C&ESAR 2022 Call for Papers

C&ESAR's Program Board

Tuesday, May 10, 2022

Abstract

The cybersecurity conference C&ESAR solicits submissions on the subject "Ensuring Trust in a Decentralized World". The submission deadline for abstracts is Wednesday, May 18, 2022.

About 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. The complete call for papers is available on a dedicated web page presenting the call and as a PDF file.

C&ESAR's 2022 Topic: *Ensuring Trust in a Decentralized World*

This topic is subtitled: Control and Audit of Interactions in a Decentralized System.

Summary

C&ESAR solicits submissions presenting **clear surveys, innovative solutions, or insightful experience reports** dealing with the problem of **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? The scope covers technical issues as well as legal issues.

Among the main keywords are: Zero Trust, IAM, Work-from-Home, Hybrid Multi-Cloud, International Law

Detailed

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 [2] [11], 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 [13]. 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 [2] [11].

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 [9]. 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 [9].

Zero Trust [7] [1] 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 [10] [9] as well as public institutions [3] [4]. Rather than a specific architecture or a set of methods and technologies, Zero Trust is a set of cybersecurity design principles and management strategies [8] [7]. 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 [13]. "[T]rust is never granted implicitly but must be continually evaluated" [7] prior (control) and posterior (audit) to granting it. This principle is not new and can be traced back to the Jericho Forum [6] in 2004 [7]. Other principles, such as the *least privilege principle* [12] [15], 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 [2].

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 [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. 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 [7] [14] [1], as well as in general [5] [3].

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?

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

The scope covers:

- 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 include (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 (https://www.wavestone.com/app/uploads/2020/12/Radar_CISO_2021_v1-1.jpg);
- 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 ;
- …

Keywords (all 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.

References

[1] ANSSI, "Le modèle Zero Trust," ANSSI, Avis scientifique et technique, Apr. 2021. [Online]. Available: 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, Aug. 2021.

[3] DoD, "DoD digital modernization strategy: DoD information resource management strategic plan fy 19–23," Department of Defense, Jul. 2019. [Online]. Available: 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), Jan. 2021. [Online]. Available: 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," Apr. 2021.

[6] Jericho Forum, "Jericho Forum™ Commandments," Open Group, May 2007. Version 1.2. [Online]. Available: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf.

[7] NIST, "Zero Trust Architecture," NIST, Special Publication 800-207, Aug. 2020. [Online]. Available: 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, Feb. 2021. [Online]. Available: 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, Jan. 2021. Sponsored by CESIN. [Online]. Available: https://www.cesin.fr/fonds-documentaire-6eme-edition-du-barometre-annuel-du-cesin.html.

[10] B. Osborn, J. McWilliams, B. Beyer, and M. Saltonstall, "BeyondCorp: Design to deployment at google,"*;login:* vol. 41, pp. 28–34, 2016, [Online]. Available: https://www.usenix.org/publications/login/spring2016/osborn.

[11] F. Pouchet and G. Billois, "What is the next generation cybersecurity model?" Wavestone, Insights, Mar. 2017. [Online]. Available: 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, no. 7, pp. 388–402, Jul. 1974, doi: 10.1145/361011.361067.

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

[14] R. Ward and B. Beyer, "BeyondCorp: A new approach to enterprise security,"*;login:* vol. 39, no. 6, pp. 6–11, Dec. 2014, [Online]. Available: https://research.google/pubs/pub43231/.

[15] Wikipedia contributors, "Principle of least privilege — Wikipedia, the free encyclopedia." 2021, [Online]. Available: https://en.wikipedia.org/w/index.php?title=Principle_of_least_privilege&oldid=1062355963.

Submission process

C&ESAR solicits two types of papers:

- ***Regular paper***: ***8 to 16 pages*** paper describing work not yet published;
- ***Extended abstract***: ***3 to 6 pages*** abstract of a large audience didactic paper recently published in a peer-reviewed journal or conference proceedings (papers of interest include in particular: states of the art or practice; surveys; experience reports; and directly applicable solutions to common problems).

Steps

- *First phase (abstract)*: title, authors and abstract of the proposals have to be registered no later than ***Wednesday, May 18, 2022*** on EasyChair: https://easychair.org/conferences/?conf=cesar2022.

