C&ESAR'25: Computer & Electronics Security Application Rendezvous (preface)

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 held every fall in Rennes, France. The scope covers all issues related to cybersecurity during all stages of a system lifecycle and in relation with every technology and environment. C&ESAR 2025 received 20 submissions for peer-review. Out of these, 6 papers were accepted for presentation at the conference.

Keywords

Cybersecurity, C&ESAR, Conference, Preface

1. C&ESAR

Since 1997, the French Ministry of Defense organizes C&ESAR, an annual cybersecurity conference that has become a key event within the European Cyber Week (ECW). Held every fall in Rennes, Brittany, France, C&ESAR serves as an important forum for cybersecurity professionals, researchers, and decision-makers.

The conference brings together experts from government, industry, and academia, fostering a unique interdisciplinary exchange. It provides operational practitioners with insights into emerging technologies, while industry and research communities gain exposure to real-world challenges. This synergy helps shape the future of cybersecurity by bridging the gap between theoretical advancements and practical implementation.

2. Solicited Papers

C&ESAR invites submissions on a broad range of cybersecurity topics, covering:

- All phases of the system lifecycle – from requirements elicitation to decommissioning, including legal and regulatory aspects, DevSecOps, operational cyber defense, penetration testing, and disinformation.
- All types of technologies and environments – including socio-economic systems, networks, embedded systems, industrial control systems, IoT, personal devices, cloud, and edge computing.

C&ESAR welcomes submissions in two main categories:

- Scholarly Papers: presenting original research, innovative methodologies, or systematization of knowledge (SoK); or summarizing significant prior research contributions.
- Professional/Trade Papers: presenting applied research or practical insights; or exposing industry best practices, case studies, technical experiments, legal perspectives, or geopolitical analyses.

C&ESAR'25: Computer & Electronics Security Application Rendezvous, Nov. 19-20, 2025, Rennes, France
gurvan.le_guernic@inria.fr (G. Le Guernic)
0000-0003-0387-9738 (G. Le Guernic)

3. Review Process

C&ESAR follows a 3 steps submission process (abstract, proposal, final version). Evaluation and selection is done on the proposal and final version steps. During the proposal step, a selective evaluation is done with a low acceptation rate on a detailed outline of the proposed article (or directly on the final version if a final version is submitted as proposal). During the final version step, an evaluation with a high acceptation rate (high number of articles selected) is done on the final version of the accepted proposals.

C&ESAR'25 received 20 submissions. Among those, 12 proposals have been selected for the final round of reviews (60% pre-selection rate). Out of those pre-selected proposals, 9 final versions were submitted; out of which, 6 have been selected for presentation at the conference (a 67% acceptation rate for the final round of reviews, and a 30% overall acceptation rate for the conference).

4. Keynotes

This year, the following speakers were invited to give a keynote during C&ESAR.

4.1. "Artificial Intelligence for Cybersecurity: from LLM-Powered Offensive Capabilities to AI-Driven Attack Path Prediction" by Abdelkader LAHMADI

Biography. Abdelkader Lahmadi is a Full Professor of Computer Science at Université de Lorraine in France. He leads the RESIST research group at LORIA and the Inria Centre of Université de Lorraine. His research focuses on bridging the gap between Artificial Intelligence and cybersecurity for complex networked systems, with a particular emphasis on attack detection, prediction, and automated response. Beyond academia, he is the co-founder of CYBI, a cybersecurity company that develops AI-driven attack-path management and prioritization solutions, transferring cutting-edge research into real-world cybersecurity operations.

Abstract. As Artificial Intelligence (AI) becomes deeply integrated into cybersecurity operations, its dual role as both a defensive enabler and an offensive catalyst is increasingly evident. On one side, AI supports defenders by enhancing detection, prediction, and mitigation of cyber threats. On the other, attackers are swiftly adopting AI models—particularly Large Language Models (LLMs)—to automate and amplify offensive operations. In this talk, I will explore this evolving landscape and illustrate how AI reshapes both sides of the cybersecurity battlefield. I will present recent advances from our research on applying Reinforcement Learning (RL) for automated attack-path discovery and prediction, as well as on evaluating the offensive potential of general- purpose LLMs for generating vulnerability exploitation steps.

