C&ESAR 2020 – Deceptive security

call for papers

November 17 – 18, 2020 – Rennes - France

Computer & Electronics Security Applications Rendez-vous

www.cesar-conference.fr

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, both educational and scientific, gathers experts, researchers, practitioners and decision-makers in order to explore an important topic within the field of cybersecurity. This inter-disciplinary approach 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. Conference occurs during European Cyber Week (ECW).

Deceptive security

Cybersecurity has developed over the past fifteen years in response to the increasing aggressiveness of computer attacks. The rise of cyberspace is inherent in the explosion in the need for services and communications and therefore speed and new technologies. Built on a pragmatic basis to provide new products, cyberspace has reached a level of complexity that is difficult to master. This situation gave a preponderant advantage to the attackers who knew how to transform an imperfection into a breach and then into attack scenarios for hostile ends. The IT security response has evolved from deep static protection to resilient detection, and now for considering the logic of dynamic counterattacks. The time scale between the occurrence of an attack, its detection and its elimination is an important characteristic: from an indefinite duration to a few days, then from a few days to a few hours, the challenge now consists in acting in real time against the attacker. Digital deception is at the heart of this cybersecurity strategy. The aim is to return the attacker's weapons, seeking to deceive him and dissuade him from been discovered. Digital deception is part of cyber deterrence.

Defensive lure arsenal has historically relied on honeypots. These statically analyzed the deviation of components compared to a known and healthy behavior. This generation has encountered two pitfalls: scalabity to cover diversity and complexity of digital systems, and excessive false positives. Honeypots evolve to become active traps disseminated in the real environment to understand better attacker's strategies. Decoy deployment architectures specialize according to application (information systems, industrial systems, finance, medical, etc.), to the components targeted by the attacks (servers, firewalls, antivirus, etc.) or to the offensive load (malware, etc.). Lures tend to generate real positives in real time. Their effectiveness relies on two properties, one inherent in security components, non-compromise, and the other characteristic of attack: stealth.

This new generation of digital decoys consolidates investigations within security operational centers (SOC). Thus, logics of deductive (deterministic) or inductive (hypothetical) reasoning confront each other to characterize attackers' operating mode by tightening it up to attack attribution.

However, its active behavior raises regulatory issues (privacy).

Digital decoy becomes an essential component of defensive activities in cybersecurity, because it contributes to efficiency of response scenarios.

C&ESAR 2020 program committee will appreciate submissions in the following areas:

- Tools for deceptive security : honeypots, lures, traps
- decoy deployment architectures
- Specialized decoy for services, for security, against malware ...
- Digital decoy properties: non-compromise, stealth...
- Forensics : deductive / inductive reasoning, attacks characterization, attribution ...
- Security Operational Center : deceptive security in escalation scenarios
- Decoys and attack models (MITRE ATT@CK ...), contribution to characterization (CAPEC …), to knowledge of cyber risk (cyber threat intelligence - CTI)
- Decoy and regulation (privacy, NIS Directive…).

Submission process

- *First phase:* the proposals (3 to 6 pages) shall be submitted as a PDF file by **June 30th, 2020** (extended date) at the latest via https://www.easychair.org/conferences/C&ESAR_2020. 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 3rd, 2020**.
- *Second phase:* authors shall send the camera-ready version of their paper (8 to 16 pages) by **October 2nd, 2020** 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.
- *Language and selection criteria:* Papers are written in French or in English. Selection criteria are clarity, pedagogical dimension, respect of theme and guidelines of this call for papers. Specialized technical papers will be appreciate if they contribute to explain and analyze state of the art and its deficiencies. Accepted papers will be published in proceedings available on C&ESAR conference website

Important dates

- Submission of the proposals (long abstracts between 3 to 6 pages): **June 30th, 2020** (extended date)
- Notification to authors: **September 3rd, 2020**
- Final version (8 to 16 pages): **October 2nd, 2020**
- Conference: **November 17h - 18th, 2020**

Program committee

Erwan ABGRALL (MINARM)
Christophe BIDAN (CentraleSupélec)
Frédéric CUPPENS (Polytechnique Montreal)
Eric DUPUIS (Orange)
Ivan FONTARENSKY (THALES)
Sylvain LAFARGUE (SAFRAN)
Guillaume MEIER (AIRBUS)
Ludovic PIETRE-CAMBACEDES (EDF)
Eric WIATROWSKI (Orange)
José ARAUJO (ANSSI)
Yves CORREC (ARCSI)
Herve DEBAR (Télécom SudParis)
Guillaume DUVEAU (MINARM)
Patrick HEBRARD (NAVAL Group)
Benoît MARTIN (DGA)
Marc-Oliver PAHL (IMT Atlantique)
Assia TRIA (CEA)

Sponsors