Retour sur dix années de recherche sur la protection des systèmes d'exploitation

Christian Toinard

ENSI de Bourges/LIFO

JIRC 29 Mai 2013

L'histoire d'une activité de recherche

- **Problématique** de la protection des systèmes d'exploitation
- **Véritable rupture** en matière de protection
- **Faits marquants** :
  - Coopération CEA, Défi ANR (Linux), Projet européen Seed4C
- **Evolutions récentes** pour améliorer la sécurité des :
  - autres systèmes d'exploitation (Windows, Android)
  - intergiciels et applications Web
  - systèmes de calcul intensif
  - systèmes virtualisés et Clouds

Garantir des propriétés de sécurité

- Confidentialité, Intégrité
- Protection versus cryptographie : les deux sont nécessaires
- Méthodes de contrôle d'accès pour minimiser les privilèges
  - discrétionnaire (Discretionary Access Control) : impossibilité [HRU76]
  - obligatoire (Mandatory Access Control) : complexité

Contrôle d'accès obligatoire

- **Etudié depuis les années 70** (Orange Book)
- **Communauté des systèmes d'exploitation** (ex: Paris, Grenoble) élabore ces solutions (ex: capacités Chorus)
- **En 2002 constat avec le CEA de l'absence d'approche à large échelle**, la thèse de Mathieu Blanc commence à traiter le problème par une répartition des politiques MAC
  - Propriétés globales
  - Répartition en politiques MAC (ex: SELinux) locales/réduites
  - Les politiques locales évoluant sans communication réseau
- mais reste encore beaucoup de points dûrs...

Thèse de Jérémy Briffaut : approche pionnière et extensible

- **Propriétés avancées** : supporte toute la littérature, permet de définir aisément de nouvelles propriétés
- **Traite la complexité des politiques MAC** directes (ex: SELinux)
- **Améliore** les approches MAC existantes
- **Vérification, détection et prévention des violations de propriétés avancées** (combinaison de plusieurs flux directs ou indirects) : contrôle les activités qui pourraient violer les propriétés

Approche scientifique complète

- **Une formalisation** des activitées contrôlables par le système d'exploitation (ex: dépendance causale entre contextes)
- **Un langage pour exprimer les activitées avancées**
  - Enumération des activitées avancées, autorisées dans les activités directes, pour vérification/détection/contrôle
- **Approche prouvée formellement et en pratique**
  - Preuve de l'énumération (graphe de flux => relations causales)
  - Expérimentation à grande échelle (pot de miel haute intéraction) : détection efficace de plusieurs millions d'attaques
- **Thèse de Jérémy Briffaut : la suite de l'histoire prouve le caractère pionnier**

PIGA-OS

- **Application de la thèse de Jérémy Briffaut** pour fournir un système d'exploitation Linux protégé en profondeur
- **Equipe de 5 personnes** Briffaut, Rouzaud-Cornabas, Solanki, Toinard, Venelle plus des étudiants dont Peres, Dodier, Ravier
- **Vainqueur des trois phases du défi**
  - MAC contrôlant processus, interface graphique et réseau
    - PIGA-MAC améliore et facilite les protections
  - PIGA-SYSTRANS (merci Martin!) permet des domaines (impôts, email, e-commerce,...) spécialisants la protection
- **Efficacité de la défense** vis à vis des solutions EADS/Supélec Rennes et INRIA Orsay/LIP6

SEWindows - thèse de Damien Gros avec le CEA

- Approche **MAC configurable** pour Windows
- Transposition du **"type enforcement"** de SELinux
- **Contextes de sécurité et contrôle des flux directs**
- **Avantages**
  - Garantie de propriétés de confidentialité et d'intégrité
  - Possibilité d'utiliser PIGA (***goal...!!***)
  - Protection des processus et des ressources Windows
  - Analyse de malwares dynamique et précise
- **Protection des postes et des Clouds Windows** (IaaS/PaaS/SaaS)

