Cybersecurity Institute
Univ. Grenoble Alpes

Subscribe to our newsletter

Newsletter #9 – November 2019

Editorial

In this month's edition, we are happy to announce that a presentation of the Grenoble Alpes Cybersecurity Institute focused on interdisciplinary research has just been published in the latest edition of the Gazette du GdR Sécurité Informatique. We would also like to thank the Pôle d'Excellence Cyber in Rennes for inviting us to present Cyber@Alps during the European CyberWeek (ECW) on november 20th.

Regarding future events, do not forget to register to our workshop on Post-Quantum Cryptography and to the next edition of the Atelier PARI/GP hosted by Institut Fourier on January 20th-24th. We will also be present at the next International Cybersecurity Forum in Lille on January 28-30th.

We also want to remind you that a lot of internship offers are available on our website. Apply now!

Finally, this edition's monthly column focuses on the cybersecurity research activities of the CAS3C3 team of Laboratoire Jean Kuntzmann.

Events

Workshop on Post-Quantum Cryptography – December 17th 2019
In collaboration with Quantum Engineering Univ. Grenoble Alpes, Cyber@Alps is organizing a workshop on Post-quantum Cryptography. The event will take place in the Maison Jean Kuntzmann on december 17th 2019.

Workshop PARI/GP – January 20th - 24th 2020
Register now! Week-long workshop on the computer algebra system PARI/GP, to discuss the current and future development of the PARI/GP system but is open to all arithmeticians with an interest for explicit computations.

International Cybersecurity Forum (FIC) – January 28th-30th 2020 (Lille)
For the third year in a row, Cyber@Alps will be present at FIC2020. More information about our activities will be available shortly.

PhD positions

- DNS Naming and Services for Secure Seamless IoT

Internships

- Vulnérabilités et évaluation des générateurs de nombres aléatoires des composants sécurisés
- Design and study of fast AES-256 and SHA-3 implementations resistant against Side channel and fault attacks
- Reverse engineering of FPGA firmware in control systems devices
- SRAM-Based PUF with STM Controllers
- Visualisation d'indicateurs sur la cybergouvernance
- Implémentation d'algorithmes cryptographiques dans une mémoire intelligente et caractérisation contre les attaques par canaux auxiliaires sur la consommation

Univ. Grenoble Alpes
Editorial executive: philippe.elbaz-vincent@univ-grenoble-alpes.fr
Editor: romain.xu@univ-grenoble-alpes.fr

- Mise en œuvre d'un démonstrateur pour la « self-sovereign identity »
- RealPhish : Detection of phishing domains
- Fault modeling analysis through experimental attacks
- Modification du flot d'implémentation pour la sécurisation de blocs matériels
- Hybrid Number Field Sieve (NFS): Classical and Quantum approaches
- New Steps in Crypto Crowdfunding and their Related Risks
- Market Microstructure and Cryptocurrency Exchanges
- Etude d'un outil de test de pénétration de communication inter-composants
- Nouveaux schémas de Pseudonymisation
- TRUSTEE
- Static analysis of programs for micro-architecture aware fault models
- Ensuring Control-Flow Integrity in presence of Faults Injection
- Protecting a software against Control-Flow Integrity attacks
- Modeling Control-Flow Attackers of a Secure Cryptoprocessor
- Implémentation de primitives pour la cryptographie sur courbes elliptiques définies sur GF(p)
- Sécurisation de blocs matériels contre les attaques physiques en modifiant les options d'implémentation

Monthly column

Focus on: Cybersecurity Research activities of the CAS3C3 Team of Laboratoire Jean Kuntzmann

Cybersecurity research activities of the CAS^{3}C^3 team (Computer Algebra, Security, Complex Systems, Codes, Secrets, Cryptology) are focused on:

- Design and analysis of symmetric cryptographic primitives and their secure and efficient implementation.
- Proof of work certificates for outsourced cloud computing.
- Fault tolerant schemes in linear algebra.
- Secure protocols for multi-party, zero-knowledge or industrial control systems. **Read more**

Univ. Grenoble Alpes
Editorial executive: philippe.elbaz-vincent@univ-grenoble-alpes.fr
Editor: romain.xu@univ-grenoble-alpes.fr