Sécurité des applications graphiques sous X et Wayland

jres Nantes 2017

Problématique

Sécurité d'un poste de travail GNU/Linux au niveau de l'interface utilisateur

Clavier, souris,...

Accès aux événements des périphériques d'entrée
Raccourcis clavier ou keylogger ?

Copie d'écran

Screencast ou espionnage de l'affichage ?

Mode Plein écran

Video plein écran ou fausse interface ?

Alertes et notifications

Quelle est l'application qui demande un mot de passe ?
→ authentification de l'origine des pop-ups

Copier/Coller

Qui peut accéder aux données du presse-papier ?
S'il contient un mot de passe super secret ?

X Windows

- Communications inter-clients via ICCCM et EWMH
- Pas de sécurité : tous les clients ont accès à tout.

Bibliographie

[1] S. Dodier-Lazaro et M. Peres.
Security in Wayland-based desktop environments : Privileged clients, authorization, authentication and sandboxing !
Dans *XDC2014*, Bordeaux, Septembre 2014.
https://www.x.org/wiki/Events/XDC2014/XDC2014DodierPeresSecurity/.

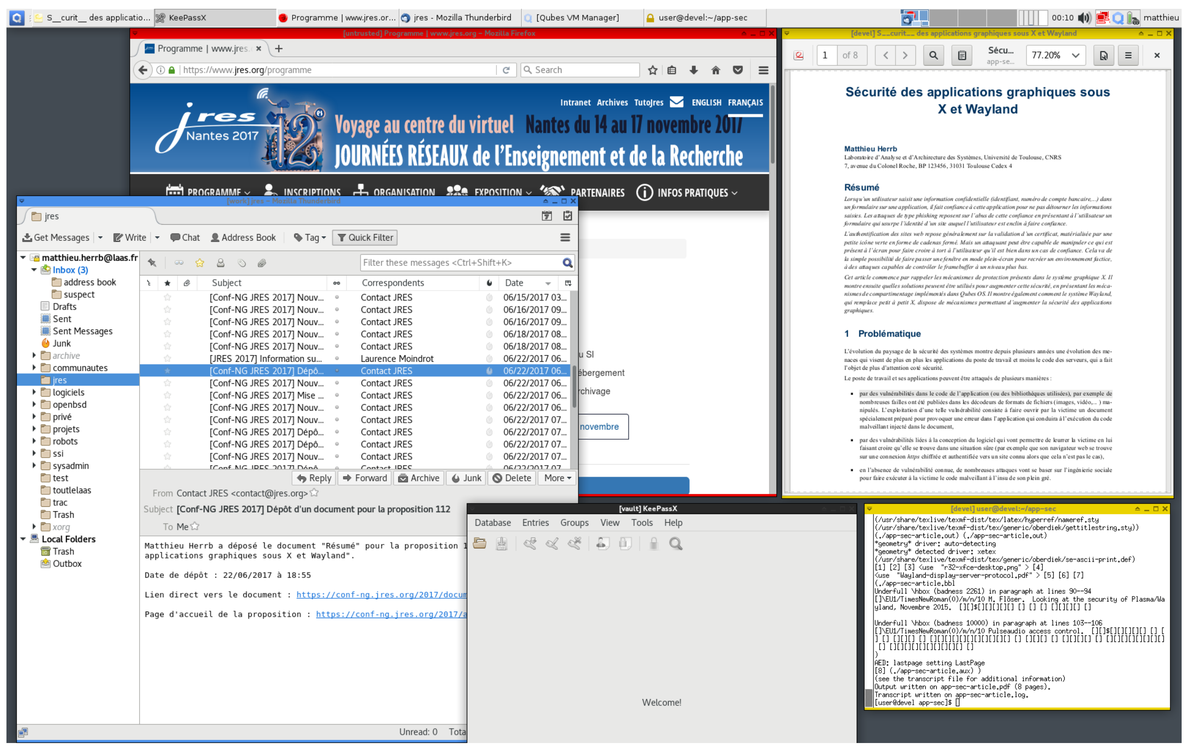
[2] M. Marczykowski-Górecki.
Improving client systems security with Qubes OS.
Dans *RMLL2016*, Paris, Juillet 2016.
https://sec2016.rmll.info/files/20160704-04-Marczykowski-QubesOS.pdf.

