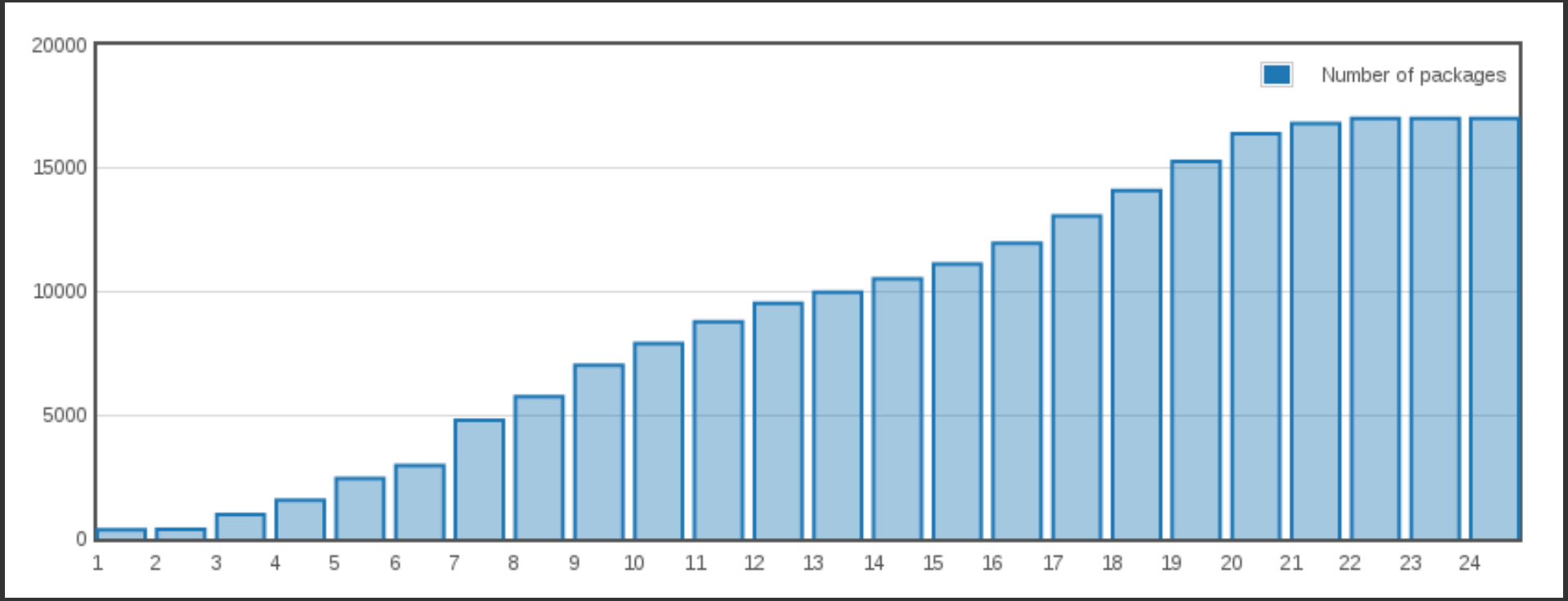
Matthias Clasen
Flock 2015

Why sandboxed apps?

Why sandboxed apps?



Why sandboxed apps?



Why sandboxed apps?

- Users are interested in applications

Why sandboxed apps?

- Users are interested in applications
- Application developers are not packagers

