Appel à communications pour C&ESAR 2022

Conseil de programmation de C&ESAR

mardi 10 mai 2022

Résumé

La conférence en cybersécurité C&ESAR sollicite des propositions de contribution sur le thème “Comment garantir la confiance dans un monde décentralisé ?”. La date limite de soumissions des résumés est le mercredi 18 mai 2022.

À propos de C&ESAR

Chaque année depuis 1997, le Ministère des Armées organise une conférence sur la cybersécurité, appelée C&ESAR. Cette conférence est désormais l'un des principaux événements de la European Cyber Week (ECW) organisée chaque automne à Rennes, France.

L'objectif de C&ESAR est de rassembler et faciliter les échanges entre divers acteurs gouvernementaux, industriels et universitaires ayant un intérêt pour la cybersécurité. Cet événement, à la fois pédagogique et scientifique, rassemble des experts, des chercheurs, des praticiens et des décideurs. Cette approche interdisciplinaire permet aux praticiens opérationnels de connaître et d'anticiper les futures (r)évolutions technologiques, et permet aux académiques et industriels de confronter la recherche et le développement de produits et services aux réalités opérationnelles. Chaque année, C&ESAR explore un sujet différent dans le domaine de la cybersécurité.

Le thème de cette année est : ***Comment garantir la confiance dans un monde décentralisé ?***. Ce thème est sous-titré : Contrôle et audit des interactions dans un système décentralisé. L'appel à communications complet est disponible sur une page web dédiée à l'appel et sous forme de fichier PDF.

Thème de C&ESAR 2022 : *Comment garantir la confiance dans un monde décentralisé ?*

Ce thème est sous-titré : Contrôle et audit des interactions dans un système décentralisé.

Résumé

C&ESAR sollicite des soumissions présentant des **états de l'art ou de la pratique clairs, des solutions innovantes ou des retours d'expérience pertinents** traitant du problème de la **confiance, d'un point de vue sécuritaire, dans les interactions au sein de systèmes décentralisés**. Comment faire confiance, notamment par le contrôle et l'audit, à la légitimité des interactions dans le cadre du travail à distance, du cloud hybride et d'autres concepts de décentralisation ? Le champ d'application couvre les questions techniques ainsi que les questions juridiques.

Parmi les principaux mots-clés, on trouve : Zero Trust, IAM, Travail à distance, Multi-Cloud hybride, législation internationale

Détail

La notion de confiance dans le cadre de cet appel renvoie aux notions d'intégrité, d'innocuité, d'adéquation à l'usage, … Puis-je me fier à ces données pour agir en conséquence ? Puis-je faire confiance à ce traitement pour le laisser "s'exécuter" dans mon système ou sur mes données ? Puis-je faire confiance à cette entité pour lui permettre d'accéder à ces services et données ? Puis-je (toujours) faire confiance à un sous-système (potentiellement le mien, et potentiellement uniquement un canal de communication) pour exécuter mes traitements et gérer mes données ?

Au "bon vieux temps" des systèmes d'information atomiques clos et gardés [2] [11], les enjeux de confiance se réduisaient (très) grossièrement à la question suivante : êtes-vous (ou votre initiateur) déjà dans le système, ou êtes-vous toujours en dehors ? Toute entité à l'intérieur du système (ou processus initié de l'intérieur) est *implicitement* légitime pour accéder, agir sur, agir au nom ou supporter le système [13]. Chaque entité composant le système (matériel ou logiciel) a été "vérifiée" par le biais d'un processus d'approvisionnement impliquant un certain niveau (variable) d'évaluation ; les données de votre système ont été principalement produites par vous-même ; les processus de votre système sont exécutés sous votre contrôle ; et, l'accès à votre système est principalement un problème de contrôle physique (pas un problème informatique), à l'exception de certains points bien identifiés tels que les sites Web et les serveurs de messagerie. L'administrateur a un contrôle (presque) total sur (presque) tout dans un périmètre clairement défini. Le jeu consiste à maintenir la confiance à l'intérieur de ce périmètre en maintenant les entités ou "ressources" non fiables à l'extérieur de ce périmètre. Cette approche de sécurisation de tels systèmes atomiques et sous contrôle est appelée le "Castle Security Model" [2] [11].

