

C&ESAR 2019

Virtualisation et Cybersécurité

19 – 20 Novembre 2019 – Rennes - France



À propos de C&ESAR

Depuis 1997, le ministère français des armées organise chaque année un colloque dédié à la cybersécurité réunissant les acteurs gouvernementaux, industriels et académiques. Cet événement vise un double objectif, scientifique et opérationnel, en rassemblant experts, chercheurs, praticiens et décideurs, pour un tour d'horizon sur un sujet particulier. Le thème choisi est abordé dans une perspective opérationnelle aussi bien que théorique, avec une dimension didactique prononcée pour aider les professionnels de secteurs différents à partager une compréhension commune. Cette approche interdisciplinaire de la cybersécurité permet aux utilisateurs de terrain d'étudier et d'anticiper les avancées théoriques ou techniques, et aux industriels ou aux scientifiques de confronter la recherche et le développement des produits aux réalités opérationnelles. La conférence se déroule dans le cadre de la European Cyber Week (ECW).

Virtualisation et cybersécurité

L'actualité de la virtualisation est portée par la dématérialisation des données. Introduite progressivement par l'émergence du cloud, puis par le développement des objets connectés elle est amplifiée par l'arrivée de l'Intelligence artificielle qui permet de nouvelles capacités de traitement des données massives. L'élaboration d'informations à valeur ajoutée s'appuie désormais sur des données dont il devient difficile de saisir au sens propre la matérialité spatiale et temporelle.

Les cadres d'application sont multiples. La future 5G poursuivra la virtualisation au niveau du réseau (SDN - Software Defined Network) et des services (NFV - Network Functions Virtualization). Les systèmes autonomes (transports, véhicules, drones...) et les terminaux d'utilisateurs intègrent déjà la virtualisation dans des systèmes embarqués avec des exigences de cloisonnement et d'échanges renforcés.

La menace cyber s'adapte à ces nouveaux contextes. Il convient de s'interroger si ces environnements n'offrent pas avantageusement de nouvelles opportunités aux attaquants et d'analyser les moyens de se prémunir des risques induits. En particulier, l'adaptation de la Lutte Informatique Défensive (LID) aux changements automatiques des systèmes d'informations virtualisés sans dégradation de l'offre de service devient un véritable défi. La virtualisation repose sur des fonctions d'orchestration de déploiement dont la robustesse doit être éprouvée.

Pour répondre à ces enjeux, les services évoluent en s'appuyant sur des profils de sécurité centrés sur la donnée.

La conférence C&ESAR propose ainsi d'analyser les différentes dimensions de la virtualisation sous l'angle de la protection et du partage de la donnée et sous la pression de la menace cyber.

Le comité de programme attend des propositions de communication sur :

- Les menaces cyber et la sécurisation des réseaux de nouvelle génération : SDN/NFV, 5G
- La sécurisation de l'embarqué : étanchéité et cloisonnement, vulnérabilités hyperviseurs versus conteneurs
- La protection des orchestrateurs de virtualisation
- Les perspectives de virtualisation du chiffrement
- La virtualisation des fonctions de détection
- L'apport de l'IA pour la sécurisation de la virtualisation en protection et en détection
- Les plates-formes et usage de la virtualisation pour la cybersécurité : problématique de validation
- Les opportunités de la sécurité centrée sur les données pour les environnements virtualisés

Modalités de soumission

- *Première étape* : les propositions de communication (3 à 6 pages) sont à soumettre au plus tard le **28 juin 2019** via <https://www.easychair.org/conferences/C&ESAR2019> au format PDF. Doivent y figurer le titre de la communication, les noms et prénoms des auteurs ainsi que leur affiliation, l'adresse électronique de l'auteur principal, un résumé (10 lignes max.) et une liste de mots clés. Les auteurs seront prévenus de l'acceptation ou du rejet le **3 septembre 2019**.
- *Seconde étape* : les auteurs envoient au plus tard le **4 octobre 2019** une version définitive de la communication (de 8 à 16 pages) à contact@cesar-conference.org, copie à benoit-f.martin@intra-def.gouv.fr. Les auteurs s'engagent dans cette version définitive à prendre en compte les remarques des relecteurs transmises lors de la notification de la décision.
- *Instructions pour la version définitive de l'article* : document PDF au format A4 sans les numéros de page, suivant le modèle Springer Lecture Notes in Computer Science (modèle LaTeX : <ftp://ftp.springernature.com/cs-proceeding/llncs/llncs2e.zip>; modèle Word : <ftp://ftp.springernature.com/cs-proceeding/llncs/word/splnproc1703.zip>).
- *Langues et critères de sélection* : les communications peuvent être rédigées en français ou en anglais. Les critères de sélection seront principalement le respect du thème de la conférence et de l'appel à communications, la clarté et l'effort pédagogique. Les exposés techniques seront considérés dans la mesure où ils présentent aussi un état de l'art d'un domaine et non uniquement un résultat particulier. Les communications ne doivent pas être à vocation commerciale. Les communications acceptées seront publiées dans les actes du colloque.

Dates importantes

- Soumission des propositions de communications (entre 3 et 6 pages) : **28 juin 2019**
- Notification aux auteurs : **3 septembre 2019**.
- Version finale (entre 8 et 16 pages) : **4 octobre 2019**
- Conférence : **du 19 au 20 novembre 2019**

Comité de programme

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)

Partenaires