[3] M. Flöser.
Looking at the security of Plasma/Wayland, Novembre 2015.
https://blog.martin-graesslin.com/blog/2015/11/looking-at-the-security-of-plasmawayland/.

[4] A. Larsson.
The flatpack security model, Janvier 2017.
https://blogs.gnome.org/alexl/2017/01/18/the-flatpak-security-model-part-1-the-basics/.

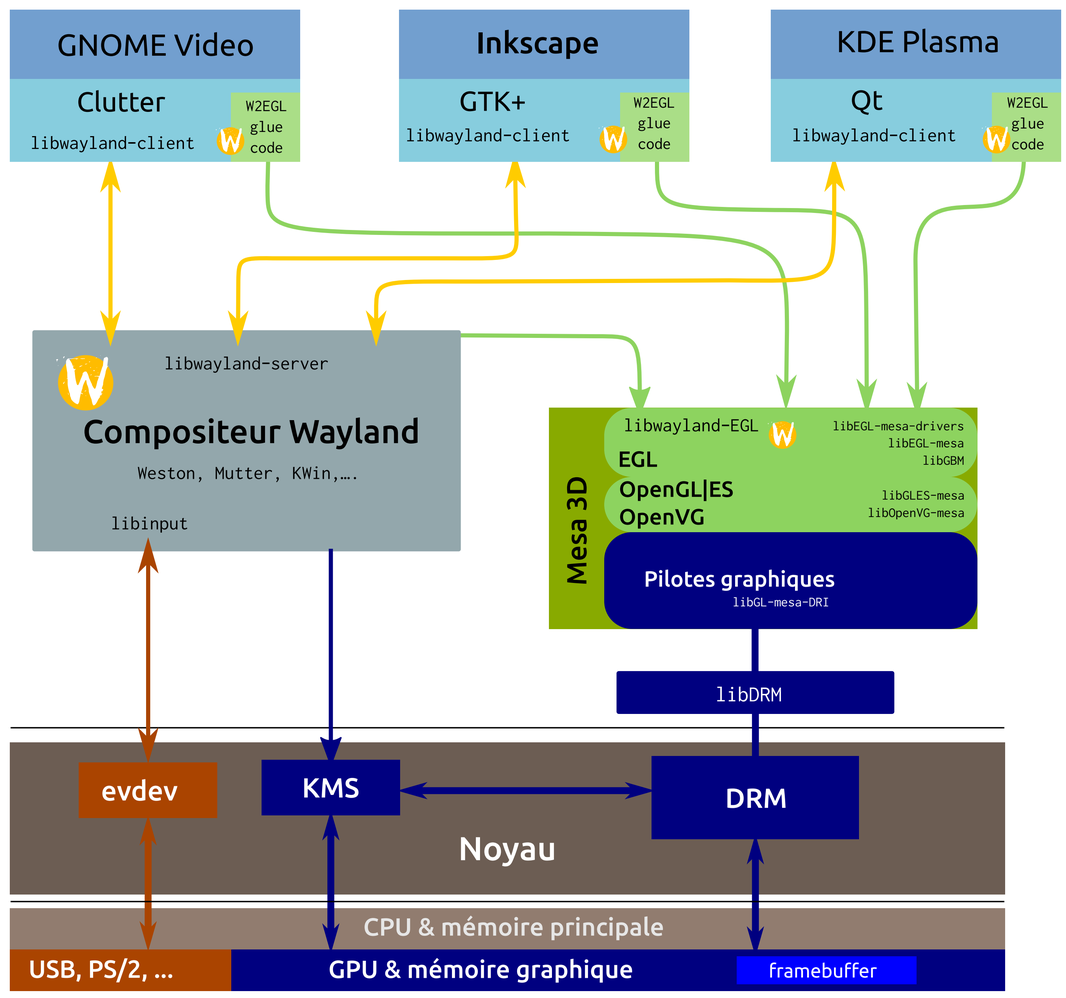
Qubes OS

- Isolation des applications dans des VM de niveaux de sécurité différents.
- Qubes Gui contrôle les échanges entre VMs
- Marquage explicite (code couleur) des applications par niveau de sécurité.



Wayland

- Pas de communication directe inter-clients
- Toutes les communications passent par le *Compositeur*



Conteneurs

Mode de distribution des paquets binaires du futur

- flatpak (redhat)
- Subgraph OS

Matthieu Herrb
Laboratoire d'Analyse et d'Archirecture des Systèmes, Université de Toulouse, CNRS