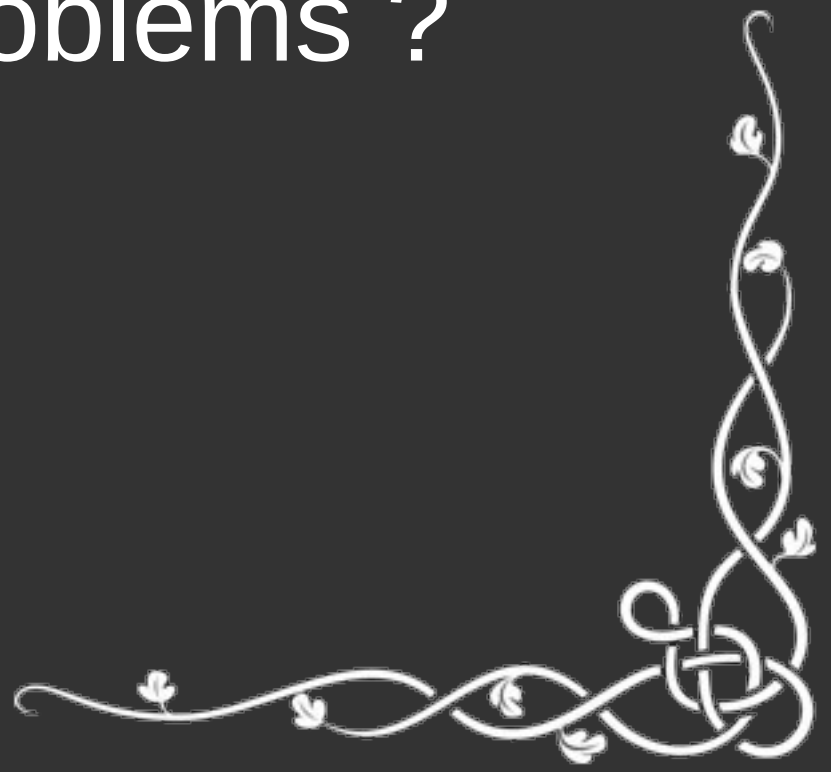
Why sandboxed apps?

- Users are interested in applications
- Application developers are not packagers
- Packaging does not scale

Why sandboxed apps?

- Users are interested in applications
- Application developers are not packagers
- Packaging does not scale
- Everybody downloads binary rpms off the internet

What are the problems ?

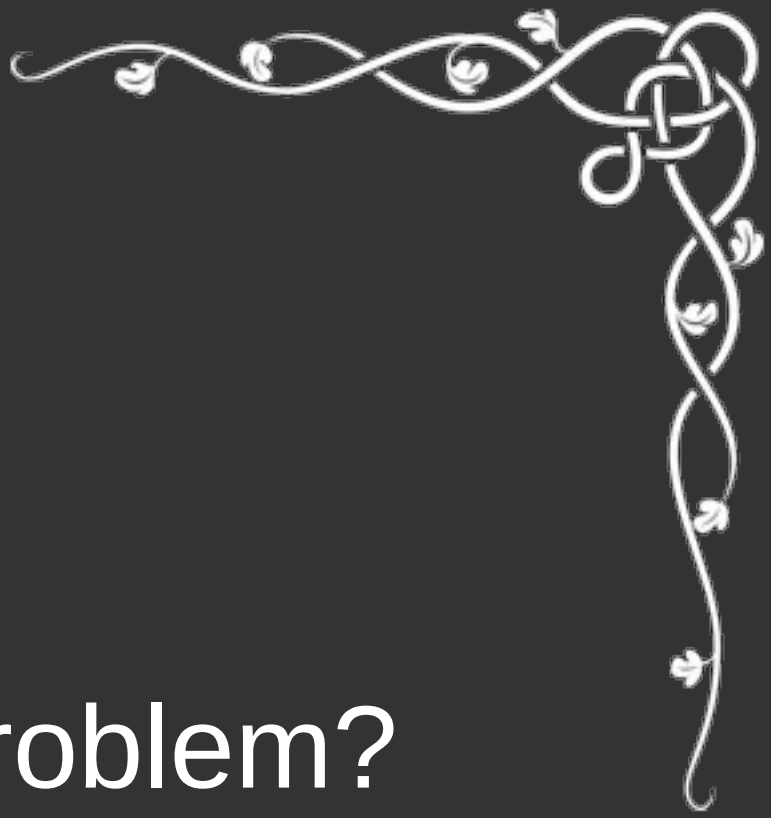


What are the problems ?

- Application developers need to get their apps to users

What are the problems ?

