2024 IEEE Secure Development Conference (SecDev 2024)

Pittsburgh, Pennsylvania, USA
7-9 October 2024

IEEE Catalog Number: CFP24H06-POD
ISBN: 979-8-3503-9194-7

Copyright © 2024 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: CFP24H06-POD
ISBN (Print-On-Demand): 979-8-3503-9194-7
ISBN (Online): 979-8-3503-9193-0

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

2024 IEEE Secure Development Conference (SecDev)

SecDev 2024

Table of Contents

Message from Program Chairs .... **viii**

2024 IEEE Secure Development Conference

Verifiable Multi-Agent Multi-Task Assignment 1
Thomas Lavaur (Fédération ENAC ISAE-SUPAERO ONERA and Université Toulouse III Paul Sabatier, France), Déborah Conforto Nedelmann (Fédération ENAC ISAE-SUPAERO ONERA, France), Corentin Chauffaut (Fédération ENAC ISAE-SUPAERO ONERA, France), Jérôme Lacan (Fédération ENAC ISAE-SUPAERO ONERA, France), and Caroline P. C. Chanel (Fédération ENAC ISAE-SUPAERO ONERA, France)

Designing Secure AI-Based Systems: A Multi-Vocal Literature Review 13
Simon Schneider (Hamburg University of Technology, Germany), Ananya Saha (Hamburg University of Technology, Germany), Emanuele Mezzi (Vrije Universiteit Amsterdam, The Netherlands), Katja Tuma (Vrije Universiteit Amsterdam, The Netherlands), and Riccardo Scandariato (Hamburg University of Technology, Germany)

Repairing Infrastructure-as-Code using Large Language Models 20
En Low (Singapore University of Technology and Design, Singapore), Carmen Cheh (Illinois Advanced Research Center at Singapore Ltd., Singapore), and Binbin Chen (Singapore University of Technology and Design, Singapore)

Evasion Attacks on Object Detection Models using Attack Transferability 28
Arjun E. R. R (Coimbatore Institute of Technology, India), Pavan Kulkarni (Bosch Global Software Technologies Pvt. Ltd., India), Yuvaraj Govindarajulu (Bosch Global Software Technologies Pvt. Ltd., India), Harshit Shah (University of Southern California, USA), and Manojkumar Parmar (Bosch Global Software Technologies Pvt. Ltd., India)

From Automation to CI/CD: A Comparative Evaluation of Threat Modeling Tools 35
Dimitri Van Landuyt (KU Leuven, Belgium), Laurens Sion (KU Leuven, Belgium), Walewein Philips (KU Leuven, Belgium), and Wouter Joosen (KU Leuven, Belgium)

BliMe Linter 46
Hossam ElAtali (University of Waterloo, Canada), Xiaohe Duan (University of Waterloo, Canada), Hans Liljestrand (Intel Labs, Canada), Meng Xu (University of Waterloo, Canada), and N. Asokan (University of Waterloo, Canada)

Understanding the Challenges in Detecting Vulnerabilities of Rust Applications 54
Diane B. Stephens (University of Georgia, USA), Kawkab Aldoshan (University of Georgia, USA), and Mustakimur Rahman Khandaker (University of Georgia, USA)

User Privacy in the Digital Playground: An In-Depth Investigation of Facebook Instant Games 64
Sideeq Bello (Louisiana State University, USA), Babangida Bappah (Louisiana State University, USA), Nicholas R Tanet (Louisiana State University, USA), Arabelle S Betzwieser (Louisiana State University, USA), and Aisha Ali-Gombe (Louisiana State University, USA)

iConPAL: LLM-Guided Policy Authoring Assistant for Configuring IoT Defenses 76
Mahbub Alam (Syracuse University, USA), Siwei Zhang (Syracuse University, USA), Eric Rodriguez (Syracuse University, USA), Akib Nafis (Syracuse University, USA), and Endadul Hoque (Syracuse University, USA)

Community Security Champions: Studying the Most Influential Users on Security Stack Exchange 93
Partha Das Chowdhury (University of Bristol, UK), Mohammad Tahaei (International Computer Science Institute), Matthew Edwards (University of Bristol, UK), Claudia Peersman (University of Bristol, UK), Lata Nautiyal (University of Bristol, UK), Kopo Marvin Ramokapane (University of Bristol, UK), and Awais Rashid (University of Bristol, UK)

Sharing Without Showing: Secure Cloud Analytics with Trusted Execution Environments 105
Marcus Birgersson (KTH Royal Institute of Technology, Sweden), Cyrille Artho (KTH Royal Institute of Technology, Sweden), and Musard Balliu (KTH Royal Institute of Technology, Sweden)

GENIE: Guarding the npm Ecosystem with Semantic Malware Detection 117
Matías F. Gobbi (Bundeswehr University Munich, Germany) and Johannes Kinder (LMU Munich, Germany)

Octal: Efficient Automatic Data-Oblivious Program Transformations to Eliminate Side-Channel Leakage 129
Biniyam Tiruye (University of Michigan, U.S.A.), Lauren Biernacki (Lafayette College, U.S.A.), Tersiteab Adem (University of Michigan, U.S.A.), Petros Mola (Addis Ababa University, Ethiopia), and Todd Austin (University of Michigan, U.S.A.)

Moving from the Developer Machine to IoT Devices: An Empirical Study 140
Rabbi Alam (University of North Carolina at Charlotte, USA), Jinpeng Wei (University of North Carolina at Charlotte, USA), Sajidul Islam Sajid (Towson University, USA), Qingyang Wang (Louisiana State University, USA), and Chenglong Fu (University of North Carolina at Charlotte, USA)

Lessons Learned and Challenges of Deploying Control Flow Integrity in Complex Software: the Case of OpenJDK's Java Virtual Machine 153
Sabine Houy (Umeå University, Sweden) and Alexandre Bartel (Umeå University, Sweden)

DeTRAP: RISC-V Return Address Protection With Debug Triggers 166
Isaac Richter (University of Rochester, USA), Jie Zhou (George Washington University, USA), and John Criswell (University of Rochester, USA)

A NAND Use Case for Cybersecurity Experiments 178
Timothy Fraser (Timothy Jon Fraser Consulting LLC, USA), Xuwei Liu (Purdue University, USA), Qingkai Shi (Purdue University, USA), Xiangyu Zhang (Purdue University, USA), Mark Wutka (Vanderbilt University, USA), Daniel Balasubramanian (Vanderbilt University, USA), Hao Chen (Yale University, USA), and Zhong Shao (Yale University, USA)

Toward Partial Proofs of Vulnerabilities 180
Jonathan Brossard (Conservatoire National des Arts et Métiers, France)

Reverse Engineering Branch Prediction Capabilities in Modern Micro-Architectures 183
Rodrigo Branco (Oregon State University, USA) and Ben Lee (Oregon State University, USA)

Tutorial: Open Source Software (OSS) Transparency 186
Carol Woody (Software Engineering Institute, Carnegie Mellon University, USA) and Scott Hissam (Software Engineering Institute, Carnegie Mellon University, USA)

Author Index **189**