2023 IEEE Secure Development Conference (SecDev 2023)

Atlanta, Georgia, USA
18-20 October 2023

IEEE Catalog Number: CFP23H06-POD
ISBN: 979-8-3503-3133-2

**Copyright © 2023 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:	CFP23H06-POD
ISBN (Print-On-Demand):	979-8-3503-3133-2
ISBN (Online):	979-8-3503-3132-5

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

2023 IEEE Secure Development Conference (SecDev)

SecDev 2023

Table of Contents

Message from the Program Chairs ix
Organizing Committee x
Program Committee xi
Steering Committee xiii
Practitioner Session Committee xiv
Keynotes xv

Invited Tutorial

Invited Tutorial: Counteracting Web Application Abuse in Malware 1
Mingxuan Yao (Georgia Institute of Technology), Jonathan Fuller (United States Military Academy), Ranjita Pai Sridhar (Georgia Institute of Technology), Saumya Agarwal (Georgia Institute of Technology), Amit K. Sikder (Georgia Institute of Technology), and Brendan Saltaformaggio (Georgia Institute of Technology)

Tutorial: Crypto-Ransomware: Analysis, Defense, and Criminal Negotiation 3
Wenjia Song (Virginia Tech, USA) and Arianna Schuler Scott (Virginia Tech, USA)

Tutorial: The End of Binary Protocol Parser Vulnerabilities 5
Alexander Senier (AdaCore, Germany)

Aiding Secure Development

Characterizing Static Analysis Alerts for Terraform Manifests: An Experience Report 7
Hanyang Hu (Company A, USA), Yani Bu (Company A, USA), Kristen Wong (Company A, USA), Gaurav Sood (Company A, USA), Karen Smiley (Company A, USA), and Akond Rahman (Auburn University, USA)

Securing Your Crypto-API Usage Through Tool Support — A Usability Study 14
Stefan Krüger (Independent), Michael Reif (Independent), Anna-Katharina Wickert (Technische Universität Darmstadt), Sarah Nadi (University of Alberta), Karim Ali (University of Alberta), Eric Bodden (University of Paderborn), Yasemin Acar (University of Paderborn), Mira Mezini (Technische Universität Darmstadt), and Sascha Fahl (CISPA Helmholtz-Center for Information Security)

Grading on a Curve: How Rust can Facilitate New Contributors While Decreasing Vulnerabilities 26
Justin Tracey (University of Waterloo, Canada) and Ian Goldberg (University of Waterloo, Canada)

Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study 37
Michal Kepkowski (Macquarie University, Australia), Maciej Machulak (n/a), Ian Wood (Macquarie University, Australia), and Dali Kaafar (Macquarie University, Australia)

Misplaced Trust: The Security Flaw in Modern Code Signing Process 49
Pranshu Bajpai (Motorola Solutions) and Raghudeep Kannavara (Meta Platforms Inc)

11 things about Securing Microservice 51
Yuvaraj Madheswaran (General Motors Financial Company, USA)

Defenses

Friend or Foe Inside? Exploring In-Process Isolation to Maintain Memory Safety for Unsafe Rust 54
Merve Gülmez (Ericsson Security Research, Sweden; imec-DistriNet, KU Leuven, Belgium), Thomas Nyman (Ericsson Product Security, Sweden), Christoph Baumann (Ericsson Product Security, Sweden), and Jan Tobias Mühlberg (imec-DistriNet, KU Leuven; Université Libre de Bruxelles, Belgium)

Assessing the Impact of Efficiently Protecting Ten Million Stack Objects from Memory Errors Comprehensively 67
Kaiming Huang (Penn State University), Jack Sampson (Penn State University), and Trent Jaeger (Penn State University)

BLADE: Towards Scalable Source Code Debloating 75
Muaz Ali (University of Arizona), Rumaisa Habib (LUMS), Ashish Gehani (SRI International), Sazzadur Rahaman (University of Arizona), and Zartash Uzmi (LUMS)

Evaluating Container Debloaters 88
Muhammad Hassan (Lahore University of Management Sciences), Talha Tahir (Lahore University of Management Sciences), Muhammad Farrukh (Lahore University of Management Sciences), Abdullah Naveed (Lahore University of Management Sciences), Anas Naeem (Lahore University of Management Sciences), Fahad Shaon (Google), Fareed Zaffar (Lahore University of Management Sciences), Ashish Gehani (SRI International), and Sazzadur Rahaman (University of Arizona)

