

Journées Nationales du GDR Sécurité Informatique

Mercredi 12 juin

08:45 – 09:15 **Accueil**

09:15 – 09:30 **Ouverture des Journées Nationales**

09:30 – 10:30 **Keynote I – Herbert Bos** (VU Amsterdam) *[en anglais] The House is Built on Sand: exploiting hardware glitches and side channels to compromise software without bugs*

10:30 – 11:00 **Pause café**

11:00 – 11:45 **Thomas Baignères & Matthieu Finiasz** (Olvid) *Modèle de sécurité des messageries mobiles*

11:45 – 12:30 **Mathieu Cunche** (Insa Lyon, Inria) *Mécanismes anti-traçage dans les réseaux sans-fil*

12:30 – 14:00 **Pause déjeuner**

14:00 – 15:45 **Session parallèle 1a : Sécurité des systèmes, des logiciels et des réseaux**

14:00 – 14:15: ouverture

14:15 – 15:00: **Lucca Hirschi** (Inria, Loria) – A Formal Analysis of 5G Authentication

15:00 – 15:45: **Timothée Ravier** (ANSSI) – CLIP OS : un système d'exploitation durci open-source

14:00 – 15:45 **Session parallèle 1b : Protection de la vie privée**

14:00 – 14:15: ouverture

14:15 – 15:00: **Sonia Ben Mokhtar** (CNRS/LIRIS) – User Re-Identification Attacks: Tell Me How You Move I will Tell You Who You Are

15:00 – 15:45: **Tristan Allard** (Université de Rennes I, IRISA) – PINED-RQ: A Differentially Private Index for Range Query Processing in Clouds

15:45 – 16:30 **Pause café**

16:30 – 18:00 **Session parallèle 2a : Sécurité des systèmes, des logiciels et des réseaux**

16:30 – 17:15 : **Antoine Vastel** (Inria Lille) – Renforcer la sécurité sur le web en disséquant les empreintes de navigateurs

17:15 – 18:00 : **Kave Salamatian** (Université Savoie Mont Blanc) – Large scale BGP monitoring: where security meets Riemmanian Geometry

16:30 – 18:00 **Session parallèle 2b : Protection de la vie privée**

16:30 – 17:15: **Catuscia Palamidessi** (Inria) *[anglais]* – Local Differential Privacy and trade-off with Utility

Jeudi 13 juin

08:45 – 10:30 **Session parallèle 3a : Sécurité et données multimédia**

08:45 – 09:00: ouverture

09:00 – 09:45: **Christophe Rosenberger** (Normandie Université) – Transformation de données biométriques pour la protection de la vie privée

09:45 – 10:30: **Amine Naït-Ali** (UPEC) – Biométrie cachée : vers une exploration spatio-temporelle

08:45 – 10:30 **Session parallèle 3b : Session commune Codage et cryptographie & Sécurité des systèmes matériels**

08:45 – 09:00: ouverture

09:00 – 09:45: **Pierre-Yves Strub** (Ecole Polytechnique) – Jasmin: High-Assurance and High-Speed Cryptograph

09:45 – 10:30: **Annelie Heuser** (CNRS, Iria) *[en anglais]* – Machine learning for profiled side-channel analysis

10:30 – 11:00 **Pause café**

11:00 – 12:30 **Session parallèle 4a : Sécurité et données multimédia**

11:00 – 11:25: **Jean-Luc Dugelay** (EURECOM) – Malicious Facial Image Processing and Counter-Measures: a review

11:25 – 12:50: **Jean-François Mainguet** (CEA LETI) – Spoofing et capteurs d’empreintes digitales thermiques actifs

11:50 – 12:15: **Aladine Chetouani** (Polytech’ Orléans) – Authentification biométrique comportementale continue sur mobile

12:15 – 12:40: **Philippe Carré** (XLIM) – Tatouage : robustesse et invisibilité

11:00 – 12:30 **Session parallèle 4b : Session commune Codage et cryptographie & Sécurité des systèmes matériels**

11:00 – 11:45 **Vincent Grosso** (CNRS, Uni. Saint Etienne) – Block ciphers tailored for side-channel protection

11:45 – 12:30 **Rina Zeitoun** (IDEMIA) – Side-Channel Attacks and High-Order Countermeasures

12:30 – 14:00 **Pause déjeuner**

14:00 – 14:45 **Adeline Roux-Langlois** (CNRS, Irista) *Signatures reposant sur les réseaux euclidiens*

14:45 – 15:30 **Florent Retraint** (UT Troyes) *Criminalistique des images à partir de modèles statistiques*

15:30 – 16:15 **Pause café**

16:15 – 17:15 **Keynote II – Jean-Jacques Quisquater** (UC Louvain) *Histoires secrète et publique de la carte à puce*

17:15 – 18:30 **Annonces (rump) et discussions**

18h30-21:00 **Visite du Musée des Arts & Métiers**

Vendredi 14 juin

08:45 – 09:30 **Véronique Cortier** (CNRS, Loria) *Electronic voting: how logic can help?*

09:30 – 10:00 **Retour sur les Rencontres Entreprises DOCTORANTS Sécurité (REDOCS)**

10:00 – 10:45 **Pause café**

10:45 – 11:30 **Viktor Fischer** (Université de Saint Etienne) *Random number generation for cryptography – past, present, future*

11:30 – 12:15 **Remise du Prix de Thèse du GDR Sécurité Informatique**

12:15 – 12:30 **Clôture des Journées Nationales**