- *Second phase (proposal)*: proposals ***(3 to 6 pages for both types of papers)*** have to be submitted as a PDF file no later than ***Wednesday, May 25, 2022*** via EasyChair. Authors will be notified of their proposal preselection by *Wednesday, July 13, 2022* (a final selection will be made on the final version).
  - ***Regular paper***: If desired authors can already submit a complete paper of up to 16 pages. However, reviewers will not be required to invest more efforts at this stage than they would for a 6 pages proposal.
  - ***Extended abstract*** proposals must: be explicitly identified as such by the mention "extended abstract" in their title; explicitly identify and cite the original publication; and, contain an appendix (in addition to the 3 to 6 pages) containing the (anonymized) comments made by the reviewers of the original publication.
- *Third phase (final version)*: authors of preselected papers have to upload the final version of their paper on EasyChair by ***Wednesday, September 14, 2022***. Authors of preselected papers commit to address reviewers' comments in this final version. A final selection with a really high selection rate is performed at this stage.

Language and selection criteria

Language

Papers are written in French or in English (English translations of title and abstract of papers written in French must be provided).

Audience

C&ESAR is aimed at the following audience of decision makers and practitioners:

- Decision makers interested in:
  - broad and well constructed overview of a problematic and its solutions;
- "technology scouts" of operational units interested in:
  - knowing more about the state of practice (what others in the same domain do),
  - identifying recent mature technologies that may help solving some of their operational problems;
- Engineers and researchers of innovation units interested in:
  - knowing more about the state of the art in their specialty,
  - knowing more about the operational problems addressed by others in their community,
  - identifying recent to be matured technologies that may help solving some of their operational problems;
- Engineers and researchers of research units interested in:
  - knowing more about the state of the art in specialties related to their own,

– identifying operational problems related to their research specialties

Selection criteria

For both types of papers, selection criteria include in particular: fitness for the audience; clarity; pedagogical (didactical) value; and respect of this call for papers topic and guidelines.

For ***regular papers***, specialized technical papers will be appreciated if they contribute to explain and analyze the state of the art or practice and their deficiencies.

For ***extended abstracts***, the original publication must be clearly identified and cited. Moreover, the selection process is more selective, and emphasizes the didactical quality and large audience of the papers.

Instructions for the format of proposals and papers

Proposals and papers must be submitted as PDF files, without page numbering, following the single column format of "CEUR Workshop Proceedings" (http://ceur-ws.org).

Templates are available for LaTeX, docx (Word) and ODT (Word or LibreOffice) at the following URL: http://ceur-ws.org/Vol-XXX/CEURART.zip.

A PDF example and a TeX template configured for C&ESAR 2022 are available on Overleaf at https://www.overleaf.com/read/cptqyyqwbbhs (it must be duplicated before edition). Submissions not looking like this example will not be considered for inclusion in the official proceedings.

Proceedings

As far as possible (and as in 2021), the official conference proceedings are submitted for publication to "CEUR Workshop Proceedings" (http://ceur-ws.org), and efforts are performed in order to facilitate indexing of articles in DBLP and Google Scholar. This publication is conditioned by the respect of this publisher's constraints (http://ceur-ws.org/HOWTOSUBMIT.html) and acceptance criteria, in particular respect of its paper format and having a majority of high quality articles written in English.

In order to increase the probablity of acceptance by the publisher and indexing by publication databases such as DBLP, only a curated list of the most qualitative papers form the official conference proceedings which are submitted for publication as a volume of "CEUR Workshop Proceedings". The official proceedings inclusion decision is at the discretion of the editors of the proceedings and is based, in part, on the following recommendations:

- articles that do not respect the "CEUR Workshop Proceedings" format are not included;

- articles in French are unlikely to be included;
- articles should describe the state of the art, and position the content of the article in this context;
- articles should contain a number of references and citations in adequation with the volume of publications related to the work described.

Articles accepted for presentation at the conference, but not included in the official conference proceedings (all articles if there are no proceedings published as a volume of "CEUR Workshop Proceedings"), are published on C&ESAR conference's website.

Deadlines

- **Registration of proposals** (title and abstract): Wednesday, May 18, 2022
- **Submission of the *proposals*** (3 to 6 pages): Wednesday, May 25, 2022
- Notification of preselection to authors: Wednesday, July 13, 2022
- **Submission of the *final version***: Wednesday, September 14, 2022
  - 8 to 16 pages for *regular papers*
  - 3 to 6 pages for *extended abstracts*
- Notification of acceptation to authors: Wednesday, September 28, 2022
- European Cyber Week (ECW): Tuesday, November 15, 2022 to Thursday, November 17, 2022

Program board

- 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

Sponsors

Figure 1: Sponsors list

Contacts

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