2021 International Symposium on Secure and Private Execution Environment Design (SEED 2021)

Virtual Conference
20-21 September 2021

IEEE Catalog Number: CFP21Z58-POD
ISBN: 978-1-6654-2026-6

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP21Z58-POD
ISBN (Print-On-Demand):	978-1-6654-2026-6
ISBN (Online):	978-1-6654-2025-9

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

2021 International Symposium on Secure and Private Execution Environment Design (SEED)

SEED 2021

Table of Contents

Message from General Chairs ix
Message from Program Chairs x
Organizing Committee xii
Program Committee xiii
Steering Committee xiv
Keynotes xv

Session 1: "The Eternal War of Side Channels"

Cloak & Co-Locate: Adversarial Railroading of Resource Sharing-Based Attacks on the Cloud 1
Hosein Mohammadi Makrani (UC Davis, USA), Hossein Sayadi (California State University Long Beach, USA), Najmeh Nazari (UC Davis, USA), Khaled N. Khasawneh (George Mason University, USA), Avesta Sasan (UC Davis, USA), Setareh Rafatirad (UC Davis, USA), and Houman Homayoun (UC Davis, USA)

Seeds of SEED: A Side-Channel Resilient Cache Skewed by a Linear Function over a Galois Field 14
Scott Constable (Security and Privacy Research (SPR), Intel Corporation) and Thomas Unterluggauer (Security and Privacy Research (SPR), Intel Corporation)

Seeds of SEED: R-SAW: New Side Channels Exploiting Read Asymmetry in MLC Phase Change Memories 22
Md Hafizul Islam Chowdhuryy (University of Central Florida), Rickard Ewetz (University of Central Florida), Amro Awad (North Carolina State University), and Fan Yao (University of Central Florida)

Seeds of SEED: H2Cache: Building a Hybrid Randomized Cache Hierarchy for Mitigating Cache Side-Channel Attacks 29
Xingjian Zhang (Zhejiang University, China), Ziqi Yuan (Zhejiang University, China), Rui Chang (Zhejiang University, China), and Yajin Zhou (Zhejiang University, China)

Bespoke Cache Enclaves: Fine-Grained and Scalable Isolation from Cache Side-Channels via Flexible Set-Partitioning 37
Gururaj Saileshwar (Georgia Institute of Technology, USA), Sanjay Kariyappa (Georgia Institute of Technology, USAA), and Moinuddin Qureshi (Georgia Institute of Technology, USA)

Session 2: "All Good Memories!"

Performance-Enhanced Integrity Verification for Large Memories 50
Yanan Guo (University of Pittsburgh, USA), Andrew Zigerelli (University of Pittsburgh, USA), Yueqiang Cheng (NIO, USA), Youtao Zhang (University of Pittsburgh, USA), and Jun Yang (University of Pittsburgh, USA)

Seeds of SEED: Efficient Access Pattern Obfuscation for Untrusted Hybrid Memory System 63
Yuezhi Che (Illinois Institute of Technology), Gang Liu (Hunan University), and Rujia Wang (Illinois Institute of Technology)

Seeds of SEED: H-CRAM: In-Memory Homomorphic Search Accelerator Using Spintronic Computational RAM 70
Husrev Cilasun (University of Minnesota, Twin Cities, United States), Salonik Resch (University of Minnesota, Twin Cities, United States), Zamshed I. Chowdhury (University of Minnesota, Twin Cities, United States), Masoud Zabihi (University of Minnesota, Twin Cities, United States), Zhengyang Zhao (University of Minnesota, Twin Cities, United States), Thomas Peterson (University of Minnesota, Twin Cities, United States), Jian-Ping Wang (University of Minnesota, Twin Cities, United States), Sachin S. Sapatnekar (University of Minnesota, Twin Cities, United States), and Ulya R. Karpuzcu (University of Minnesota, Twin Cities, United States)

Seeds of SEED: NMT-Stroke: Diverting Neural Machine Translation Through Hardware-Based Faults 76
Kunbei Cai (University of Central Florida, USA), Md Hafizul Islam Chowdhuryy (University of Central Florida, USA), Zhenkai Zhang (Clemson University, USA), and Fan Yao (University of Central Florida, USA)

Seeds of SEED: New Security Challenges for Persistent Memory 83
Naveed Ul Mustafa (University of Central Florida, USA), Yuanchao Xu (NCSU, USA), Xipeng Shen (NCSU, USA), and Yan Solihin (University of Central Florida, USA)

Session 3: "To Speculate or Not, That is the Question!"