Depuis, les systèmes d'information ont beaucoup évolué. Les systèmes d'information sont de plus en plus décentralisés. Pour le cas "simple" d'un système d'information constitué de plusieurs enclaves entièrement contrôlées et interconnectées, l'utilisation de Réseaux Privés Virtuels (VPN) permet de revenir à une situation compatible avec le "Castle Security Model" (même si cela peut ne

pas être pertinent pour les attaques d'aujourd'hui qui, entre autres différences, impliquent plus de mouvements latéraux qu'au "bon vieux temps"). Cependant, les systèmes d'information d'aujourd'hui sont généralement plus décentralisés que cela et ont perdu plus de contrôle sur leurs mécanismes de défense et leurs dépendances. Ils peuvent avoir des contrôles physiques plus faibles des périmètres de leurs enclaves, comme dans le cas du *Travail à distance/domicile* et de l'*Internet des Objets* (IoT). Ils s'appuient de plus en plus sur le cloud et, de l'*Infrastructure as a Service* (IaaS) à la *Platform as a Service* (PaaS), perdent de plus en plus le contrôle d'une partie de leurs interconnexions, de leur isolement des processus voisins et de la pile d'exécution, perdant même le contrôle de leur charge utile dans le cas du *Software as a Service* (SaaS). Ils peuvent également accepter le fait que certains de leurs "composants de support" peuvent ne pas être administrés du tout, ou du moins pas à un niveau professionnel, comme c'est le cas avec la tendance *Bring Your Own Device* (BYOD). Le processus de décentralisation lui-même peut ne pas être totalement maîtrisé, comme dans le cas du Shadow IT qui est l'un des principaux risques de cybersécurité selon 44% des répondants à une récente enquête sur la cybersécurité [9]. Même si l'utilisation du cloud est contrôlée, il y a des problèmes de confiance avec celui-ci, comme le manque de contrôle sur l'accès des administrateurs du fournisseur de cloud pour 45 % des répondants, et l'absence de visibilité sur la chaîne d'approvisionnement du fournisseur de cloud pour 51 % des répondants. Globalement, 86% des entreprises estiment que les outils fournis par les fournisseurs de cloud ne permettent pas de sécuriser les données et que d'autres outils spécifiques sont nécessaires [9].

Zero Trust [7] [1] est un modèle de sécurité qui répond à une partie des enjeux de cybersécurité résultant de la décentralisation des systèmes d'information. Il gagne de plus en plus de terrain dans le monde réel et est déployé dans l'industrie [10] [9] ainsi que dans les institutions publiques [3] [4]. Plutôt qu'une architecture spécifique ou un ensemble de méthodes et de technologies, Zero Trust est un ensemble de principes de conception et de stratégies de gestion de la cybersécurité [8] [7]. Son principe principal est de ne jamais compter sur la confiance *implicite*. En particulier, les autorisations (non seulement pour l'accès mais pour tout type de transaction) ne doivent jamais être accordées uniquement sur la base de l'emplacement de son demandeur (de quel réseau provient la demande). Cela ne signifie pas que le système ne doit pas reposer sur la confiance, mais cette confiance doit être gagnée et renouvelée [13]. "[T]rust is never granted implicitly but must be continually evaluated" [7] avant (contrôle) et postérieur (audit) à son octroi. Ce principe n'est pas nouveau et remonte au Jericho Forum [6] en 2004 [7]. D'autres principes, tels que le *principe du moindre privilège* [12] [15], sont encore plus anciens mais sont devenus plus prégnants avec la décentralisation et plus faciles à appliquer avec les technologies modernes. Un autre principe important de Zero Trust est d'affiner la granularité des contrôles jusqu'aux transactions unitaires. Le but est d'autoriser le moins de privilèges nécessaires *juste pendant la durée* du besoin [2].

