C&ESAR'22: Ensuring Trust in a Decentralized World (Preface)

C&ESAR'22: Comment garantir la confiance dans un monde décentralisé ? (Préface)

Gurvan Le Guernic[1,2]

[1] DGA Maîtrise de l'Information, Rennes, France
[2] Univ Rennes, Inria, CNRS, IRISA, Rennes, France

Abstract

C&ESAR is an educational, professional and scientific conference on cybersecurity whose specific topic changes every year. This year C&ESAR is focused on means to ensure trust in a decentralized digital world. The digital world is becoming more and more decentralized. The traditional cybersecurity perimeter defense paradigm does not fit well with those decentralized architectures. New means are required in order to gain confidence from a security point of view in the transactions going on in a decentralized system. How can one trust, especially through control and audit, in the legitimacy of interactions in the context of remote work, hybrid cloud, and other decentralization concepts? C&ESAR 2022 received 16 submissions for peer-review. Out of these, 8 papers were accepted for presentation at the conference. After the conference, 7 were short listed for inclusion in this volume.

Keywords

Cybersecurity, Trust, Decentralization, C&ESAR, Conference, Preface

Résumé

C&ESAR est une conférence pédagogique, professionnelle et scientifique sur la cybersécurité dont le thème spécifique change chaque année. Cette année, C&ESAR se concentre sur les moyens d'assurer la confiance dans un monde numérique décentralisé. Le monde numérique est de plus en plus décentralisé. Le paradigme traditionnel de défense périmétrique ne correspond pas bien à ces architectures décentralisées. De nouveaux moyens sont nécessaires pour gagner la confiance d'un point de vue sécuritaire dans les transactions qui se déroulent dans un système décentralisé. 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 ? C&ESAR 2022 a reçu 16 soumissions pour examen par les pairs. Parmi ceux-ci, 8 articles ont été acceptés pour présentation à la conférence, dont 7 pour inclusion dans les actes.

C&ESAR'22: Computer & Electronics Security Application Rendezvous, Nov. 15-16, 2022, Rennes, France

EMAIL: gurvan.le_guernic@inria.fr (G. Le Guernic)
ORCID: 0000-0003-0387-9738 (G. Le Guernic)

1. C&ESAR

Every year since 1997, the French Ministry of Defense organizes a cybersecurity conference, called C&ESAR. This conference is now one of the main events of the European Cyber Week (ECW) organized every fall in Rennes, Brittany, France.

The goal of C&ESAR is to bring together governmental, industrial, and academic stakeholders interested in cybersecurity. This event, both educational and scientific, gathers experts, researchers, practitioners and decision-makers. This inter-disciplinary approach allows operational practitioners to learn about and anticipate future technological inflection points, and for industry and academia to confront research and product development to operational realities. Every year, C&ESAR explores a different topic within the field of cybersecurity.

This year's topic is: ***Ensuring Trust in a Decentralized World***. This topic is subtitled: Control and Audit of Interactions in a Decentralized System.

2. Ensuring Trust in a Decentralized World

The notion of trust in the context of this call relates to the notions of integrity, harmlessness/innocuousness, fitness for purpose, … Can I trust this data to act on it? Can I trust this treatment to let it "execute" in my system or on my data? Can I trust this entity to let it access those services and data? Can I (still) trust a subsystem (potentially my own, and potentially only a communication channel) to rely on it to run my operations and handle my data?

In the "good old days" of atomic enclosed and guarded information systems [1, 2], trust issues were (very) roughly reduced to the following question: are you (or your initiator) already in the system, or are you still out? Any entity inside the system (or process initiated from inside) was *implicitly* trusted to have the legitimate right to access, act on, act on behalf, or support the system [3]. Every entity composing the system (hardware or software) was "vetted" through your procurement process involving some (varying) level of evaluation; data in your system was mostly produced by yourself; processes in your system were executed under your control; and, access to your system was mostly a (trusted) physical control problem (not an IT one), except for some well-identified points such as (early days) websites and email servers. You had (nearly) full control over (nearly) everything in a clearly defined perimeter. The game was to maintain trust inside this perimeter by maintaining untrusted entities or "resources" outside of this perimeter. This approach to securing such systems is called the Castle Security Model [1, 2].

