Cybersecurity Institute
Univ. Grenoble Alpes

Subscribe to our newsletter

# Newsletter #5 – May 2019

## Editorial

For this month editorial, we would like to congratulate the members of the CODEC project (Hardware/Software CO-DEsign of processor Countermeasures) which has been selected in the context of the IRS call for projects held by the IDEX Univ. Grenoble Alpes. This interdisciplinary project represents a new collaboration between members of the CTSYS and Verimag teams, focused on designing applications resilient against fault injection, and embodies the values of the Grenoble Alpes Cybersecurity Institute for a holistic approach to cybersecurity.

We would also like to mention the CyberSmartLearn project, presented by Jean-Marie Flaus at the Forum 5i (Grenoble – May 15th 2019). This project uses innovative machine learning algorithms in order to build a model of normal behavior for IoT networks. This model is then used for detecting anomalies on IoT networks without interfering with the normal execution of the system.

Finally, this edition's monthly column focuses on the research activities of the CTSYS team in the LCIS laboratory.

## Events and calls for papers

Global Challenges Science Week – June 3-6th 2019
During the Global Challenges Science Week, the Grenoble Alpes Cybersecurity Institute will organize a workshop entitled "*Cybersecurity and society: on the necessity of an interdisciplinary approach*". The full program and registration form is available here.

Call for papers: Artificial Intelligence & Defense (C&ESAR conference) – November 21st 2019
The first conference "AI & Defense" will take place on November 21st 2019 during the 4th edition of the European Cyber Week (ECW). The call for papers is now opened and will close on June 28th 2019.

## Accepted papers and conferences

- Franck Sicard, Eric Zamaï, Jean-Marie Flaus, **An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems,** Reliability Engineering & System Safety, Volume 188, August 2019, Pages 584-603

## PhD positions

- Vulnerability search in Industrial Control Systems; a reverse engineering approach
- Hardware/Software co-design of countermeasures against fault injection
- Tools and methods for securing a memory hierarchy against software side-channel attacks
- Study of new solutions for the security of embedded systems
- Protecting binary elliptic curve cryptography against Template attacks and Horizontal attacks
- Securing integrated circuits against deep learning based attacks
- Resistant and resilient processor to fault attacks and side-channel attacks

- Sécurisation matérielle de cryptographie post-quantique basée sur les isogénies entre courbes elliptiques
- Trusted Internet-of-Things integration into pervasive applications

## Monthly column

### Focus on: Research activities of the CTSYS team (LCIS)

*Vincent Beroulle & David Hély*

Research activities of the CTSYS team (LCIS Lab) in Valence are focused on "safety and security of embedded systems and distributed systems". Distributed and pervasive systems are smart, communicating, often open and dynamically reconfigurable systems. They mix many hardware components (sensors, connected objects, switches) with software components (embedded or non-embedded). These systems are ubiquitous in critical applications and security applications in which safety and security are two key issues. **Read more**