

# C&ESAR 2019

## Virtualization and Cybersecurity

November 19 - 20, 2019 – Rennes - France



### About C&ESAR

Every year since 1997, the French Ministry of Defense has organized a cybersecurity event to bring together governmental, industrial, and academic stakeholders. This event is both educational and scientific, gathering experts, researchers, practitioners and decision-makers in order to explore an important topic within the field of cybersecurity. The chosen themes are covered from both a theoretical and practical perspective, with a strong emphasis on educational approach in order to help information security professionals with different backgrounds share a common understanding of complex issues. This interdisciplinary approach within the cybersecurity profession allows operational practitioners to learn about and anticipate future technological inflexion points, and for industry and academia to confront research and product development to operational realities of the field. Conference occurs during [European Cyber Week \(ECW\)](#).

### Virtualization and cybersecurity

Virtualization is driven by dematerialization of data. Introduced gradually by the Cloud and then by the IoT (Internet of Things), virtualization is amplified by the development of Artificial Intelligence that allows new processing capabilities with the datalakes. Value-added information is now based on data with spatial and temporal materiality that is difficult to locate.

The application frameworks are multiple. The future 5G will introduce network-level virtualization (SDN – Software Defined Network) and services (NFV - Network Functions Virtualization). Autonomous systems in transport already integrate virtualization into embedded systems with strong compartmentalization and exchange requirements.

Cyber threat also evolves in these new contexts. It is important to clarify whether these contexts do not advantageously offer new opportunities to attackers and to analyse ways to prevent against the risks involved.

Thus, the adaptation of attack detection to automatic changes of virtualized systems without degradation of the service, offer becomes a real challenge. Virtualization is based on orchestration features whose robustness must be proven.

To meet these challenges, services evolve to data-centric security profiles.

C&ESAR conference proposes to analyse virtualization from the point of view of the protection and sharing of data, under cyber threat.

Program committee will appreciate submissions in the following areas:

- Cyber threats and securing next-generation networks: SDN / NFV, 5G
- Embedded security: tightness and compartmentalization, vulnerabilities and hypervisors versus containers
- Protection of virtualization orchestrators
- Prospects for encryption virtualization
- Virtualization of detection functions
- AI contribution to securing virtualization in protection and detection
- Virtualization platforms and usage for cybersecurity: validation problem
- Opportunities for data-centric security for virtualized environments

## Submission process

- *First phase:* the proposals (3 to 6 pages) shall be submitted as a PDF file by **July 5<sup>th</sup>, 2019 (updated)** at the latest via <https://www.easychair.org/conferences/C&ESAR2019>. Each submission shall include a title, the category of communication (analysis, protection, attacks, qualification and certification), the authors' names and affiliation, the email address of the corresponding author, an abstract (10 lines max.), and a list of keywords. The authors will be notified of their proposal acceptance by **September 3<sup>rd</sup>, 2019**.
- *Second phase:* authors shall send the camera-ready version of their paper (8 to 16 pages) by **October 4<sup>th</sup>, 2019** to [contact@cesar-conference.org](mailto:contact@cesar-conference.org), cc to [benoit-f.martin@intra.def.gouv.fr](mailto:benoit-f.martin@intra.def.gouv.fr). Authors whose papers are accepted commit to address reviewers comments in the final version.
- *Instructions for the camera-ready version of the paper:* PDF in A4 layout without page numbering, following the Springer Lecture Notes in Computer Science template:  
LaTeX template: <ftp://ftp.springernature.com/cs-proceeding/llncs/llncs2e.zip>;  
Word template: <ftp://ftp.springernature.com/cs-proceeding/llncs/word/splnproc1703.zip>.
- *Language and selection criteria:* the papers can be written in French or in English. Selection criteria include clarity and educational dimension, as well as the respect of the theme of the conference and the guidelines of this call for papers. Specialized technical papers will be taken into consideration to the extent that they contribute to explaining and analyzing the state of the art or its deficiencies, rather than presenting only individual technical contributions. Accepted papers will be published in both online and printed versions in the proceedings of the conference.

## Important dates

- Submission of the proposals (long abstracts between 3 to 6 pages): **July 5<sup>th</sup>, 2019 (updated)**
- Notification to authors: **September 3<sup>rd</sup>, 2019**
- Final version (8 to 16 pages): **October 4<sup>th</sup>, 2019**
- Conference: **November 19<sup>th</sup> - 20<sup>th</sup>, 2019**

## Program committee

José ARAUJO (ANSSI)

Christophe BIDAN (CentraleSupélec)

Frédéric CUPPENS (IMT - Atlantique)

Guillaume DUVEAU (MINARM - DPID)

Sylvain GOMBAULT (IMT Atlantique)

Sylvain LAFARGUE (SAFRAN E&D)

Guillaume MEIER (AIRBUS)

Eric WIATROWSKI (ORANGE)

Boris BALACHEFF (HP)

Yves CORREC (ARCSI)

Herve DEBAR (Télécom SudParis)

Ivan FONTARENSKY (THALES)

Patrick HEBRARD (NAVAL Group)

Benoît MARTIN (MINARM - DGA-MI)

Ludovic PIETRE-CAMBACEDES (EDF)

## Sponsors