Since then, information systems have evolved a lot. Information systems are becoming more and more decentralized. For the "simple" case of an information system made of multiple fully controlled and interconnected enclaves, using Virtual Private Networks (VPN) allows getting back to a setting compatible with the Castle Security Model (although it may not be relevant for today's attacks, which among other differences involve more lateral movements than in the "good old days"). However, today's information systems are usually more decentralized than that and have lost more control over their defenses and dependencies. They may have weaker physical controls of their enclaves perimeters, such as in the case of *Remote work / Work from Home* and *Internet of Things* (IoT). They rely more and more heavily on the cloud and, from *Infrastructure as a Service* (IaaS) to *Platform as a Service* (PaaS), lose more and more control over part of their interconnections, isolation from neighboring processes, and execution stack, loosing even control over their payload in the case of *Software as a Service* (SaaS). They may even accept the fact that some of their "supporting components" may not be administered at all, or at least not at an enterprise level, as is the case with the *Bring Your Own Device* (BYOD) trend. The decentralization process itself may even not be fully controlled, as in the case of Shadow IT which is one of the main cybersecurity risks according to 44% of respondents to a recent cybersecurity survey [4]. Even if usage of the cloud is controlled, there are trust issues with it, such as lack of control over the access of the cloud provider administrators for 45% of the respondents, and no visibility on the cloud provider's supply chain for 51% of the respondents. Overall, 86% of companies estimate that the tools provided by cloud providers do not allow to secure data and that other specific tools are required [4].

Zero Trust [5, 6] is a security model that addresses part of the cybersecurity issues resulting from the decentralization of information systems. It is gaining more and more traction in the real world and is getting deployed in the industry [7, 4] as well as public institutions [8, 9]. Rather than a specific architecture or a set of methods and technologies, Zero Trust is a set of cybersecurity design principles and management strategies [10, 5]. Its main principle is to never rely on *implicit* trust. In particular authorizations (not only for access but for any transactions) should never be given solely based on the location of its requester (from which network the request comes). It does not mean that the system should not rely on trust, but that trust must be gained and renewed [3]. "[T]rust is never granted implicitly but must be continually evaluated" [5] prior (control) and posterior (audit) to granting it. This principle is not new and can be traced back to the Jericho Forum [11] in 2004 [5]. Other principles, such as the *least privilege principle* [12, 13], are even older but became more pregnant with decentralization and easier to enforce with modern technologies. Another important principle of Zero Trust is to refine the granularity of controls toward a per transaction basis. The goal is to authorize the least privileges needed *just-in-time* of need [1].

Not all of the principles of Zero Trust are covered by C&ESAR 2022. Exact definitions of Zero Trust vary, but the NSA summarizes it to 4 main points [10]: 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. In the scope of this Zero Trust definition, C&ESAR 2022 focuses on points b and c in a highly decentralized setting: at a fine granularity level, how to gain trust in requests for resources, network traffic, devices, and infrastructure? Implied by this question, but not equivalent, is the problem of authentication which is one of the main concerns for Zero Trust [5, 14, 6], as well as in general [15, 8].

Though useful to address some of the problems related to trust in a decentralized system, some of the issues covered by C&ESAR 2022 may or may not be included in Zero Trust depending on the definition used.

Related to Zero Trust are the problem of transitive trust and trust propagation. For example, in the setting of a developer in a controlled enclave that pushes code to a version control SaaS, that pushes this code to a Continuous Integration / Continuous Deployment (CI/CD) SaaS of another provider, that pushes the resulting "binaries" to a web server SaaS of yet another provider, what are the potential solutions for the developer to trust (control and audit) SaaS not to abuse their privileges to push something different on your behalf? What are the potential solutions for the SaaS providers to trust other providers to faithfully act on behalf of the developer, including and beyond signature preserving versioning and compilation? More generally, how to trust a previously unknown or unvetted entity starting to interact with your system? How to rely on the trust of others to trust an interaction?

On a different subject, trust evaluation requires (meta)data. In a highly geographically decentralized system that may move payloads between enclaves, how to ensure the dissemination and synchronization of this (meta)data in a secured way compatible with the timing constraints of the system and the laws applicable to the owner of the (meta)data, the owner of the payload, and the location where the executing enclave resides?

3. Solicited Papers

In this context, C&ESAR solicited submissions presenting **clear surveys, innovative solutions, or insightful experience reports** on the subject "Ensuring Trust in a Decentralized World".

The scope covered:

- all steps of cybersecurity, from system design to operational cyberdefense or pentesting, including DevSecOps loops and disposal/retirement of equipment and systems;
- all types of systems as long as they have a decentralized architecture (every type of decentralized information system, IoT, extended enterprise networks, ...) ;
- all types of trust, control, and audit-related technologies and methodologies (as long as a focus on the decentralized setting is made).

