PhD Offer

by Orange Labs, Issy-Les-Moulineaux, Paris region, France
and Ecole des Mines de Nantes, Nantes, France

==

Title

Unified architecture isolation and mechanisms protecting
against side channels for decentralized Cloud infrastructures

Environment and applications

This PhD will be co-supervised by researchers from Orange's Lab at Issy-Les-Moulineaux (Paris region) and …cole des Mines de Nantes at Nantes.

The application procedure is open until a suitable candidate has been
selected. In order to start the PhD soon, a fast-track decision process will be used.

In order to apply, please send to:

Marc.Lacoste@orange.com, Mario.Sudholt@mines-nantes.fr

the following information:

- A short CV that contains all pertinent information on your knowledge and competences relevant for the research and technical challenges of the PhD.

- Detailed information about your MSc (domain, thesis, grades).

- A short motivation statement.

- At least two addresses of researchers that may provide references for you.

Context

The emerging paradigm of decentralized Cloud infrastructures (DCIs) -
eg., Fog Computing, Swarm Computing, ...) place virtualized Cloud resources at the network frontiers. These hybrid architectures

include standard data centers (DCs) and "integrated" peripherals, such as PoPs that play the role of "mini-DSc." They have several advantages: the geographical proximity of code and data, small latencies, support for mobility ... Their heterogeneity, however, underlies several critical security-related challenges:

1. Isolation breaches: security guarantees between two endpoints of a DCI are based on a strong isolation hypotheses between execution environments (VMs). In practice, this hypothesis is not valid, notably because of resource sharing (eg., of cache memory) between VMs in hypervisors. Such sharing entails indirect information flows (execution time, patterns of cache accesses) that can be exploited to steal of modify the data of clients.

2. Attack propagation: the heterogeneity of the virtualized architecture of an DCI may rapidly entail the propagation of attacks between the Cloud and embedded peripherals. Currently no unified isolation architecture for DCIs exists that provides an abstraction layer guaranteeing strong end-to-end isolation properties.

3. Applications: the DCI architectures are currently interesting for telecom-based Cloud operators because they harness their facilities. Protecting their security is therefore of high interest to telecom operators but requires strong end-to-end security guarantees including control over information flows.

Objective

The principal objective of his PhD is the provision of strong end-to-end isolation properties in the physical nodes of DCIs. To this end, the PhD student will work on two challenges.

- A layer for distributed security that permits to abstract the heterogeneity of security techniques and to avoid the propagation of threats between the Cloud and embedded peripherals. The resulting new virtualization architecture will bridge the current semantic gap between the different forms of virtualization in the Cloud and among peripherals.

- A set of effective countermeasures against side-channel attacks (SCAs) that may target resources from the application level to the hypervisor level via hardware that is part of virtualized platforms in each node of a DCI.

The following results are targeted:

1. The design of the unified security architecture.

2. Its implementation in terms of a container architecture with better isolation properties than current approaches.

3. An integrated set of countermeasures to SCAs in form of a tool box that supports different trade-offs between security, performance, genericity, compatibility with existing approaches, for software operating from the IaaS to the SaaS level.

4. The integration of the preceding results in a realistic DCI prototype infrastructure.

The following problems are of particular interest in the context of this thesis. As to isolation properties, a first problem consists in the proposal of countermeasures against complete, i.e. multi-level, attacks and not only attacks at a single hardware or software layer. A second problem concerns countermeasures enabling different trade-offs for the following properties: (1) the compatibility of different Cloud platforms, i.e., requiring no or few modifications to virtualization infrastructures; (2) supporting a high security level by removing or reducing information leaks; (3) no reliance on a specific hardware/software architecture.

As to attack propagation. the main problem consists in the heterogeneity of architectures for virtualization between the Cloud and embedded peripherals, a source of complexity and security weaknesses by itself. This problem should be handled by a security approach "by design" that provides end-to-end security guarantees.