

Campagne 2010

Fiche descriptive de la thèse

Encadrant Orange Labs: Marc Lacoste

Adresse électronique de l'encadrant : marc.lacoste@orange-ftgroup.com

Site: Orange Labs, Issy-Les-Moulineaux

Sujet de la thèse : Architecture de sécurité globale et mécanismes d'auto-protection pour le « cloud computing »

Contexte global de l'étude et état de l'art

L'émergence récente du « *cloud computing* » ouvre de nombreuses perspectives pour un opérateur de télécommunications comme Orange. Ce nouveau modèle d'architecture et de programmation largement répartie est basé sur l'idée d'externalisation d'un système d'information à des tiers pour fournir ressources et services à la demande et sur mesure sur le réseau. Les bénéfices escomptés sont nombreux: gestion flexible et dynamique de ressources dont l'administration est simplifiée par son automatisation, mise à disposition quasi-illimitée de ressources de calcul, réseau, ou de stockage grâce aux techniques de virtualisation entraînant économies d'échelle et réductions importantes de coûts de gestion d'infrastructure. Plusieurs acteurs majeurs comme Microsoft et Google proposent déjà des solutions de type « cloud ».

Cependant, l'ouverture des systèmes et le partage des ressources associées posent de nombreux problèmes de sécurité, qui reste l'une des barrières majeures pour l'adoption de ces technologies [4]. De nouveaux risques viennent se superposer aux menaces traditionnelles: vulnérabilités introduites par la *virtualisation des plates-formes* comme les hyperviseurs [1]; incertitudes sur la *sécurité réseau* en termes de sécurisation des accès et de placement des contre-mesures dans des topologies complètement virtualisées; *isolation et la protection des données personnelles* sur des plates-formes multi-tenants; et plus généralement *instauration de la confiance* entre utilisateurs et fournisseurs de solutions « cloud ».

Si les techniques traditionnelles de contrôle d'accès et de chiffrement restent applicables dans le contexte du « cloud », ces nouvelles menaces requièrent des mécanismes spécifiques. Malheureusement, peu de solutions existent aujourd'hui pour traiter ces problèmes [6][7]. De plus, ces mécanismes sont hétérogènes et fragmentés, avec un *manque de vision d'ensemble sur leur orchestration* et intégration avec des techniques protection traditionnelles au sein d'une architecture de sécurité globale.

Par ailleurs, la forte dépendance des menaces en fonction du modèle de service et de déploiement du « cloud », la réactivité nécessaire pour déployer les contre-mesures, et l'impossibilité d'une administration manuelle de la sécurité requièrent une *gestion flexible et automatisée de la sécurité* dans ces environnements, ce qui n'est pas le cas aujourd'hui.

L'objectif de cette thèse est d'apporter des éléments de réponse aux deux lacunes majeures précédentes.

Approche méthodologique

Le sujet de la thèse poursuit un objectif double. Il s'agit d'une part de proposer et mettre en œuvre une **architecture de sécurité de bout en bout** pour un environnement de type « cloud » fournissant une vue d'ensemble et intégrée des mécanismes de protection. Il s'agit aussi de définir au sein de cette architecture globale de sécurité, une architecture et des mécanismes permettant **l'auto-protection du « cloud »**.

Pour atteindre le premier objectif, de nombreux travaux [2] ont démontré la viabilité de *l'approche à composants* pour concevoir de manière souple des systèmes complexes à partir de briques hétérogènes, en particulier pour atteindre une sécurité forte mais flexible en formulant le problème comme une reconfiguration architecturale d'un ensemble de composants de sécurité. Cette approche sera donc explorée pour réaliser la composition, l'orchestration, et la reconfiguration de services de sécurité dans un « cloud » (par exemple sous forme de Web Services) afin de pouvoir composer au sein d'une architecture de sécurité globale des mécanismes élémentaires de chiffrement, de pare-feux, ou de tunneling. Ces services exprimeront les propriétés de sécurité fournies sous forme de *contrats*, par exemple de type SLA (Service Level Agreement). L'objectif est de pouvoir garantir le respect d'un contrat global de sécurité au niveau de l'ensemble de l'infrastructure.

Pour atteindre le deuxième objectif, l'approche introduite par IBM de *gestion autonome de la sécurité* (« *autonomic computing* ») [3] a également démontré son intérêt pour réaliser une infrastructure où les coûts d'administration de la sécurité soient minimisés, en permettant également de satisfaire des besoins de sécurité multiples ainsi que de réagir très rapidement aux menaces détectées. Dans cette approche, un système devient *auto-protégeable* car les services de sécurité sont automatiquement adaptés en fonction du niveau de risque ambiant pour fournir une protection optimale. Des travaux récents [5] ont défini un canevas logiciel générique à composants appelé ASPF permettant l'auto-protection de systèmes. Le doctorant devra évaluer dans quelle mesure ASPF répond aux besoins d'une gestion autonome de la sécurité d'un « cloud » et/ou proposer les extensions nécessaires pour y parvenir.

