Demi-journée Scientifique

Défi Clé ICO

SÉCURITÉ POUR ET PAR LE MATÉRIEL

04 mai 2026

14h - 17h45

IRIT
Institut de Recherche en Informatique de Toulouse
CNRS - Toulouse INP - UT - UT Capitole - UT2

AMPHI HERBRAND
IRIT
UNIVERSITÉ DE TOULOUSE
118 ROUTE DE NARBONNE
TOULOUSE

Évènement placé sous le signe de la collaboration avec la THCon 2026

Défis Clés OCCITANIE
La Région Occitanie Pyrénées - Méditerranée
cnrs
ICO Institut Cybersécurité Occitanie

PROGRAMME

14h00 **ACCUEIL**

14h00 - 14h15
INTRODUCTION

14h00 - 14h15

Vincent NICOMETTE
(INSA TOULOUSE,
LAAS-CNRS)

Introduction - Présentation du Défi Clé « ICO »

14h15 - 16h00
INTERVENTIONS

14h15 - 14h50

Sophie DUPUIS
(LIRMM)

Logic locking: ten years since the SAT attack

Logic Locking is a prominent Design-for-Trust technique aiming at protecting IP against supply-chain attacks.

Since it was successfully attacked in 2015 by the well-known SAT attack, a cat-and-mouse game has been established between developing and attacking Logic Locking techniques, resulting in dozens of defense techniques and attack strategies.

This talk surveys notable advances in the field of Logic Locking, focusing more on recent trends. Among the works cited, particular attention will be paid to the work we have been conducting at LIRMM for the past ten years or so.

PROGRAMME

Sophie DUPUIS received the M.Sc. and Ph.D. degrees in microelectronics and design on integrated circuits from Pierre and Marie Curie University, Paris, France, in 2004 and 2009, respectively.

She has been an Associate Professor with LIRMM, University of Montpellier, Montpellier, France, since 2011.

Her current research interests are oriented toward hardware security and trust, particularly the design of trusted circuits despite potential untrustworthy design steps.

14h50-15h25

Benoît MORGAN (Intel)

Scholar Inside: A Journey from Academia to Offensive Security in the Semiconductor Industry

This presentation highlights key offensive security research activities conducted by the INT31 group. In particular, it explores the major challenges we face and how addressing them has required specialized approaches, reshaping the expectations of a researcher transitioning from academia to industry.

Benoît MORGAN earned his PhD in 2016, focusing on remote attestation for complex systems. He is an assistant professor at INP-ENSEEIHT, a public engineering school, and recently joined Intel's offensive security research group, INT31. His current work focuses on microarchitectural vulnerability research and the development of offensive security tools.

PROGRAMME

15h25 - 16h00

Philippe MAURINE (LIRMM)

ARTHEMIS

ARTHEMIS est une nouvelle équipe de recherche dont les activités ont pour centre de gravité la sécurité du matériel. Cette présentation aura pour but de présenter l'équipe ainsi que certaines de ses activités ou verrous scientifiques et techniques qu'elle souhaite aborder à l'avenir. Ceux-ci concernent à la fois l'anticipation des menaces et les solutions de protection à déployer tout au long du processus de conception et de caractérisation d'un produit intégré assurant des services de sécurité.

Philippe MAURINE est professeur à l'Université de Montpellier et membre du Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM). Il est spécialisé dans les domaines de la microélectronique, de la sécurité des circuits intégrés, de l'injection de fautes et des attaques par canaux auxiliaires, exploitant notamment le canal électromagnétique. Ses travaux de recherche portent notamment sur la modélisation et la protection des circuits sécurisés, ainsi que sur l'analyse des vulnérabilités matérielles.

16h00 - 16h30 ***PAUSE CAFÉ***

16h30 - 17h45

INTERVENTIONS

PROGRAMME

16h30 - 17h05

Victor LOMNÉ
(NinjaLab)

Practical Side-Channel Attacks on Real World Devices

In this talk we will present our public research works about practical side-channel attacks on real world devices. We will describe how we studied the side-channel security of secure devices like the Ledger Nano S (the most sold crypto-currency hardware wallet), the Google Titan Security Key (the hardware token for second factor authentication used by all Google employees) and the Yubico Yubikey Series 5 (the most sold hardware token for second factor authentication with 40% of market share), found a vulnerability, and transformed it in a practical key-recovery attack.

Victor LOMNÉ holds a master degree in cryptology and computer security from the university of Bordeaux, France, and a PhD degree in microelectronics from the university of Montpellier, France. He worked during 7 years as security expert in the hardware security team of the scientific division of ANSSI (French Cybersecurity Agency) in Paris, France. During these years he created and was responsible for the team lab, worked as penetration tester on a wide range of products, and was technical support for the ANSSI National Certification Center. He then came back to work as researcher at the LIRMM (laboratory of computer science, robotics and microelectronics of the university of Montpellier), before co-founding NinjaLab. Victor is also an active academic researcher in the fields of cryptology and hardware security, with publications, keynotes and program committee membership in top conferences like CHES, FDTC and CASCADE.

PROGRAMME

17h05 -17h40

Karine HEYDEMANN
(Thales)

Micro-architecture des processeurs et vérification d'implémentations logicielles masquées

Le masquage représente une contre-mesure couramment adoptée pour protéger contre les attaques par canaux auxiliaires reposant sur l'analyse de la consommation électrique ou des émissions électromagnétiques. Une implémentation masquée peut être formellement prouvée robuste par rapport à un modèle de fuite. Toutefois, sa mise en œuvre logicielle demeure complexe: les optimisations du compilateur peuvent altérer la sécurité garantie au niveau du code source, tandis qu'une implémentation en assembleur, bien que prouvée sécurisée, peut s'avérer vulnérable en pratique en raison des spécificités microarchitecturales de la plateforme cible. Dans un premier temps, nous montrerons l'importance de tenir compte de la microarchitecture lors de la vérification formelle de la sécurité d'un logiciel masqué, avant de présenter la modélisation d'une plateforme SMT32 intégrant un microcontrôleur Cortex-M3, réalisée dans le but de vérifier l'absence de fuites dans les implémentations masquées. Après avoir exposé les limites de cette approche, la dernière partie de l'exposé introduira aLEAKATOR, une nouvelle méthode automatisée permettant la co-vérification de programmes et de processeurs dans divers modèles de fuite. Nous détaillerons le principe d'aLEAKATOR, qui repose sur la simulation en domaines mixtes pour extraire les informations utiles à la vérification, ainsi que des résultats expérimentaux obtenus, avant de conclure cette présentation.

PROGRAMME

Karine HEYDEMANN, titulaire d'un doctorat en informatique de l'Université de Rennes 1, a été recrutée maître de conférences à Sorbonne Université en 2006. Elle a soutenu son HDR en 2017. Depuis 2023, elle est senior expert en sécurité matérielle chez Thales et chercheuse associée au laboratoire LIP6 du Sorbonne Université. Ses travaux de recherche portent sur la sécurité du logiciel ou du couple logiciel matériel face aux attaques en faute et par canal auxiliaire, incluant notamment la modélisation des effets des fautes ou des sources de fuite, ainsi que les méthodes d'analyse de la sécurité des implémentations.

17h40 - 17h45
DISCUSSION GÉNÉRALE - CONCLUSIONS

CONTACT

bureau@ico-occitanie.fr

Défis Clés OCCITANIE

La Région Occitanie Pyrénées - Méditerranée

Institut Cybersécurité Occitanie