

SUPERCLOUD WORKSHOP—XDOM0'17
Co-located with EuroSys 2017

General Information

The SUPERCLOUD Consortium organized a **workshop on Security and Dependability of Multi-Domain Infrastructures (XDOM0 2017)**. The workshop took place on Sunday, **23rd of April 2017** and was **co-located with the EuroSys 2017** Conference in **Belgrade/Serbia**.

The workshop was very successful, ran smoothly, and raised many **interesting discussions**. The topics of the workshop related to system-level control challenges, abstractions, and mechanisms for secure and resilient computation and networking on multi-domain infrastructures.

Session 1 focused on **"Network security"**. The program also featured a [keynote from Clémentine Maurice](#), from the Secure Systems Group at the Graz University of Technology, in Austria. She gave an exciting and insightful talk on side-channel attacks in virtualized environments and isolation threats such as side-channels across cores, or across CPUs. Afterwards, Session 2 dealt with the subject of **"Systems Security"**. The XDOM0 workshop finally featured **four posters in the workshops poster session** in the evening that raised many interesting discussions with workshops and conference attendees, SUPERCLOUD being represented with one poster on the Sirius virtualization system.

XDOM0 2017

International Workshop on Security and Dependability of Multi-Domain Infrastructures

OVERVIEW


Multi-domain infrastructures are rapidly growing as "the" broad class of architecture for large-scale distributed systems that are software-defined, virtualize resources, and blend multiple clouds and networks. Acute **security and dependability** challenges, such as preventing insider attacks or avoiding wide-area single points of failure, require novel approaches, both to system architecture and to security and resilience mechanism implementation, to restore a high level of control over infrastructure layers and across domains, and to overcome infrastructure heterogeneity and complexity.

The aim of the workshop was to bring together **researchers and practitioners** from security and dependability Communities in virtualization of **systems, storage, and networking**, to discuss current trends and challenges and propose novel system-level solutions for the design, implementation, and deployment of secure and resilient multi-domain infrastructures.

Key Data:

<i>Start Date:</i>	1 st February 2015	<i>Consortium:</i>	9 partners (6 countries)
<i>End Date:</i>	31 st January 2018	<i>Project Coordinator:</i>	Dr. Klaus-Michael Koch coordination@supercloud-project.eu
<i>Duration:</i>	36 months	<i>Technical Leader:</i>	Dr. Marc Lacoste marc.lacoste@orange.com
<i>Project Reference:</i>	643964	<i>Project Website:</i>	www.supercloud-project.eu
<i>Project Costs:</i>	€ 6.863.279		



 This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 643964. This work is supported (also) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0091. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government.

Technical Takeaways

Among technical takeaways, it seems there are still a lot of challenges ahead for full control of multi-domain infrastructures to lift security and availability barriers.

Notably: (1) the virtualization infrastructure design should be the starting point, such as the network hypervisor and embedding to bridge virtual and physical worlds; (2) isolation remains a major challenge, e.g., for user-centric, hardware-based isolation (e.g., Trustzone), or in terms of new frontiers in side-channel attacks and mitigation; (3) much remains to explore on the impact of multi-tenancy, e.g., for DDoS mitigation; (4) policies and policy-based management are keys for control and security automation; and (5) the control system must also be resilient to attacks.

Accepted Papers

5 papers were accepted out of 10 submissions, yielding a 50 % acceptance rate. The program was well-balanced with 2 papers accepted from SUPERCLOUD, respectively on the Sirius secure and dependable network virtualization system (FFCUL) and on SDN-based network attack mitigation (IMT). 3 papers were also came from outside the project, notably from the US and Australia, or from other Europeans project such as H2020 SERECA:

- **“Implementing Geo-Blocking and Spoofing Protection in Multi-Domain Software Defined Interconnects”**, Himal Kumar (UNSW, Australia), Anu Mercian (Hewlett-Packard Enterprise, US), Sujata Banerjee (VMware, US), Craig Russell (CSIRO Data 61, Australia), and Vijay Sivaraman (UNSW, Australia).
- **“Secure and Dependable Multi-Cloud Network Virtualization”**, Max Alaluna, Eric Vial, Nuno Neves, and Fernando M. V. Ramos (LaSIGE, Faculdade de Ciencias, Universidade de Lisboa, Portugal).
- **“Towards intrusion-resilient security monitoring in multi-cloud infrastructures”**, Hans P. Reiser (University of Passau).
- **“Adaptive Policy-driven Attack Mitigation in SDN”**, Rishikesh Sahay (Télécom SudParis), Gregory Blanc (Télécom SudParis), Zonghua Zhang (IMT Lille Douai), Khalifa Toumi (Télécom SudParis), and Hervé Debar (Télécom SudParis).
- **“TrApps: Secure Compartments in the Evil Cloud”**, Stefan Brenner (TU Braunschweig), David Goltzsche (TU Braunschweig), and Rüdiger Kapitza (TU Braunschweig).

Published papers are available in the ACM Digital Library at this URL: <http://dl.acm.org/citation.cfm?id=3071064>

Workshop Programme

08.30 – 09.00	Registration
09.00 – 09.10	Opening and Welcome
09.10 – 10.30	Session 1: Network Security
10.30 – 11.00	Coffee Break
11.00 – 12.00	Keynote: Microarchitectural Attacks in the Cloud
12.00 – 12.20	Session 2: Systems Security
12.20 – 12.30	Closing

Key Data:

<i>Start Date:</i>	1 st February 2015	<i>Consortium:</i>	9 partners (6 countries)
<i>End Date:</i>	31 st January 2018	<i>Project Coordinator:</i>	Dr. Klaus-Michael Koch coordination@supercloud-project.eu
<i>Duration:</i>	36 months	<i>Technical Leader:</i>	Dr. Marc Lacoste marc.lacoste@orange.com
<i>Project Reference:</i>	643964	<i>Project Website:</i>	www.supercloud-project.eu
<i>Project Costs:</i>	€ 6.863.279		



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 643964. This work is supported (also) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0091. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government.