Do Not Predict - Recompute! How Value Recomputation Can Truly Boost the Performance of Invisible Speculation 89
Christos Sakalis (Uppsala University, Sweden), Zamshed I. Chowdhury (University of Minnesota, USA), Shayne Wadle (University of Wisconsin, USA), Ismail Akturk (Ozyegin University, Turkey), Alberto Ros (University of Murcia, Spain), Magnus Själander (Norwegian University of Science and Technology, Norway), Stefanos Kaxiras (Uppsala University, Sweden), and Ulya R. Karpuzcu (University of Minnesota, USA)

Seeds of SEED: Preventing Priority Inversion in Instruction Scheduling to Disrupt Speculative Interference 101
Christos Sakalis (Uppsala University, Sweden), Magnus Själander (Norwegian University of Science and Technology, Norway), and Stefanos Kaxiras (Uppsala University, Sweden)

SoK: Hardware Defenses Against Speculative Execution Attacks 108
Guangyuan Hu (Princeton University, USA), Zecheng He (Princeton University, USA), and Ruby B. Lee (Princeton University, USA)

Session 4: Roundtable: "All Roads Lead to Privacy-Enhanced Computing”

Security Analysis of Confidential-Compute Instruction Set Architecture for Virtualized Workloads 121
Ravi Sahita (Intel Corp., USA), Dror Caspi (Intel Corp., USA), Barry Huntley (Intel Corp., USA), Vincent Scarlata (Intel Corp., USA), Baruch Chaikin (Intel Corp., USA), Siddhartha Chhabra (Intel Corp., USA), Arie Aharon (Intel Corp., USA), and Ido Ouziel (Intel Corp., USA)

Confidential Computing——A Brave New World 132
Dominic P. Mulligan (Arm Research, UK), Gustavo Petri (Arm Research, UK), Nick Spinale (Arm Research, UK), Gareth Stockwell (Arm Research, UK), and Hugo J. M. Vincent (Arm Research, UK)

VIP-Bench: A Benchmark Suite for Evaluating Privacy-Enhanced Computation Frameworks 139
Lauren Biernacki (University of Michigan), Meron Zerihun Demissie (Addis Ababa University), Kidus Birkayehu Workneh (Addis Ababa University), Galane Basha Namomsa (Addis Ababa University), Plato Gebremedhin (Addis Ababa University), Fitsum Assamnew Andargie (Addis Ababa University), Brandon Reagen (New York University), and Todd Austin (University of Michigan)

Context-Aware Privacy-Optimizing Address Tracing 150
Deeksha Dangwal (University of California, Santa Barbara), Zhizhou Zhang (University of California, Santa Barbara), Jedidiah R Crandall (Arizona State University), and Timothy Sherwood (University of California, Santa Barbara)

Session 5: “Memory Safety - Does it Need to be HARD?”

EPI: Efficient Pointer Integrity for Securing Embedded Systems 163
Evgeny Manzhosov (Columbia University, United States), Vasileios P. Kemerlis (Brown University, United States), Simha Sethumadhavan (Columbia University, United States), Mohamed Tarek Ibn Ziad (Columbia University), and Miguel A Arroyo (Columbia University)

Track Conventions, Not Attack Signatures: Fortifying X86 ABI and System Call Interfaces to Mitigate Code Reuse Attacks 176
Sarp Ozdemir (Binghamton University, NY), Rutvik Saptarshi (Binghamton University, NY), Aravind Prakash (Binghamton University, NY), and Dmitry Ponomarev (Binghamton University, NY)

Session 6: "What's in Store for Secure Execution Environments?"

JAXED: Reverse Engineering DNN Architectures Leveraging JIT GEMM Libraries 189
Malith Jayaweera (Northeastern University, USA), Kaustubh Shivdikar (Northeastern University, USA), Yanzhi Wang (Northeastern University, USA), and David Kaeli (Northeastern University, USA)

Seeds of SEED: Characterizing Enclave-Level Parallelism in Secure Multicore Processors 203
Brandon D'Agostino (University of Connecticut, USA) and Omer Khan (University of Connecticut, USA)

Seeds of SEED: Building and Verifying Foundationally Isolated Hardware Architectures 210
Jason Oberg (Tortuga Logic, Inc., USA)

Implementing a Security Architecture for Safety-Critical Railway Infrastructure 215
Michael Eckel (Fraunhofer Institute for Secure Information Technology SIT, Germany), Don Kuzhiyelil (SYSGO GmbH, Germany), Christoph Krauß (Darmstadt University of Applied Sciences, Germany), Maria Zhdanova (Fraunhofer Institute for Secure Information Technology SIT, Germany), Stefan Katzenbeisser (University of Passau, Germany), Jasmin Cosic (DB Netz, Germany), Matthias Drodt (DB Netz, Germany), and Jean-Jacques Pitrolle (SYSGO GmbH, Germany)

Author Index **227**