Projet d'Année 2A

ENSI BOURGES

Sécurité et Technologies Informatiques — Année 2011

Sujet : **Capture d'activités système pour PIGA-SYSTRANS**

Nom : Dimitri GRESSIN & Timothée RAVIER

Encadrant ENSI : Jérémy BRIFFAUT

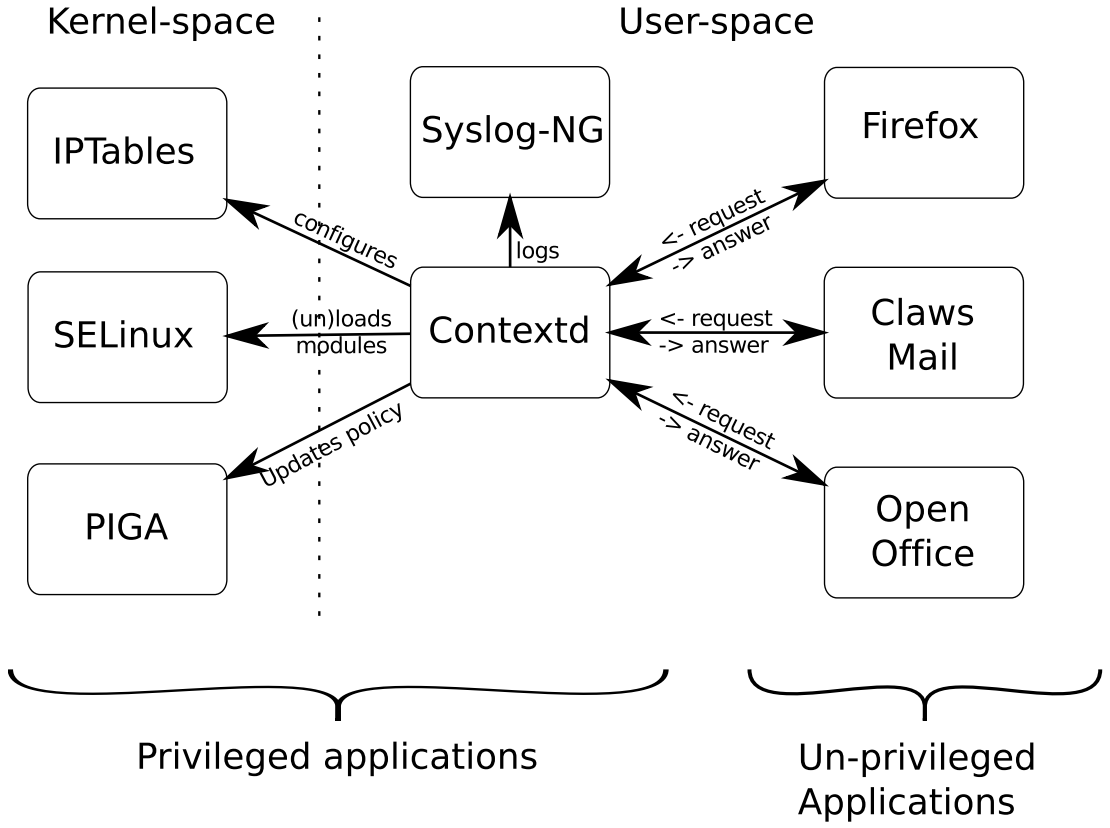
Contextd est un démon permettant de coordonner différents outils de sécurité sur un système Linux (iptables, SELinux, PIGA).

Concepts de domaines :

1 activité (impôts, E-commerce, …)

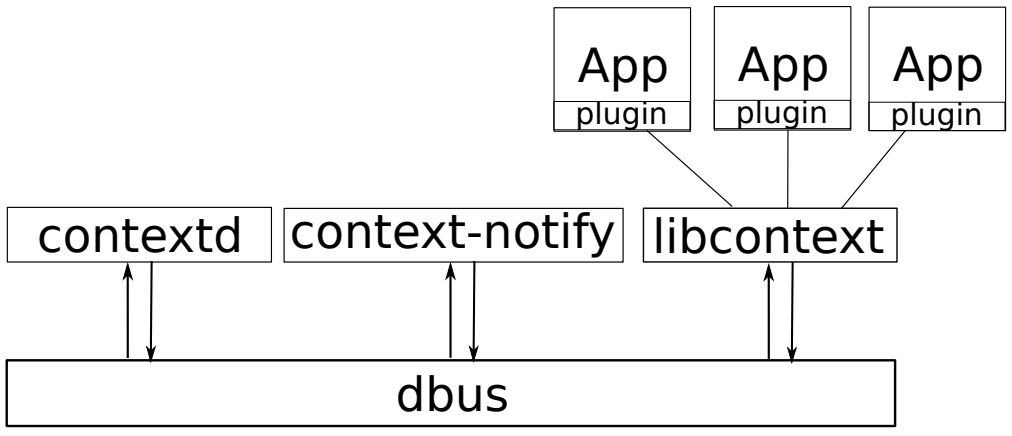
⇔

1 domaine

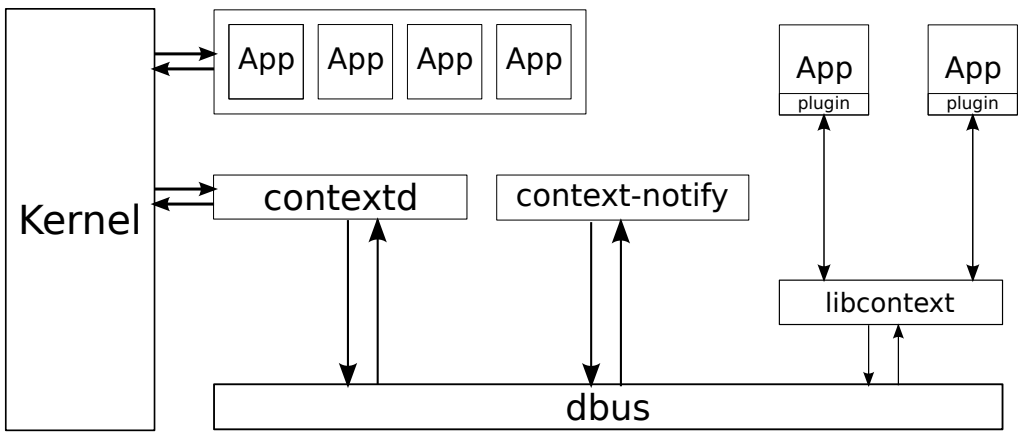


Pour que les changements de domaines soient synchronisés sur les actions de l'utilisateur, il fallait modifier les applications, telles que Firefox, pour qu'elles discutent avec Contextd, par l'intermédiaire de Dbus.

Notre travail a été d'implémenter une nouvelle solution, dans le noyau, afin de s'affranchir des contraintes de communication (plugins). Ainsi, certaines applications n'ont plus besoin d'être modifiées.



Fonctionnement avant



Fonctionnement après

Principale difficulté : Travail sur le noyau Linux