- Application developers need to get their apps to users
- Users want to keep their data and their computer safe



Installation is a problem?

Installation is a problem?

- Not if you live in a Linux distro bubble

Installation is a problem?

- Not if you live in a Linux distro bubble
- For a third-party application developer: Yes

Installation is a problem?

- Not if you live in a Linux distro bubble
- For a third-party application developer: Yes
  - What package format ?

Installation is a problem?

- Not if you live in a Linux distro bubble
- For a third-party application developer: Yes
  - What package format ?
  - How do you handle dependencies ?

Installation is a problem?

- Not if you live in a Linux distro bubble
- For a third-party application developer: Yes
  - What package format ?
  - How do you handle dependencies ?
  - Can users discover the application ?

Installation is a problem?

- Not if you live in a Linux distro bubble
- For a third-party application developer: Yes
  - What package format ?
  - How do you handle dependencies ?
  - Can users discover the application ?
  - Will I ever be able to get updates to them ?

Installation is a problem?

- Not if you live in a Linux distro bubble
- For a third-party application developer: Yes
  - What package format ?
  - How do you handle dependencies ?
  - Can users discover the application ?
  - Will I ever be able to get updates to them ?
  - Can I get payed for this ?

What are our answers ?

What are our answers ?

- Simpler building

What are our answers ?

- Simpler building
- Ostree – efficient distribution of not just files, but entire trees

What are our answers ?

- Simpler building
- Ostree – efficient distribution of not just files, but entire trees
- Runtimes – bundling with a twist

What are our answers ?

- Simpler building
- Ostree – efficient distribution of not just files, but entire trees
- Runtimes – bundling with a twist
- gnome-software – a friendly UI for discovering and installing applications

What are the problems ?

- Application developers need to get their apps to users
- Users want to keep their data and their computer safe

What needs protection?

What needs protection?

- X applications can snoop on each others input and fake each others output – no isolation

What needs protection?

- X applications can snoop on each others input and fake each others output – no isolation
- File system: the home directory is free for all

What needs protection?

- X applications can snoop on each others input and fake each others output – no isolation
- File system: the home directory is free for all
- Session bus: apps can steal bus names, etc

What needs protection?

- X applications can snoop on each others input and fake each others output – no isolation
- File system: the home directory is free for all
- Session bus: apps can steal bus names, etc
- Other connections: Sound (pulseaudio)

What needs protection?

- X applications can snoop on each others input and fake each others output – no isolation
- File system: the home directory is free for all
- Session bus: apps can steal bus names, etc
- Other connections: Sound (pulseaudio)
- Devices: webcam, etc

What needs protection?

- X applications can snoop on each others input and fake each others output – no isolation
- File system: the home directory is free for all
- Session bus: apps can steal bus names, etc
- Other connections: Sound (pulseaudio)
- Devices: webcam, etc
- Shared databases: tracker, online accounts, etc

What are our answers ?

What are our answers ?

- X – Wayland: isolation is built in from the start

What are our answers ?

- X – Wayland: isolation is built in from the start
- File system – bind mounts of a limited view

What are our answers ?

- X – Wayland: isolation is built in from the start
- File system – bind mounts of a limited view
- Session bus – kdbus and portal APIs

What are our answers ?

- X – Wayland: isolation is built in from the start
- File system – bind mounts of a limited view
- Session bus – kdbus and portal APIs
- Devices – pinos (aka pulsevideo) effort

What are our answers ?

- X – Wayland: isolation is built in from the start
- File system – bind mounts of a limited view
- Session bus – kdbus and portal APIs
- Devices – pinos (aka pulsevideo) effort
- Other connections, shared databases – no clear answer yet

Putting it all together: xdg-app

More Information

https://wiki.gnome.org/Projects/SandboxedApps

http://lists.freedesktop.org/mailman/listinfo/xdg-app

IRC: #xdg-app on freenode

Bugzilla: http://bugs.freedesktop.org, product xdg-app

http://videos.guadec.org/2015

https://lwn.net/Articles/654128

fedora
WORKSTATION

Questions ?