Tous les principes de Zero Trust ne sont pas couverts par C&ESAR 2022. Les définitions exactes de Zero Trust varient, mais la NSA le résume en 4 points

principaux [8] : a) “Coordinated and aggressive system monitoring, system management, and defensive operations capabilities” ; b) “Assuming all requests for critical resources and all network traffic may be malicious” ; c) “Assuming all devices and infrastructure may be compromised” ; d) “Accepting that all access approvals to critical resources incur risk, and being prepared to perform rapid damage assessment, control, and recovery operations”. Dans le cadre de cette définition du concept Zero Trust, C&ESAR 2022 se concentre sur les points b et c dans un cadre hautement décentralisé : à un niveau de granularité fine, comment gagner la confiance dans les demandes de ressources, le trafic réseau, les appareils supports et l'infrastructure en général ? Sous-entendu par cette question, mais non équivalent, le problème de l'authentification est l'une des principales préoccupations du concept Zero Trust [7] [14] [1], et en général des responsables de sécurité informatique [5] [3].

Bien qu'utile pour résoudre certains des problèmes liés à la confiance dans un système décentralisé, selon la définition utilisée, certaines des questions couvertes par C&ESAR 2022 peuvent ou non être incluses dans le concept Zero Trust.

Parmi celles-ci, il y a le problème de la confiance transitive et de la propagation de la confiance. Par exemple, dans le cas d'un développeur dans une enclave contrôlée qui pousse du code vers un SaaS de contrôle de version, qui pousse ce code vers un SaaS d'Intégration Continue / Déploiement Continu (CI/CD) d'un autre fournisseur, qui lui-même pousse les “binaires” résultants à un serveur web SaaS d'encore un autre fournisseur, quelles sont les solutions potentielles pour que le développeur puisse avoir plus de confiance (contrôle et audit) dans les différents SaaS pour ne pas abuser de leurs privilèges ? Quelles sont les solutions potentielles pour que les fournisseurs SaaS fassent confiance à d'autres fournisseurs pour agir fidèlement au nom du développeur, y compris et au-delà de potentiels gestionnaires de version et de compilateurs préservant les signatures ? Plus généralement, comment faire confiance à une entité auparavant inconnue ou non vérifiée qui commence à interagir avec votre système en votre nom ou au nom d'un de vos utilisateurs ? Comment compter sur la confiance des autres pour faire confiance à une interaction ?

Sur un autre sujet, l'évaluation de la confiance nécessite des (méta)données. Dans un système très décentralisé géographiquement pouvant déplacer des charges utiles entre enclaves, comment assurer la diffusion et la synchronisation de ces (méta)données de manière sécurisée compatible avec les contraintes temporelles du système et les lois applicables au propriétaire des (méta)données données, le propriétaire de la charge utile et l'emplacement où réside l'enclave d'exécution ?

Dans ce contexte, C&ESAR sollicite des soumissions présentant des **états de l'art ou de la pratique clairs, des solutions innovantes ou des retours d'expérience pertinents** sur le sujet “Comment garantir la confiance dans un monde décentralisé ?”.

Le périmètre couvre :

— toutes les étapes de la cybersécurité, de la collecte du besoin à la cyber-

défense opérationnelle ou au pentesting, en passant par le DevSecOps et l'élimination/retrait des équipements et systèmes ;
- tous types de systèmes tant que leur architecture est décentralisée (tous types de Systèmes d'Information décentralisés, IoT, entreprise étendue, …) ;
- tous les types de technologies et de méthodologies liées à la confiance, au contrôle et à l'audit (à condition de se concentrer sur le cadre décentralisé).

Les sujets incluent (sans s'y limiter et appliqués dans un contexte décentralisé) ceux mentionnés ci-dessus et ci-dessous :

- les mots-clés liés à la confiance dans les première et deuxième zones du Global CISO Radar de Wavestone (https://www.wavestone.com/app/uploads/2020/12/Radar_CISO_2021_v1-1.jpg) ;
- le concept Zero Trust lié à l'inférence et à l'évaluation de la confiance ;
- la gestion des identités, des authentifications et des accès ;
- l'utilisation des technologies blockchain pour la confiance, le contrôle et l'audit (mais pas le fonctionnement propre des technologies blockchain) ;
- les méthodes et techniques pour améliorer la confiance dans la chaîne d'approvisionnement (mais pas les rapports d'attaque de la chaîne d'approvisionnement) ;
- les problématiques techniques et légales liées à la gestion et exploitation des données de contrôle et audit dans les contextes du Edge Computing et Tactile Internet ;
- …