4.2. "From Theory to Practice: Detecting and Preserving Constant-Time" by Clémentine MAURICE

Biography. Clémentine Maurice is a Research Scientist at CNRS in the CRIStAL laboratory in Lille. She received her PhD from Telecom ParisTech in 2015, and subsequently worked as a postdoctoral researcher at Graz University of Technology in Austria. Her research focuses on microarchitectural attacks and their countermeasures. She also presented her work at hacker conferences such as CCC and Blackhat Europe, and is featured twice in the Mozilla Hall of Fame.

Abstract. Side-channel vulnerabilities keep showing up in cryptographic software—despite a decade of automated detection tools meant to stop them. Why do these leaks keep slipping through? In the first part of this keynote, we explore this paradox, benchmarking tools against real-world vulnerabilities and uncovering why detection is harder than it looks. In the second part, we show that even when developers get constant-time code right, the compiler may not. Optimization passes in GCC and LLVM can quietly sabotage security, turning constant time into wishful thinking. We reveal which

optimizations are to blame, how to catch them, and what practical defenses developers can actually use. Your compiler is not your friend—but with the right knowledge, you can keep it from turning against you. We conclude by analyzing the impact of recent attacks on automated detection tools.

4.3. "Software Compartmentalization Everywhere - What Will it Take?" by Hugo LEFEUVRE

Biography. Hugo Lefeuvre is a Postdoctoral Research Fellow at the University of British Columbia in Vancouver (Canada), where he researches topics at the intersection of systems and security. Earlier he was a PhD candidate at the University of Manchester (UK) and a Microsoft PhD Research Fellow. His PhD dissertation was awarded the EuroSys Roger Needham PhD Award.

Abstract. Software compartmentalization is the practice of breaking down a program into isolated components to mitigate the impact of bugs and security vulnerabilities. In the event of a compromise, compartmentalization contains the exploit, raising the bar for attackers to mount successful attacks. Although vastly successful in popular software such as web browsers or server software, compartmentalization is still not a widespread software development practice. In this talk, based on our recent publication "SoK: Software Compartmentalization" at IEEE S&P 2025, we will discuss compartmentalization approaches in industry and academia to understand the remaining challenges to making compartmentalization a truly widespread practice, raise awareness on this practice, and show how it can lead to fundamentally more secure and dependable software.

4.4. "Four Decades of Malware Research: Milestones, Synthesis, and Open Challenges" by Davide BALZAROTTI

Biography. Davide Balzarotti is a full Professor and the head of the Digital Security Department at EURECOM. He received his Ph.D. from Politecnico di Milano in 2006 and his research interests include most aspects of software and system security and in particular the areas of binary and malware analysis, reverse engineering, computer forensics, and web security. Davide authored more than 100 publications in leading conferences and journals. He has been the Program Chair Usenix Security 2024, ACSAC 2017, RAID 2012, and Eurosec 2014. Davide received an ERC Consolidator and an ERC PoC Grants for his research on the analysis of compromised systems. Davide is is also member of the "Order of the Overflow" team, which organized the DEF CON CTF competition between 2018 and 2021.

Abstract. Since the emergence of the initial self-replicating viruses in the 1980s, the history of malware has undergone a rich and fascinating evolution - which attracted the interest of researchers, nation-state agencies, and multi-billion dollars corporations. By examining the main contributions in the field through the lens of thousands of published papers, in this talk I will identify a number of recurring themes and long-lasting challenges. The talk will also break down different areas of malware research and try to distill the major results that researchers obtained in this fascinating field.

4.5. "Inside the Russian Approach to Cyber Interference" by Christine DUGOIN-CLÉMENT

Biography. Christine Dugoin-Clément is a Research Associate at the "Risks" Chair of the IAE Business School, Paris 1 Panthéon-Sorbonne University, at the Observatory of Artificial Intelligence (Paris 1), and at the Research Center of the French National Gendarmerie (CRGN). A former auditor of the French Institute for Advanced Studies in National Defense (IHEDN), her research focuses on Ukraine, defense, influence strategies, and cybersecurity. Her most recent book, « Géopolitique de l'ingérence russe : la stratégie du chaos », was published by the Presses Universitaires de France (PUF).

Abstract. This presentation examines the new forms of digital interference driven by Russia, focusing on the hybridization of cyber and information operations, the use of disinformation, and the exploitation of social networks and generative artificial intelligence. It highlights the evolution of cybercrime since the war in Ukraine, the growing ties between state and criminal actors, and the influence and manipulation strategies deployed across digital platforms and cultural spaces. The talk also reflects on the broader challenges of credibility, regulation, and resilience in the face of today's information warfare and its implications for democratic societies.