Objectifs de la thèse

- *Spécification et mise en oeuvre d'une architecture de sécurité de référence pour le « cloud »* : L'approche à composants sera privilégiée pour la définition de l'architecture. Il s'agira de décrire comment orchestrer et composer dynamiquement différentes briques de sécurité comme des hyperviseurs, des éléments matériels de sécurité (par exemple de type TPM), des contre-mesures réseau (pare-feux, IDS/IPS, VPNs, VLANs...), des mécanismes de stockage sécurisé et de gestion de la privacy, ou des composants spécifiques de gestion de la confiance. Les composants devront expliciter sous forme de contrats les garanties de sécurité fournies, qui seront composés pour dériver les garanties de sécurité au niveau du « cloud ». Cette architecture de bout en bout sera validée en réalisant un prototype correspondant de « cloud » sécurisé.
- *Spécification et implantation de mécanismes d'auto-protection pour le « cloud »* : Le doctorant devra identifier les composants nécessaires à la réalisation d'une ou plusieurs boucles d'auto-protection pour gérer la sécurité d'un « cloud » de manière autonome. Il pourra s'appuyer sur des travaux existants comme le canevas logiciel ASPF pour définir l'architecture d'auto-protection correspondante. Ces composants de sécurité seront ensuite implantés et intégrés dans le prototype de « cloud » sécurisé.

Résultats attendus

- Analyse de l'état de l'art des mécanismes de sécurité pour le « cloud computing » et pour la sécurité des systèmes autonomes.
- Proposition et spécification d'une architecture de référence à composants pour un « cloud » sécurisé orchestrant les mécanismes précédents. Définition de contrats de sécurité explicitant les propriétés individuelles de sécurité fournies par ces composants, et étude de leur composition pour obtenir les garanties de sécurité de niveau « cloud »
- Implantation de cette architecture dans un prototype de « cloud » sécurisé.

- Spécification d'un raffinement de l'architecture de sécurité permettant la mise en œuvre d'une ou plusieurs boucles d'auto-protection pour un « cloud ».
- Implantation du canevas logiciel correspondant au sein du prototype de « cloud » sécurisé pour obtenir un prototype réaliste de « cloud » auto-protégeable.
- Validation de l'architecture et des prototypes obtenus sur des cas d'usage applicatifs.

Défis scientifiques

- *Hétérogénéité des mécanismes de sécurité pour le « cloud »*: il s'agit d'intégrer au sein d'une même architecture de sécurité des briques élémentaires provenant de domaines de recherche très divers comme la sécurité des systèmes d'exploitation, les techniques de virtualisation, la sécurité réseau, la cryptographie, la privacy, la sécurité des systèmes autonomes, et les architectures à composants.
- *Réalisation de boucles d'auto-protection* : la réalisation de chaque élément de telles boucles est un défi scientifique à part entière. On peut citer l'attentivité au contexte pour évaluer le niveau de risque ambiant, les algorithmes de décision permettant de modifier la configuration des mécanismes de sécurité, ou la réalisation de services de sécurité adaptables. Une « question dure » associée est la spécification des stratégies d'adaptation de gestion de la sécurité dans ces systèmes. Enfin, rendre la sécurité adaptable ne devra pas mettre en danger la sécurité elle-même en introduisant de nouvelles vulnérabilités, ni présenter un impact trop important sur les performances.

Planning global du déroulement de la thèse

Première année:

- Analyse de l'état de l'art: mécanismes de sécurité pour le « cloud », canevas logiciels pour la sécurité autonome, architectures à composants.
- Première version d'architecture et de canevas logiciel pour un « cloud » sécurisé avec capacités d'auto-protection.

Deuxième année:

- Spécification et implantation d'une architecture de sécurité de référence pour « cloud ».
- Raffinement et implantation dans un prototype de « cloud » auto-protégeable.

Troisième année:

- Finalisation de l'architecture et des prototypes.
- Validation de l'architecture et des prototypes (performances, cas d'usage applicatifs...).
- Rédaction du manuscrit de thèse et soutenance.

Références

1. P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. "Xen and the Art of Virtualization". *ACM Symposium on Operating Systems Principles (SOSP)*, 2003.
2. E. Bruneton, T. Coupaye, M. Leclerc, V. Quema, and J.B. Stefani. "An Open Component Model and its Support in Java". *International Symposium on Component-Based Software Engineering (CBSE)*, 2004. Software available at <http://fractal.objectweb.org>.

3. D. Chess, C. Palmer, and S. White, "Security in an Autonomic Computing Environment". *IBM Systems Journal*, 42(1):107–118, 2003.
4. Cloud Security Alliance. "Top Threats To Cloud Computing". Technical Report, March 2010. Available at: <http://www.cloudsecurityalliance.org/topthreats.html>
5. R. He, M. Lacoste, and J. Leneutre. "A Policy Management Framework for Self-Protection of Pervasive Systems". *International Conference on Autonomic and Autonomous Systems (ICAS)*, 2010.
6. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds". *ACM Conference on Computer and Communications Security (CCS)*, 2009.
7. J. Rutkowska, and R. Wojtczuk. "Detecting and Preventing the Xen Hypervisor Subversions". *BlackHat Technical Security Conference (BLACKHAT)*, 2008.