Mots clés (tous appliqués dans un contexte décentralisé) : Zero Trust [Network [Access] | Architecture | Security Model] (ZT…), Trust Algorithm (TA), Continuous Adaptive Risk and Trust Assessment (CARTA), Identity and Access Management (IAM), Identity, Credential, and Access Management (ICAM), Password, Passwordless Authentication, Multi-Factor Authentication (MFA), Single Sign-On (SSO), Trusted Platform Module (TPM), Access Policy Manager (APM), Identity Aware Proxy (IAP), Policy Decision Point (PDP), Policy Enforcement Point (PEP), Continuous Diagnostics and Mitigation (CDM), Identity Governance Program (IGP), Secure Access Service Edge (SASE), Work-from-Home, Hybrid Multi-Cloud, Edge Computing, "Tactile Internet", IoT, Cybersecurity Mesh Architecture.

Références

[1] ANSSI, « Le modèle Zero Trust », ANSSI, Avis scientifique et technique, avr. 2021. [En ligne]. Disponible sur : https://www.ssi.gouv.fr/agence/publication/le-modele-zero-trust/.

[2] ANSSI, « Système d'Information Hybride et Sécurité : un Retour à la Réalité », ANSSI, Note Blanche, août 2021.

[3] DoD, « DoD Digital Modernization Strategy : DoD Information Resource

Management Strategic Plan FY 19–23 », Department of Defense, juill. 2019. [En ligne]. Disponible sur : https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.pdf.

[4] DOT&E, « FY 2020 Annual Report », Director, Operational Test ; Evaluation (DOT&E), janv. 2021. [En ligne]. Disponible sur : https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/other/2020DOTEAnnualReport.pdf.

[5] ECSO's Users Committee, « Survey Analysis Report : Chief Information Security Officers' (CISO) Challenges & Priorities », avr. 2021.

[6] Jericho Forum, « Jericho Forum™ Commandments », Open Group, mai 2007. Version 1.2. [En ligne]. Disponible sur : https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf.

[7] NIST, « Zero Trust Architecture », NIST, Special Publication 800-207, août 2020. [En ligne]. Disponible sur : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[8] NSA, « Embracing a Zero Trust Security Model », NSA, Cybersecurity Information U/OO/115131-21, févr. 2021. [En ligne]. Disponible sur : https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.pdf.

[9] OpinionWay, « Baromètre de la cyber-sécurité des entreprises », OpinionWay, Rapport CESIN, janv. 2021. Sponsored by CESIN. [En ligne]. Disponible sur : https://www.cesin.fr/fonds-documentaire-6eme-edition-du-barometre-annuel-du-cesin.html.

[10] B. Osborn, J. McWilliams, B. Beyer, et M. Saltonstall, « BeyondCorp : Design to Deployment at Google », *;login :* vol. 41, p. 28-34, 2016, [En ligne]. Disponible sur : https://www.usenix.org/publications/login/spring2016/osborn.

[11] F. Pouchet et G. Billois, « What is the next generation cybersecurity model ? », Wavestone, Insights, mars 2017. [En ligne]. Disponible sur : https://www.wavestone.com/en/insight/next-generation-cybersecurity-model/.

[12] J. H. Saltzer, « Protection and the Control of Information Sharing in Multics », *Commun. ACM*, vol. 17, n 7, p. 388-402, juill. 1974, doi : 10.1145/361011.361067.

[13] S. Viou, « Zero Trust Network : faut-il (vraiment) n'avoir confiance en rien ? », StromShield, Paroles d'experts, avr. 2021. [En ligne]. Disponible sur : https://www.stormshield.com/fr/actus/zero-trust-network-access-avoir-confiance-en-rien/.

[14] R. Ward et B. Beyer, « BeyondCorp : A New Approach to Enterprise Security », *;login :* vol. 39, n 6, p. 6-11, déc. 2014, [En ligne]. Disponible sur : https://research.google/pubs/pub43231/.

