SUPER CLOUD EUROSYS

1ST INTERNATIONAL WORKSHOP ON SECURITY AND DEPENDABILITY OF MULTI-DOMAIN INFRASTRUCTURES:

XDOM0 2017

23rd April 2017

Belgrade, Serbia

Co-located with the EuroSys 2017 conference

CALL FOR PAPERS

Paper submission deadline: 28th February 2017

Workshop description:

Multi-domain infrastructures are increasingly imposing themselves as leading architectures for distributed systems. They achieve effective convergence of cloud systems and networks through virtualization. They allow federating resource-specialized infrastructures into unified control and data planes for computing, storage, networking, and device resources, their architectures ranging from centralized to fully distributed (also known as cloud-of-clouds, edge, fog, etc.).

One central property of such infrastructures is also being software-defined: the domain abstraction plays a central role for resource control, either shallow, or reaching deep in multiple infrastructure layers. The control capabilities are more extensive for private infrastructures where security services may be selectively added at low-level, SDN also enabling full network control. In public networks, on the other hand, control is much reduced, as the hardware remains out of reach, visible only as a "big-switch" abstraction.

Due to their heterogeneity and complexity, such infrastructures raise acute security and dependability challenges. The potential of (insider) attacks renders many central software layers, such as the hypervisor, untrustworthy. This calls for primitives for secure isolated computation, and strong system mechanisms for trust guarantees across layers and domains. Similarly, making the infrastructure immune to cloud or network availability zone outage in a multi-provider setting, in order to avoid Internet-scale single point of failures, calls for fault-tolerant, replicated, and distributed control architectures.

Lack of control on the infrastructure also prevents building user-centric clouds and networks and full customization of security and their related benefits, e.g., overcoming vendor lock-ins, choosing best-of-breed providers (price, performance, etc.). Heterogeneity of system abstractions and mechanisms in the virtualization infrastructure remains a major barrier towards such goals.

This workshop focuses on new system architectures and mechanisms for security and availability of multi-domain infrastructures. The aim is to explore how such system-level solutions could allow the user to regain control over such infrastructures and address the previous security and resilience challenges. Platforms that include hybrid clouds, and SDN-based virtualized networks require novel models, architectures, designs, security and resilience mechanisms that go beyond traditional virtualization and networking architectures. Finding the right abstraction and system mechanisms can help enforce control at all (necessary) levels, both across domains and layers to enhance security and dependability of such infrastructures. Additionally, infrastructures of such complexity require holistic automation of security and dependability, posing new research problems on specification, enforcement, and management of policies and SLAs.

Workshop topics:

Specifically, we invite submissions focusing on advanced virtualization systems for secure and resilient multi-domain infrastructures, but not exclusively:

- Open, minimal, or modular hypervisor architectures
- Lightweight virtualization platforms
- VM, container, or unikernel isolation and protection across heterogeneous clouds
- Hardware security mechanisms in virtualized environments
- Trusted execution and trustworthy infrastructures
- Distributed secure computation in multi-clouds
- Multi-cloud storage systems
- Resilient database systems
- Network virtualization for multi-clouds
- Network embedding techniques
- Network slicing for multi-domains
- Resilient virtualized network functions
- Secure and dependable software-defined computing, storage, or networking
- Automation of security management for multi-clouds and virtualized networks
- Specification, negotiation, enforcement, monitoring, auditing of security policies

Paper/Presentation submission:

Authors are invited to submit original papers of up to 6 pages, with 10-point font, in a two-column format (including figures, tables and references). Submitted papers need not be anonymized.

Electronic submissions:

The submissions page at HotCRP is open:
https://hotcrp.com/

Important dates:

Position papers due:	28th February 2017
Author Notification:	22nd March 2017
Camera ready versions:	4th April 2017
XDOm0'17 Workshop:	23rd April 2017

Organisers:

Marc Lacoste, Orange Labs, France
marc.lacoste@orange.com

Fernando M.V. Ramos, University of Lisbon, Portugal
fvramos@ciencias.ulisboa.pt

H2020 SUPERCLOUD project
https://supercloud-project.eu/

Workshop committee:

General Co-Chairs
Marc Lacoste, Orange Labs, France
Fernando Ramos, University of Lisbon, Portugal
TPC Co-Chairs
Hervé Debar, Télécom SudParis, France
Ahmad-Reza Sadeghi, TU Darmstadt, Germany

Publication Chair
Barbara Gaggl, Technikon, Austria
Web Chair
Max Alaluna, University of Lisbon, Portugal
Programme Committee Members
TBC

XDOM0'17 workshop web page
http://xdom0-2017.supercloud-project.eu/home/index.html