# Intégration de PIGA dans le noyau Linux Projet recherche 2011 – 2012



Timothée Ravier

École Nationale Supérieure d'Ingénieurs de Bourges

16 décembre 2011

## Plan

#### SELinux et PIGA

Intégration dans le noyau



#### SELinux et PIGA

#### Principe d'une protection système avancée

■ Propriétés de sécurité évoluées

■ Base de signatures Etape d'administration Contrôle de ces activités Langage **Politique** Propriétés -. description détection d'activités **Politique** Base convertion détection Graphes Alertes de contrôle d'accès analyse signatures des propriétés Phase 1 : Construction des graphes Phase 2 : Génération de la base de signatures Phase 3 : Détection Etape de détection



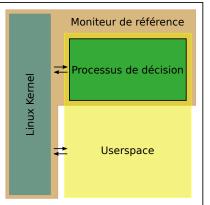
## Plan

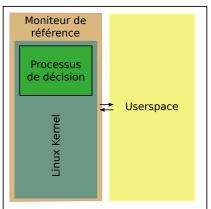
SELinux et PIGA

Intégration dans le noyau



# Intégration dans le noyau





- meilleures performances
- robustesse (attaques sur le moniteur de référence plus difficile)



## Plan

SELinux et PIGA

Intégration dans le noyau