[15] Wikipedia contributors, « Principle of least privilege — Wikipedia, The Free Encyclopedia ». 2021, [En ligne]. Disponible sur : https://en.wikipedia.org

/w/index.php?title=Principle_of_least_privilege&oldid=1062355963.

Processus de soumission

C&ESAR sollicite deux types de communications :

- ***Article régulier*** (regular paper) : communication de ***8 à 16 pages*** décrivant des travaux non encore publiés ;
- ***Résumé étendu*** (extended abstract) : résumé de ***3 à 6 pages*** d'une communication pédagogique à large audience publiée récemment dans une revue ou les actes d'un congrès avec comité de lecture (les publications concernées incluent en particulier : les états de l'art ; les états de la pratique ; les enquêtes et sondages ; les retours d'expériences ; et les solutions directement applicables à des problématiques courantes).

Déroulé

- *Première phase (résumé)* : titre, auteurs et résumé des propositions doivent être enregistrées au plus tard le ***mercredi 18 mai 2022*** sur EasyChair : https://easychair.org/conferences/?conf=cesar2022.
- *Deuxième phase (proposition)* : les propositions ***(3 à 6 pages pour les deux types de communication)*** doivent être soumises sous forme de fichier PDF au plus tard le ***mercredi 25 mai 2022*** via EasyChair. Les auteurs seront informés de la préselection de leur proposition le *mercredi 13 juillet 2022* (une sélection finale est effectuée sur les versions finales).
  - ***Article régulier*** : S'ils le souhaitent, les auteurs peuvent déjà soumettre un article complet d'au maximum 16 pages. Cependant les relecteurs n'auront pas obligation d'investir plus d'efforts qu'ils ne le feraient pour une proposition de 6 pages.
  - Les propositions de communication de type ***résumé étendu*** doivent : être clairement identifiées par la mention "résumé étendu" ou "extended abstract" dans leur titre ; clairement identifier et citer la publication originale résumée ; et contenir une annexe (en plus des 3 à 6 pages) contenant les retours (anonymisés) effectués par les relecteurs de la publication originale résumée.
- *Troisième phase (version finale)* : les auteurs des articles présélectionnés doivent charger la version finale de leur article sur EasyChair avant le ***mercredi 14 septembre 2022***. Les auteurs s'engagent à répondre aux commentaires des relecteurs dans cette version finale. Une dernière sélection avec un très haut taux de sélection est effectuée à cette étape.

Langue et critères de sélection

Langue

Les articles sont rédigés en français ou en anglais (si l'article est en français, il doit être accompagné d'une traduction en anglais de son titre et résumé).

Audience

C&ESAR s'adresse au public suivant de décideurs et de praticiens :

- Décideurs intéressés par :
  - un aperçu large et bien construit d'une problématique et de ses solutions ;
- « éclaireurs technologiques » d'unités opérationnelles intéressés par :
  - l'état de la pratique (ce que font les autres dans le même domaine),
  - identifier les technologies matures récentes qui peuvent aider à résoudre certains de leurs problèmes opérationnels ;
- Ingénieurs et chercheurs d'unités d'innovation intéressés par :
  - l'état de l'art dans leur spécialité,
  - les problèmes opérationnels abordés par d'autres dans leur communauté,
  - identifier les technologies récentes à mûrir qui peuvent aider à résoudre certains de leurs problèmes opérationnels ;
- Ingénieurs et chercheurs d'unités de recherche intéressés par :
  - l'état de l'art des spécialités liées à la leur,
  - identifier les problèmes opérationnels liés à leurs spécialités de recherche

Critères de sélection

Pour les deux types de communication, les critères de sélection incluent en particulier : l'adéquation à l'audience ; la clarté ; la dimension pédagogique ; et le respect du thème et des instructions de cet appel à contributions.

Pour les ***articles réguliers***, les communications très techniques ou très spécialisées sont les bienvenus si elles contribuent à expliquer et analyser l'état de l'art ou de la pratique et leurs lacunes.

Pour les ***résumés étendus***, la publication originale doit être clairement identifiée et citée. En outre, le processus de sélection est plus relevé, et met un focus particulier sur l'aspect pédagogique et l'audience large des communications.