4.6. "Beyond the Hype: Real-World 5G Security Challenges & Operational Strategies" by Rémy HAREL

Biography. Rémy Harel is a seasoned cybersecurity leader, currently heading a team of 20 mobile network cybersecurity experts at Orange Group, a role he has held for the past seven years. As a former security auditor, Rémy played a pivotal role in shaping 5G network security from its foundational stages, notably as Chairman of the 5G Security Group at NGMN. His practical expertise was instrumental in the selection and initial deployment of Orange Group's 5G networks, where he and his team conducted extensive on-site security audits to assess real-world security postures. Rémy actively collaborates with major 5G core network vendors, providing critical input on the security architecture and resilience of their solutions.

Abstract. 5G is not "just another mobile generation"; it is a revolution poised to transform industries and lives. At C&ESAR 2025, I will delve into the critical security imperatives underpinning this transformation. My session will cut through the hype to address the real-world challenges we face in securing 5G deployments. We'll explore the evolving threat landscape, the complexities of supply chain integrity, and the operational realities of securing CI/CD pipelines. Expect actionable insights, regulatory foresight, and practical strategies derived from frontline experience. Let's discuss how to build resilient, trustworthy 5G networks from the ground up.

4.7. "Attacks on Open Source Software Supply Chains: Vectors, Case Studies, and Defenses" by Henrik PLATE

Biography. Henrik Plate is the principal security researcher at Endor Labs, aiming to improve the security of today's software supply chains, and the secure consumption of open source. He formerly worked for SAP Security Research, where he led the focus topic "Open Source Security" starting in 2014. He co-authored several academic papers on this topic, presented at academic and industry conferences like the RSA, is the project lead and core-developer of Eclipse Steady (an open source solution using program analysis techniques to assess the exploitability of vulnerabilities), and contributes to the Risk Explorer for Software Supply Chains (an open source solution to understand supply chain threats and safeguards). He earned his PhD in 2024 from the University of Rennes, France, with a thesis titled "On the Security Risks of Open Source Consumption: Vulnerabilities and Supply Chain Attacks in the Era of Open-Source-Based Software Development". He received his MSc in Computer Science and Business Administration in 1999 from the University of Mannheim, Germany, and holds a CISSP certification.

Abstract. The widespread reliance on open source in modern software development has made it a prime target for supply chain attacks, in which adversaries inject malicious code into upstream projects, ultimately reaching developers and end users downstream. In August and September 2025 alone, several attacks against popular npm packages revealed novel techniques not previously observed in the wild—and, at the time of writing, further incidents continue to emerge. This talk surveys common attack vectors, illustrated through both historical and recent case studies, ranging from typo-squatting and dependency confusion to compromised CI/CD pipelines and npm malware. It also examines available countermeasures—both detective and preventive—highlighting their respective strengths and limitations.

5. Program Committee

The peer-review process and the construction of the conference program, including the integration of accepted submissions and invited speakers, were made possible through the commitment of the following Program Committee members:

- Jose Araujo, SNCF
- Eric Aubourg, CEA
- Mickael Bouyaud, AFIS
- Julien Bui, CESIN
- Frederic Cuppens, Polytechnique Montréal
- Guillaume Doyen, IMT Atlantique
- Ivan Fontarensky, Thales
- Jacques Fournier, ST Microelectronics
- Julien Francq, Naval Group
- Paul-Olivier Gibert, AFCDP
- Christelle Gloeckler, CNEJITA
- Brittia Guiriec, DGA MI
- Gurvan Le Guernic, DGA MI & Université de Rennes
- Frederic Majorczyk, DGA MI & CentraleSupélec
- Guillaume Meier, Airbus R&D
- Patricia Mouy, CEA
- Vivien Mura, Orange Cyberdéfense
- Laurence Ogor, DGA MI
- Marc-Oliver Pahl, IMT Atlantique & Chaire Cyber CNI
- Yves-Alexis Perez, ANSSI
- Ludovic Pietre-Cambacedes, EDF
- Florence Puybareau, CLUSIF
- Tania Richmond, Université de la Nouvelle-Calédonie
- Louis Rilling, DGA MI
- Eric Wiatrowski
- Olivier Zendra, Inria