End-to-end Security Architecture and Self-Protection Mechanisms for Cloud Computing Environments

Sujet proposé par Hervé DEBAR
Directeur de thèse: Hervé DEBAR
Doctorant: Aurelien WAILLY
Unité de recherche UMR 5157 Services répartis, Architectures, MOdélisation, Validation, Administration des Réseaux

Domaine: Département Sciences et technologies de l'information et de la communication
Secteur: Mathématiques, STIC, nanotechnologies
Thème: Sécurité
Sous-thème: Cryptologie, sécurité informatique

Projet

SUJET ATTRIBUE NE PAS CANDIDATER

The rise of cloud computing opens a whole new future for telcos like Orange. This disruptive distributed computing model for large-scale networks is based on the idea of outsourcing corporate IT infrastructures to third parties, a shared pool of computing, storage, and networking resources and services becoming accessible rapidly and on demand. Forecasted benefits include flexible and dynamic resource provisioning, simpler and automated administration of IT infrastructures, and sharing of nearly unlimited CPU, bandwidth, or storage space thanks to resource virtualization, with scalability improvements and massive cost reductions in terms of infrastructure management. Several major IT players like Amazon, Microsoft and Google are thus already proposing cloud computing solutions.

However, open systems and shared resources raise many security challenges, making security one of the major barriers to adoption of cloud computing technologies [4]. In addition to traditional threats, new issues should be addressed such as: vulnerabilities due to virtualization of computing infrastructures [1]; unclear effectiveness of traditional network security in terms of authorization and placement of security controls in fully virtualized networks; data isolation and privacy management in multi-tenant environments; and above all how to build and manage trust between users and cloud service providers.

If traditional security techniques such as encryption remain relevant for cloud infrastructures, those new threats require specific protection mechanisms. Unfortunately, few solutions are available to tackle those challenges [6][7]. Available mechanisms are highly heterogeneous and fragmented, with lack of an overall vision how to orchestrate them into an integrated security architecture for cloud environments.

Besides, the strong dependency of threats on the cloud service delivery and deployment models , the extremely short response times required to activate system defenses efficiently, and the impossibility of manual security maintenance call for a flexible, dynamic, and automated security management of cloud infrastructures, which is clearly lacking today. The ambition of this PhD is to provide elements of answer to those unsolved issues.

Enjeux

The objective of the PhD is twofold: (1) propose and implement an end-to-end security architectural blueprint for cloud environments providing an integrated view of protection mechanisms; and (2) define within that architecture, mechanisms enabling self-protection of the cloud infrastructure.

To reach the first objective, a large number of studies [2] demonstrated the viability of component-based designs to build complex systems from heterogeneous building blocks and reach flexible and yet security. That approach will be explored to orchestrate and adapt security services in a cloud (e.g., as Web Services) to compose flexibly inside a unified security architecture individual security services. Security properties provided by individual security services will be expressed as composable contracts, e.g., Service-Level Agreements (SLAs), to derive overall security objectives guaranteed by the cloud infrastructure.

To reach the second objective, IBM's autonomic computing approach [3] for self-managed security also proved its interest to build security infrastructures with minimal security administration overheads, which may satisfy multiple security requirements, and react rapidly to detected threats: security parameters are autonomously negotiated with the environment to match the ambient estimated risks and achieve an optimal level of protection. A first generic component-based framework for self-protection has been defined [5]. A first part of the PhD work will be to study whether this framework is sufficient for self-management of cloud security, or to define the necessary extensions for that purpose.

Objectives of the PhD

- Design and implement a reference security architecture for cloud environments. Component-based designs will be explored to describe how to orchestrate and dynamically compose different security building blocks like hypervisors, hardware security elements (e.g., TPMs), network protections (firewalls, IDS/IPS, VPNs), and secure storage, privacy-enhancing, or trust management mechanisms. Each component will explicit its guaranteed security properties using contracts, which will be composed to derive the overall cloud security objectives. This end-to-end security architecture will be validated through the realization of a prototype of secure cloud.

- Specify and implement self-protection mechanisms within the cloud. The PhD student will identify the components necessary to realize one or more self-protection loops to make cloud security self-managed. A self-protection architecture will also be defined. The identified security components will then be implemented and integrated into the prototype of secure cloud.

Remarques additionnelles

References

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. 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. 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.