Programme GTMFS 2025

WIFI : GTMFS2025
Password : `IL0v3GTMFS2025!`

Tuesday 18 march 2025

9h00 - 10h00 : Keynote 1

Véronique Cortier : *Electronic voting: design, attack, and formal verification*

10h00 - 10h30 : Break

10h30 - 12h00 : Session 1 - Proofs of protocols

- *Equational theories with user defined AC function symbols in Tamarin*, Elise Klein (Université de Lorraine), Jannik Dreier (Université de Lorraine), Steve Kremer (Inria Université de Lorraine)
- *Non-deduction proofs in Squirrel and the security of Signal*, Clément Hérouard (Univ. Rennes, CNRS, IRISA), Charlie Jacomme (Université de Lorraine, CNRS, Inria, LORIA), Adrien Koutsos (INRIA Paris), Joseph Lallemand (Univ. Rennes, CNRS, IRISA)
- *Formal verification of security properties of 5G slices : an elementary use case*, Ahmed Bouabdallah (IMT Atlantique)

12h00 - 14h00 : Lunch

14h00 - 15h30 : Session 2 - Code analysis

- *Formally Verified Hardening of C Programs against Hardware Fault Injection*, Basile Pesin (Ecole Nationale de l'Aviation Civile), Sylvain Boulmé (Université Grenoble Alpes), David Monniaux (Université Grenoble Alpes), Marie-Laure Potet (Université Grenoble Alpes)
- *Augmenting Search-based Program Synthesis with Local Inference Rules to Improve Blackbox Deobfuscation*, Vidal Attias (CEA-LIST), Gregoire Menguy (CEA-LIST), Sébastien Bardin (CEA-LIST)
- *Termination Resilience Static Analysis*, Naïm Moussaoui Remil (ENS PSL — Inria Paris), Urban (ENS PSL — Inria Paris)

15h30 - 16h00 : Break

16h00 - 17h00 : Tool session

17h00 - 19h00 : Free

19h00 : Diner

Wednesday 18 march 2025

9h00 - 10h30 : Session 3 - Trust and active defense

- *Vote&Check: Secure Postal Voting with Reduced Trust Assumptions*, Véronique Cortier (Université de Lorraine, CNRS, Inria, LORIA), Alexandre Debant (Université de Lorraine, CNRS, Inria, LORIA), Pierrick Gaudry (Université de Lorraine, CNRS, Inria, LORIA), Léo Louistisserand (Université de Lorraine, CNRS, Inria, LORIA)
- *Stratégies optimales de défense active basées sur la vérification formelle de systèmes multi-agent*, Gabriel Ballot (Télécom Paris - EDF R&D)
- *Formalizing trust in Cyber Threat Intelligence*, Mariam Wehbe (INSA CVL), Laurent Bobelin (INSA CVL), Sabine Frittella (INSA CVL)

10h30 - 11h00 : Break

11h00 - 12h00 : Binsec tutorial

12h00 - 13h30 : Lunch

13h30 - 19h00 : Social Event

19h00 : Gala

Thursday 18 march 2025

9h00 - 10h00 : Keynote 2

Jan Reineke *Verification and Synthesis of Hardware-Software Leakage Contracts*

10h00 - 10h30 : Break

10h30 - 12h00 : Session 4 - Symbolic execution

- *A Scalable Framework for Backward Bounded Static Symbolic Execution*, Nicolas Bellec (CEA-LIST), Grégoire Menguy (CEA-LIST), Frederic Recoules (CEA-LIST), Sébastien Bardin (CEA-LIST)
- *Design and Usage of a Modular Implementation for Relational Analyses in Binsec: Constant Time and Secret Erasure*, Yanis Sellami (CEA, List), Frédéric Recoules (CEA, List), Sébastien Bardin (CEA, List)
- *Quantitative Robustness for Vulnerability Assessment*, Guilhem Lacombe (CEA LIST, Université Paris-Saclay), Sébastien Bardin (CEA LIST, Université Paris-Saclay)

12h00 - 14h00 : Lunch

14h00 - 15h30 : Session 5 - Attacks on protocols

Automated Discovery of Subtle Attacks on Protocols using Mix-Nets, Jannik Dreier (Université de Lorraine), Pascal Lafourcade (Université Clermont-Auvergne), Dhekra Mahmoud (Université Clermont-Auvergne)

- *New Formalisation & Attack-finding for Session Unlinkability*, Ioana Cristina Boureanu (Surrey Centre for Cyber Security, University of Surrey), Fortunat Rajaona (Surrey Centre for Cyber Security, University of Surrey)
- *Differential DY fuzzing : Adding differential fuzzing to the Puffin fuzzer*, Tom Gouville (Inria Nancy)

15h30 - 16h00 : Break

16h00 - 17h30 : Rump session + Business meeting

17h30 - 19h00 : Free

19h00 : Diner