SEJava - thèse de Benjamin Venelle avec Bell Labs

- **Constat :** protection obligatoire quasi-inexistante pour la JVM (vulnérabilités sur Facebook, Twitter, ...)
- **MAC au niveau intergiciel** : protège les applications Java
- **Contextes de sécurité** pour les objets et **contrôle des flux directs** liés aux appels de méthodes et accès aux attributs
- **Avantages**
  - Traite la plupart des attaques sur Java (ex : élévation de privilèges)
  - PIGA pour contrôler les activités avancées entre les objets
  - Protège les applications Android via SEDalvik (Aline Bousquet) et SEAndroid
  - Protection des plateformes et logiciels/services Java
- Utilisation **sur les clients** (notamment Android), **les serveurs et les Clouds** (PaaS/SaaS)

SEWeb - thèse de Maxime Fonda avec Qual'Net

- **Constat :** protection obligatoire quasi-inexistante pour les applications Web (injections, élévations de privilège, ...)
- **MAC efficace au niveau HTTP**
- **Contextes de sécurité** et **contrôle des flux directs** pour les requêtes/sessions HTTP
- **Modélisation de l'application :** permet de calculer exactement les politiques directes
- **Avantages**
  - Fonctionne sur tout type de serveur Web (IIS, Apache, ...)
  - Génération des scénarios de test des politiques
  - Traite la configuration/programmation de la protection
  - Protection des applications et services Web
- Utilisation **sur les serveurs et les Clouds** (PaaS/SaaS)

PIGAInfiniband - thèse de Damien Gros avec le CEA

- **PIGA-MAC avec un surcoût nul**
- **Pas d'intervention du noyau** pour les requêtes/réponses et **moniteur de référence PIGA déporté**
- **Performance/Tolérance aux pannes :** redondance de serveurs PIGA
- **Avantages**
  - Pas d'overhead sur les noeuds de calcul
  - Moniteur PIGA performant sur une machine dédiée
  - Répartition de la charge sur plusieurs serveurs
- Détection/Prévention **sur les systèmes HPC, les grilles et les Clouds**

Protection en profondeur des systèmes hétérogènes de virtualisation et d'infrastructures de Cloud

- **Contributeurs :** Bousquet, Briffaut, Rouzaud-Cornabas plus des étudiants dont Afoulki, Lefebvre
- **PIGA-Virt**
  - contrôle les flux internes et entre les machines virtuelles
  - indépendance et optimisation vis à vis de l'hyperviseur
- **PIGA-Cloud**
  - Mécanisme de désignation répartie des machines virtuelles supportant les migrations
  - contrôle des flux entre les machines virtuelles et l'hôte
- **Protection d'infrastructures de Cloud hétérogènes** (IaaS)

Thèses d'Aline Bousquet et d'Arnaud Lefray en commun avec l'équipe INRIA Avalon

- **Projet européen Seed4C**
  - Réseau de moniteurs de référence
  - Un moniteur couvre la palette des mécanismes de sécurité (cryptographie, protection, hardware)
  - Un langage dédié permet d'exprimer les missions de sécurité
  - Une approche globale d'ordonnancement/placement permet de répartir les missions sur les noeuds
- **Avantages**
  - Supporte tout type de Cloud et de fédération
  - Optimisation de la sécurité via une adaptation aux décisions
  - Le réseau de moniteurs permet des propriétés globales via des échanges transparents des contextes
- **Change radicalement la sécurité des Clouds** (IaaS/PaaS/SaaS)

Travail sur différents aspects via des partenariats

- **Historiquement :** CEA et HPC
- **En france et aux états unis**
  - Web : Qual'Net
  - Android/Intergiciel/Télécom : Bell Labs / Gemalto
  - Mobilité/médical : différentes PMEs
- **Académique et Europe**
  - Intergiciel, Cloud, préservation de l'énergie, mobilité : INRIA, LIP6, LIPN, LaBRI
  - Advisory Board sur la sécurité du Cloud : en france via les principaux acteurs et en europe (Espagne, Finlande)
- **Caractère pionnier : avancées fonctionnelles basées sur une approche scientifique extensible à d'autres domaines** (ex : préservation de l'énergie)