The topics included (without being limited to them and applied in a decentralized world setting) those mentioned above and below:

- the trust-related keywords in the first and second areas of Wavestone's Global CISO Radar;
- Zero Trust concepts related to trust inference and evaluation;
- identity, authentication, and access management;
- usage of blockchain technologies for trust, control, and audit (but not blockchain technologies for their own sake);

- methods and techniques to improve trust in the supply chain (but not supply chain attack reports);
- technical and legal issues related to handling and exploitation of control and audit data in the Edge Computing and Tactile Internet settings ;
- ...

The topic also covered all the following keywords applied in a decentralized context: 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.

4. Review Process

C&ESAR received 16 submissions. Among those, 12 proposals have been selected for the final round of reviews (75% pre-selection rate). Out of those pre-selected proposals, 9 final versions were submitted; out of which, 8 have been selected for presentation at the conference (a 89% acceptation rate for the final round of reviews, and a 50% overall acceptation rate for the conference). Finally, 7 of the presented papers have been selected for inclusion in the proceedings (an overall acceptation rate of 44% for the proceedings).

5. Program Committee

This peer review has been made possible thanks to the dedication of the members of the following program committee:

- Erwan Abgrall
- 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
- Brittia Guiriec, DGA MI
- Gurvan Le Guernic, DGA MI & Université de Rennes 1 (Univ Rennes)
- Frédéric Majorczyk, DGA MI & CentraleSupélec

- Guillaume Meier, Airbus R&D
- Laurence Ogor, DGA MI
- Marc-Oliver Pahl, IMT Atlantique & Chaire Cyber CNI
- Yves-Alexis Perez, ANSSI
- Ludovic Pietre-Cambacedes, EDF
- Olivier Poupel, DGA MI
- Louis Rilling, DGA MI
- Franck Rousset, DGNum
- Eric Wiatrowski

References

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

[2] F. Pouchet, G. Billois, What is the next generation cybersecurity model?, Insights, Wavestone, 2017. URL: https://www.wavestone.com/en/insight/next-generation-cybersecurity-model/.

[3] S. Viou, Zero Trust Network : faut-il (vraiment) n'avoir confiance en rien ?, Paroles d'experts, StromShield, 2021. URL: https://www.stormshield.com/fr/actus/zero-trust-network-access-avoir-confiance-en-rien/.

[4] OpinionWay, Baromètre de la cyber-sécurité des entreprises, Rapport CESIN, OpinionWay, 2021. URL: https://www.cesin.fr/fonds-documentaire-6eme-edition-du-barometre-annuel-du-cesin.html, sponsored by CESIN.

[5] NIST, Zero Trust Architecture, Special Publication 800-207, NIST, 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[6] ANSSI, Le modèle Zero Trust, Avis scientifique et technique, ANSSI, 2021. URL: https://www.ssi.gouv.fr/agence/publication/le-modele-zero-trust/.

[7] B. Osborn, J. McWilliams, B. Beyer, M. Saltonstall, Beyondcorp: Design to deployment at google, ;login: 41 (2016) 28–34. URL: https://www.usenix.org/publications/login/spring2016/osborn.

[8] DoD, DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY 19–23, Technical Report, Department of Defense, 2019. URL: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.pdf.

[9] DOT&E, FY 2020 Annual Report, Technical Report, Director, Operational Test and Evaluation (DOT&E), 2021. URL: https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/other/2020DOTEAnnualReport.pdf.

[10] NSA, Embracing a Zero Trust Security Model, Cybersecurity Information U/OO/115131-21, NSA, 2021. URL: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.pdf.

[11] Jericho Forum, Jericho Forum™ Commandments, Technical Report, Open Group, 2007. URL: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf, version 1.2.

[12] J. H. Saltzer, Protection and the Control of Information Sharing in Multics, Commun. ACM 17 (1974) 388–402. URL: https://doi.org/10.1145/361011.361067. doi:10.1145/361011.361067.

[13] Wikipedia contributors, Principle of least privilege — Wikipedia, the free encyclopedia, 2021. URL: https://en.wikipedia.org/w/index.php?title=Principle_of_least_privilege&oldid=1062355963, [Online; accessed 17-January-2022].

[14] R. Ward, B. Beyer, Beyondcorp: A new approach to enterprise security, ;login: 39 (2014) 6–11. URL: https://research.google/pubs/pub43231/.

[15] ECSO's Users Committee, Survey Analysis Report: Chief Information Security Officers' (CISO) Challenges & Priorities, Technical Report, **??**www.ecs-org.eu, 2021.