Instructions pour le format des propositions et articles

Les propositions et articles en version finales doivent être soumis sous forme de fichiers PDF sans numérotation des pages, en respectant le format simple colonne des "CEUR Workshop Proceedings" (http://ceur-ws.org).

Des patrons sont disponibles pour les formats LaTeX, docx (Word) et ODT (Word et LibreOffice) à l'adresse suivante : http://ceur-ws.org/Vol-XXX/CEUR ART.zip.

Un exemple PDF et un patron TeX configurés pour C&ESAR 2022 sont disponibles sur Overleaf à l'adresse suivante : https://www.overleaf.com/read/cptq yyqwbbhs (il doit être dupliqué dans un nouveau projet pour être édité). Les soumissions ne ressemblant pas à cet exemple ne seront pas considérées pour inclusion dans les actes officiels.

Publication des actes

Dans la mesure du possible (et comme en 2021), les actes officiels de la conférence sont soumis pour publication en tant que "CEUR Workshop Proceedings" (http://ceur-ws.org), et des efforts sont mis en oeuvre pour faciliter l'indexation des articles dans DBLP et Google Scholar. Cette publication est conditionnée par le respect des contraintes de cette maison d'édition (http://ceur-ws.org/HOW TOSUBMIT.html) et ses critères d'acceptation, en particulier le respect de son format d'article et une majorité d'articles de qualité en anglais.

Dans le but d'augmenter la probabilité de publication par cette maison d'édition et l'indexation des articles dans des bases de données telles que DBLP, seulement une sélection des articles les plus qualitatifs forment les actes officiels de la conférence. La décision d'inclusion dans cette sélection pour former les actes officiels est à la discrétion des éditeurs des actes et s'appuie entre autre sur les recommandations suivantes :

- les articles ne respectant pas le format "CEUR Workshop Proceedings" ne sont pas inclus ;
- les articles en français ont une faible probabilité d'être inclus ;
- les articles doivent décrire l'état de l'art, et positionner le contenu de l'article dans ce contexte ;
- les articles doivent contenir un nombre de références et de citations en adéquation avec le volume de publications liées aux travaux décrits.

Les articles acceptés pour présentation à la conférence, mais ne faisant pas partie des actes officiels de la conférence (tous les articles si il n'y a pas d'actes publiés au format "CEUR Workshop Proceedings"), sont publiés sur le site Web de la conférence C&ESAR.

Principales dates

- **Enregistrement des propositions** (titre et résumé) : mercredi 18 mai 2022
- **Soumission des *propositions*** (3 à 6 pages) : mercredi 25 mai 2022
- Notification de présélection aux auteurs : mercredi 13 juillet 2022
- **Soumission des *versions finales*** : mercredi 14 septembre 2022

  - 8 à 16 pages pour les *articles réguliers*
  - 3 à 6 pages pour les *résumés étendus*
- Notification d'acceptation aux auteurs : mercredi 28 septembre 2022
- European Cyber Week (ECW) : mardi 15 novembre 2022 au jeudi 17 novembre 2022

Conseil de programmation

- Erwan Abgrall
- José Araujo (Orange Cyberdéfense)
- Frédéric Besson (Université de Rennes 1)
- Christophe Bidan (CentraleSupélec)
- Yves Correc (ARCSI)
- Frédéric Cuppens (Polytechnique Montréal)
- Herve Debar (Télécom SudParis)
- Ivan Fontarensky (Thales)
- Jacques Fournier (CEA)
- Julien Francq (Naval Group)
- Gurvan Le Guernic (DGA MI, Université de Rennes 1)
- Guillaume Meier (Airbus R&D)
- Marc-Oliver Pahl (IMT Atlantique, Chaire Cyber CNI)
- Yves-Alexis Perez (ANSSI)
- Ludovic Pietre-Cambacedes (EDF)
- Louis RILLING (DGA MI)
- Franck Rousset (DGNum)
- Eric Wiatrowski

Partenaires

Contacts

contact@cesar-conference.org ou cesar2022@easychair.org

FIGURE 1 – Liste des partenaires