CSAW'20 EUROPE

APPLIED RESEARCH COMPETITION

FINALIST PAPERS P.1

Published, online papers are linked in the title. Listed in random order. Presenters are in bold.

Cached and Confused: Web Cache Deception in the Wild

Seyed Ali Mirheidari (University of Trento), Sajjad Arshad (Northeastern University), Kaan Onarlioglu (Akamai Technologies), Bruno Crispo (University of Trento, KU Leuven), Engin Kirda (Northeastern University), William Robertson (Northeastern University)

Optimizing Inner Product Masking Scheme by A Coding Theory Approach

Wei Cheng (LTCI, Télécom Paris), Sylvain Guilley (Secure-IC; LTCI, Télécom Paris), Claude Carlet (LAGA, Department of Mathematics, University of Paris 8), Sihem Mesnager (LAGA, Department of Mathematics, University of Paris 8), Jean-Luc Danger (LTCI, Télécom Paris; Secure-IC)

Dragonblood is Still Leaking: Practical Cache-based Side-Channel in the Wild

Daniel De Almeida Braga (University of Rennes 1), Pierre-Alain Fouque (University of Rennes 1), Mohamed Sabt (University of Rennes 1)

LVI: Hijacking Transient Execution through Microarchitectural Load Value Injection

Jo Van Bulck (KU Leuven), Daniel Moghimi (Worcester Polytechnic Institute), Michael Schwarz (Graz University of Technology), Moritz Lipp (Graz University of Technology)

Procedural Noise Adversarial Examples for Black-Box Attacks on Deep Convolutional Networks

Kenneth T. Co (Imperial College London), Luis Muñoz-González (Imperial College London), Sixte de Maupeou (Imperial College London), Emil Lupu (Imperial College London)

CSAW'20 EUROPE

APPLIED RESEARCH COMPETITION

FINALIST PAPERS P.2

Published, online papers are linked in the title. Listed in random order. Presenters are in bold.

HYBCACHE: Hybrid Side-Channel-Resilient Caches for Trusted Execution Environments

Ghada Dessouky (Technische Universität Darmstadt), Tommaso Frassetto (Technische Universität Darmstadt), Ahmad-Reza Sadeghi (Technische Universität Darmstadt)

Understanding Screaming Channels: From a Detailed Analysis to Improved Attacks

Giovanni Camurati (EURECOM), Aurélien Francillon (EURECOM), François-Xavier Standaert (Université catholique de Louvain)

RISQ-V: Tightly Coupled RISC-V Accelerators for Post-Quantum Cryptography

Tim Fritzmann (Technical University of Munich), Johanna Sepùlveda (AIRBUS Defence and Space GmbH), Georg Sigl (Technical University of Munich)

SpecFuzz: Bringing Spectre-type vulnerabilities to the surface

Oleksii Oleksenko (TU Dresden), Bohdan Trach (TU Dresden), Mark Silberstein (Technion), Christof Fetzer (TU Dresden)

TeeRex: Discovery and Exploitation of Memory Corruption Vulnerabilities in SGX Enclaves

Tobias Cloosters (University of Duisburg-Essen), Michael Rodler (University of Duisburg-Essen), Lucas Davi (University of Duisburg-Essen)