2022 IEEE International Symposium on Secure and Private Execution Environment Design (SEED 2022)

Storrs, Connecticut, USA
26-27 September 2022

IEEE Catalog Number: CFP22Z58-POD
ISBN: 978-1-6654-8527-2

Copyright © 2022 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** 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:	CFP22Z58-POD
ISBN (Print-On-Demand):	978-1-6654-8527-2
ISBN (Online):	978-1-6654-8526-5

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

CURRAN ASSOCIATES INC.
proceedings
.com

2022 IEEE International Symposium on Secure and Private Execution Environment Design (SEED)

SEED 2022

Table of Contents

Committees .... **viii**
Keynote Speakers .... **x**
Sponsors .... **xiii**

Session 1: Caches

Avenger: Punishing the Cross-Core Last-Level Cache Attacker and Not the Victim by Isolating the Attacker 1
Yashika Verma (IIT Kanpur, India) and Biswabandan Panda (IIT Bombay, India)

Chameleon Cache: Approximating Fully Associative Caches with Random Replacement to Prevent Contention-Based Cache Attacks 13
Thomas Unterluggauer (Intel Corporation), Austin Harris (University of Texas at Austin), Scott Constable (Intel Corporation), Fangfei Liu (Intel Corporation), and Carlos Rozas (Intel Corporaton)

PREDATOR: A Cache Side-Channel Attack Detector Based on Precise Event Monitoring 25
Minjun Wu (University of Minnesota, USA), Stephen McCamant (University of Minnesota, USA), Pen-Chung Yew (University of Minnesota, USA), and Antonia Zhai (University of Minnesota, USA)

These Aren't The Caches You're Looking For: Stochastic Channels on Randomized Caches 37
Tarunesh Verma (University of Michigan, USA), Achilleas Anastasopoulos (University of Michigan, USA), and Todd Austin (University of Michigan, USA)

Data-Out Instruction-In (DOIN!): Leveraging Inclusive Caches To Attack Speculative Delay Schemes 49
Pavlos Aimoniotis (Uppsala University, Sweden), Amund Bergland Kvalsvik (Norwegian University of Science and Technology, Norway), Magnus Själander (Norwegian University of Science and Technology, Norway), and Stefanos Kaxiras (Uppsala University, Sweden)

Session 2: Crypto & ML

Accelerating Polynomial Multiplication for Homomorphic Encryption on GPUs 61
Kaustubh Shivdikar (Northeastern University, USA), Gilbert Jonatan (KAIST University, South Korea), Evelio Mora (Universidad Católica de Murcia, Spain), Neal Livesay (Northeastern University, USA), Rashmi Agrawal (Boston University, USA), Ajay Joshi (Boston University, USA), José L. Abellán (Universidad Católica de Murcia, Spain), John Kim (KAIST University, South Korea), and David Kaeli (Northeastern University, USA)

Sequestered Encryption: A Hardware Technique for Comprehensive Data Privacy 73
Lauren Biernacki (University of Michigan), Meron Zerihun Demissie (University of Michigan), Kidus Birkayehu Workneh (University of Colorado Boulder), Fitsum Assamnew Andargie (Addis Ababa University), and Todd Austin (University of Michigan)

Establishing Cooperative Computation with Hardware Embassies 85
Alvin Oliver Glova (UC Santa Barbara), Yukai Yang (University of Pennsylvania), Yiyao Wan (UC San Diego), Zhizhou Zhang (UC Santa Barbara), George Michelogiannakis (Lawrence Berkeley National Laboratory), Jonathan Balkind (UC Santa Barbara), and Timothy Sherwood (UC Santa Barbara)

Foreseer: Efficiently Forecasting Malware Event Series with Long Short-Term Memory 97
Kailash Gogineni (The George Washington University, USA), Preet Derasari (The George Washington University, USA), and Guru Venkataramani (The George Washington University, USA)

Session 3: Secure Environments

SoK: Confidential Quartet - Comparison of Platforms for Virtualization-Based Confidential Computing 109
Roberto Guanciale (Royal Institute of Technology (KTH), Sweden), Nicolae Paladi (Lund University and CanaryBit, Sweden), and Arash Vahidi (Research Institutes of Sweden (RISE), Sweden)

SoK: Limitations of Confidential Computing via TEEs for High-Performance Compute Systems 121
Ayaz Akram (University of California, Davis), Venkatesh Akella (University of California, Davis), Sean Peisert (University of California, Davis and Lawrence Berkeley National Lab), and Jason Lowe-Power (University of California, Davis)

Pagoda: Towards Binary Code Privacy Protection with SGX-Based Execute-Only Memory 133
Jiyong Yu (University of Illinois at Urbana-Champaign), Xinyang Ge (Databricks), Trent Jaeger (Penn State University), Chris Fletcher (University of Illinois at Urbana-Champaign), and Weidong Cui (Microsoft Research)

Enclyzer: Automated Analysis of Transient Data Leaks on Intel SGX 145
Jiuqin Zhou (Southern University of Science and Technology, China), Yuan Xiao (Intel Labs, US), Radu Teodorescu (The Ohio State University, US), and Yinqian Zhang (Southern University of Science and Technology, China)

Session 4: Architecture

Improving the Security and Programmability of Persistent Memory Objects 157
Derrick Greenspan (University of Central Florida, United States), Naveed Ul Mustafa (University of Central Florida, United States), Zoran Kolega (University of Central Florida, United States), Mark Heinrich (University of Central Florida, United States), and Yan Solihin (University of Central Florida, United States)

A Compiler for Transparent Namespace-Based Access Control for the Zeno Architecture 169
Jacob Abraham (Arizona State University), Alan Ehret (Arizona State University), and Michel A. Kinsy (Arizona State University)

Eliminating Micro-Architectural Side-Channel Attacks using Near Memory Processing 179
Casey Nelson (Brown University), Joseph Izraelevitz (University of Colorado Boulder), R. Iris Bahar (Colorado School of Mines), and Tamara Silbergleit Lehman (University of Colorado Boulder)

Protecting On-Chip Data Access Against Timing-Based Side-Channel Attacks on Multicores 190
Usman Ali (University of Connecticut, USA), Abdul Rasheed Sahni (University of Connecticut, USA), and Omer Khan (University of Connecticut, USA)

Author Index **203**