



Paper 63 **Osiris: Automated Discovery of Microarchitectural Side Channels**

Daniel Weber (CISPA Helmholtz Center for Information Security), **Ahmad Ibrahim** (CISPA Helmholtz Center for Information Security), **Hamed Nemati** (CISPA Helmholtz Center for Information Security), **Michael Schwarz** (CISPA Helmholtz Center for Information Security), **Christian Rossow** (CISPA Helmholtz Center for Information Security)

Paper 64 **The Cookie Hunter: Automated Black-box Auditing for Web Authentication and Authorization Flaws**

Kostas Drakonakis (Foundation for Research and Technology Hellas), **Sotiris Ioannidis** (Technical University of Crete, Greece), **Jason Polakis** (University of Illinois at Chicago, USA)

Paper 70 **Shadow-Catcher: Looking Into Shadows to Detect Ghost Objects in Autonomous Vehicle 3D Sensing**

Zhongyuan Hau (Imperial College London), **Soteris Demetriou** (Imperial College London), **Luis Muñoz-González** (Imperial College London), **Emil Lupu** (Imperial College)

Paper 83 **SEApp: Bringing Mandatory Access Control to Android Apps**

Matthew Rossi (Università degli Studi di Bergamo), **Dario Facchinetti** (Università degli Studi di Bergamo), **Enrico Bacis** (Università degli Studi di Bergamo), **Marco Rosa** (SAP Security Research), **Stefano Paraboschi** (Università degli Studi di Bergamo)

Paper 110 **Information Leakages in Code-based Masking: A Unified Quantification Approach**

Wei Cheng (Télécom Paris; Institut Polytechnique De Paris, France), **Sylvain Guilley** (Secure-IC S.A.S.; Télécom Paris; Institut Polytechnique de Paris, France), **Claude Carlet** (LAGA, Department of Mathematics, University of Paris VIII, Paris, France; University of Bergen, Norway), **Jean-Luc Danger** (Télécom Paris; Institut Polytechnique De Paris, France), **Sihem Mesnager** (LAGA, Department of Mathematics, University of Paris VIII; Telecom Paris, Polytechnic Institute of Paris, France)

Paper 111 **Rage Against the Machine Clear: A Systematic Analysis of Machine Clears and Their Implications for Transient Execution Attacks**

Hany Ragab (Vrije Universiteit Amsterdam), **Enrico Barberis** (Vrije Universiteit Amsterdam), **Herbert Bos** (Vrije Universiteit Amsterdam), **Cristiano Giuffrida** (Vrije Universiteit Amsterdam)

Paper 112 **POSEIDON: Privacy-Preserving Federated Neural Network Learning**

Sinem Sav (EPFL), **Apostolos Pyrgelis** (EPFL), **Juan Ramon Troncoso-Pastoriza** (EPFL), **David Froelicher** (EPFL), **Jean-Philippe Bossuat** (EPFL), **Joao Sa Sousa** (EPFL), **Jean-Pierre Hubaux** (EPFL)

Paper 114 **Fast verification of masking schemes in characteristic two**

Nicolas Bordes (Université Grenoble Alpes), **Pierre Karpman** (Université Grenoble Alpes)

Paper 115 **Locally Private Graph Neural Networks**

Sina Sajadmanesh (Idiap Research Institute / EPFL), **Daniel Gatica-Perez** (Idiap Research Institute / EPFL)

Paper 118 **One Glitch to Rule Them All: Fault Injection Attacks Against AMD's Secure Encrypted Virtualization**

Robert Bühren (Technische Universität Berlin - SECT), **Hans Niklas Jacob** (Technische Universität Berlin - SECT), **Thilo Krachenfels** (Technische Universität Berlin - SECT), **Jean-Pierre Seifert** (Technische Universität Berlin - SECT / Fraunhofer SIT)