Attack and Vulnerability Detection

Model-Agnostic Federated Learning for Privacy-Preserving Systems 99
Hussain M. J. Almohri (Kuwait University, Kuwait) and Layne T. Watson (Virginia Polytechnic Institute & State University, USA)

Fortifying IoT Devices: AI-Driven Intrusion Detection via Memory-Encoded Audio Signals 106
Ramyapandian Vijayakanthan (Towson University), Karley M Waguespack (Louisiana State University), Irfan Ahmed (Virginia Commonwealth University), and Aisha Ali-Gombe (Louisiana State University)

Parser Weakness Enumeration: Definition and Preliminary Assessment 118
Denley Lam (FAST Labs, BAE Systems, USA), Letitia Li (FAST Labs, BAE Systems, USA), and Anthony Gabrielson (FAST Labs, BAE Systems, USA)

Curbing the Vulnerable Parser: Graded Modal Guardrails for Secure Input Handling 126
Eric Bond (Two Six Technologies, USA) and Matthew Heimerdinger (Two Six Technologies, USA)

An In-Depth Analysis of Android's Java Class Library: Its Evolution and Security Impact 133
Timothée Riom (Umeå University, Sweden) and Alexandre Bartel (Umeå University, Sweden)

A Randomization-Based, Zero-Trust Cyberattack Detection Method for Hierarchical Systems 145
Sinnott Murphy (National Renewable Energy Laboratory, USA), Richard Macwan (National Renewable Energy Laboratory, USA), Vivek Kumar Singh (National Renewable Energy Laboratory, USA), and Chin-Yao Chang (National Renewable Energy Laboratory, USA)

Security Analysis and Design

A Lot Less Likely Than I Thought: Introducing Evidence-Based Security Risk Assessment for Healthcare Software 156
Charles Weir (Lancaster University, UK), Anna Dyson (Lancaster University, UK), and Daniel Prince (Lancaster University, UK)

Triaging Android Systems Using Bayesian Attack Graphs 171
Yu-Tsung Lee (Penn State University, USA), Rahul George (Penn State University, USA), Haining Chen (Google, USA), Kevin Chan (Army Research Lab, USA), and Trent Jaeger (Penn State University, USA)

PRICAR: Privacy Framework for Vehicular Data Sharing with Third Parties 184
Mert D. Pesé (Clemson University), Jay W. Schauer (University of Michigan), Murali Mohan (University of Michigan), Cassandra Joseph (University of Michigan), Kang G. Shin (University of Michigan), and John Moore (Ford Motor Company)

Security and Privacy Threat Analysis for Solid 196
Omid Mirzamohammadi (COSIC, KU Leuven, Belgium), Kristof Jannes (imec-DistriNet, KU Leuven, Belgium), Laurens Sion (imec-DistriNet, KU Leuven, Belgium), Dimitri Van Landuyt (imec-DistriNet, KU Leuven, Belgium), Aysajan Abidin (COSIC, KU Leuven, Belgium), and Dave Singelée (COSIC, KU Leuven, Belgium)

Bridging the Bubbles: Connecting Academia and Industry in Cybersecurity Research 207
Rasha Kashef (Toronto Metropolitan University, Rogers Cybersecure Catalyst, Canada), Monika Freunek (Lighthouse Science Consulting and Technologies Inc., Rogers Cybersecure Catalyst, Canada), Jeff Schwartzentruber (eSentire Inc., Rogers Cybersecure Catalyst, Canada), Reza Samavi (Toronto Metropolitan University, Rogers Cybersecure Catalyst, Canada), Burcu Bulgurcu (Toronto Metropolitan University, Rogers Cybersecure Catalyst, Canada), AJ Khan (Vehiqilla Inc., Rogers Cybersecure Catalyst, Canada), and Marcus Santos (Toronto Metropolitan University, Rogers Cybersecure Catalyst, Canada)

Adaptive Security: Certificate and Key Rotation for Firmware Integrity 214
Sunil Joshi (Xylem), Kenneth Crowther (Xylem), and Jarvis Robinson (Xylem)

Author Index **217**