PIGA-Cloud : une protection obligatoire des environnements d'informatique en nuage

Zaina Afoulki*, Aline Bousquet*, Jérémy Briffaut*, Laurent Clévy**,
Jonathan Rouzaud-Cornabas***, Christian Toinard*, Benjamin Venelle**

*ENSI de Bourges – LIFO, 88 bd Lahitolle, 18020 Bourges cedex, France
{zaina.afoulki, aline.bousquet, jeremy.briffaut, christian.toinard}@ensi-bourges.fr
**Alcatel-Lucent Bell Labs, 7 route de Villejust, 91620 Nozay, France
{laurent.clevy, benjamin.venelle}@alcatel-lucent.fr
***LIP ENS Lyon 46 allée d'Italie, F-69364 Lyon cedex 07, France
jonathan.rouzaud-cornabas@inria.fr

Résumé. La garantie de propriétés de sécurité nécessite la mise en place d'un contrôle d'accès obligatoire (Mandatory Access Control). Les Clouds supportent mal ces mécanismes sans offrir une protection pour tous les niveaux (hôte, invité, application, réseau). PIGA-Cloud garantit des propriétés avancées pour des flux indirects et des combinaisons variées de flux et protège en profondeur en contrôlant les flux entre les systèmes d'exploitation invités et l'hôte, les flux internes à un invité mais aussi les flux entre objets Java et les flux réseau. L'article montre comment PIGAiser des environnements aussi divers que des machines Unix, des applications Java et des Clouds. Il étend les politiques d'accès directs SELinux et sVirt à une machine virtuelle Java pour au final protéger de façon avancée des Clouds de type IaaS, PaaS ou SaaS. L'approche simplifie l'administration des politiques directes en empêchant les millions de vulnérabilités résiduelles. Ce travail est partiellement supporté par le projet européen Seed4C.

1 Introduction

Pour garantir des propriétés de confidentialité et d'intégrité, il est nécessaire d'avoir d'une part des mécanismes cryptographiques pour chiffrer et signer les informations et d'autre part des protections qui contrôlent les accès à l'information. Les deux sont indispensables. Ici nous ne traitons que du contrôle d'accès et de la seule méthode permettant des garanties à savoir une protection du type MAC qui met les politiques de protection hors de portée des usagers finaux et même de l'administrateur système (root) de la machine. L'approche développée dans PIGA-OS (J. Briffaut, 2011), durant le défi sécurité Sec&Si de l'Agence Nationale de la Recherche, a montré qu'il est nécessaire d'avoir une protection en profondeur c'est-à-dire couvrant tous les niveaux d'un système (interface graphique, processus, application et réseau) afin de contrôler efficacement les flux d'informations et de s'adapter dynamiquement aux différents domaines d'usages. En effet, la sécurité d'un système repose sur la sécurité de chacune de ses couches : une fragilité à un seul niveau compromet la garantie visée. Cependant, offrir une protection en