Computer & Electronics Security Applications Rendez-vous

www.cesar-conference.fr

C&ESAR 2018

Artificial Intelligence and Cybersecurity

November 19 - 21, 2018 – Rennes - France

About C&ESAR

Every year since 1997, the French Ministry of Defense has organized a cybersecurity event to bring together governmental, industrial, and academic stakeholders. This event is both educational and scientific, gathering experts, researchers, practitioners and decision-makers in order to explore an important topic within the field of cybersecurity. The chosen themes are covered from both a theoretical and practical perspective, with a strong emphasis on educational approach in order to help information security professionals with different backgrounds share a common understanding of complex issues. This inter-disciplinary approach within the cybersecurity profession allows operational practitioners to learn about and anticipate future technological inflexion points, and for industry and academia to confront research and product development to operational realities of the field.

Artificial Intelligence and Cybersecurity

Recent advances in artificial intelligence (AI), most notably in machine learning, promise to revolutionize a wide variety of application domains. Cybersecurity in its broadest sense (software, hardware, networks ...) already takes advantage of these advances in the conception or analysis phase, or for the defense of deployed systems.

These intelligent systems can be targeted by new classes of attacks designed to deceive them or influence their behavior. One can cite Tay, Microsoft's chatbot, as an example.

Furthermore, the lack of approaches to analyze most AI or explain their decisions introduces a risk to systems that integrate them and may hinder their adoption.

The C&ESAR 2018 conference proposes to address both parts: the contributions of AI to cybersecurity, and the cybersecurity risks associated with AIs.

The program committee solicits AI proposals on the following topics:

- *Automated risk analysis* of secure systems,
- AI-driven *protection* of secure systems,
- *Attacks* aimed at AIs,
- *Qualification and certification* of AI-based systems or algorithms.

Expected contributions will thus be about the benefits of AI to systems security in all their components (software, hardware, and networks), without forgetting about the human factor. Regarding AI, the program committee favors machine learning, but other forms or artificial intelligence will also be considered.

Submissions in the following areas will be appreciated by the program committee:

- Automatic network configuration from a security standpoint, training against cyber threats,…
- Image analysis, electronic signals analysis, network alarms analysis,…
- threat intelligence,
- decision making responsibilities involving AIs, involving humans
- fraud detection, influence attemps, data poisoning attacks, bias prevention in learning…
- automated analysis of softwares, code deobfuscation, security robustness evaluation (passwords…), automated vulnerability patching,…
- limits of AIs for cybersécurité, AI and privacy, training data gathering, weak signals detection
- Feedback on actual implementations of AI for cyber
- AI under constraints (limited resources, time, data)

Submission process

- *First phase:* the proposals (3 to 6 pages) shall be submitted as a PDF file by ~~June 29th, 2018~~ **July 6th , 2018 (new date)** at the latest via https://www.easychair.org/conferences/?conf=cesar2018. Each submission shall include a title, the category of communication (analysis, protection, attacks, qualification and certification), the authors' names and affiliation, the email address of the corresponding author, an abstract (10 lines max.), and a list of keywords. The authors will be notified of their proposal acceptance by **September 5th, 2018**.
- *Second phase:* authors shall send the camera-ready version of their paper (8 to 16 pages) by **October 2nd, 2018** to contact@cesar-conference.org, cc to benoit-f.martin@intradef.gouv.fr. Authors whose papers are accepted commit to address reviewers comments in the final version.
- *Instructions for the camera-ready version of the paper:* PDF in A4 layout without page numbering, following the Springer Lecture Notes in Computer Science template:
    - LaTeX template: ftp://ftp.springernature.com/cs-proceeding/llncs/llncs2e.zip;
    - Word template: ftp://ftp.springernature.com/cs-proceeding/llncs/word/splnproc1703.zip.

  Contact benoit-f.martin@intradef.gouv.fr in case of problem.
- *Language and selection criteria:* the papers can be written in French or in English. Selection criteria include clarity and educational dimension, as well as the respect of the theme of the conference and the guidelines of this call for papers. Specialized technical papers will be taken into consideration to the extent that they contribute to explaining and analyzing the state of the art or its deficiencies, rather than presenting only individual technical contributions. Accepted papers will be published in both online and printed versions in the proceedings of the conference.

Important dates

- Submission of the proposals (long abstracts between 3 to 6 pages): ~~June 29th, 2018~~ **July 6th , 2018 (new date)**
- Notification to authors: **September 5th, 2018**
- Final version (8 to 16 pages): **October 2nd, 2018**
- Conference : **November 19th to 21st, 2018**

Program committee

José ARAUJO (ANSSI)
Christophe BIDAN (Centrale-Supélec)
Frédéric CUPPENS (IMT Atlantique)
Ivan FONTARENSKY (THALES)
Guillaume DUVEAU (DGNUM, MINARM)
Guillaume MEIER (AIRBUS D&S)
Eric WIATROWSKI (Orange Cyberdefense)
Boris BALACHEFF (HP Labs)
Yves CORREC (ARCSI)
Herve DEBAR (Télécom SudParis)
Patrick HEBRARD (NAVAL Group)
Benoît MARTIN (DGA-MI, MINARM)
Ludovic PIETRE-CAMBACEDES (EDF)

Sponsors