

2025 IEEE Secure Development Conference (SecDev 2025)

**Indianapolis, Indiana, USA
14-16 October 2025**



**IEEE Catalog Number: CFP25H06-POD
ISBN: 979-8-3315-9596-8**

**Copyright © 2025 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:	CFP25H06-POD
ISBN (Print-On-Demand):	979-8-3315-9596-8
ISBN (Online):	979-8-3315-9595-1

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

2025 IEEE Secure Development Conference (SecDev) SecDev 2025

Table of Contents

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

2025 IEEE Secure Development Conference

Invited Tutorial: Macaron – A Comprehensive Framework for Securing and Analyzing the Software Supply Chain	1
<i>Behnaz Hassanshahi (Oracle Labs, Australia) and Trong Nhan Mai (Oracle Labs, Australia)</i>	
Tutorial: Understanding Cyber Forensic Data Generation	3
<i>Michael Reeves (Sandia National Laboratories), Tyler Morris (Sandia National Laboratories), and Clint Baxley (ECS Tech)</i>	

Privacy Hardening Techniques

A First Look at Privacy Compliance of Zoom Apps	5
<i>Andrew York (Clemson University, USA), Mohammed Aldeen (Clemson University, USA), Jingwen Yan (Clemson University, USA), Pranav Silimkhan (Viasat Inc., USA), Song Liao (Texas Tech University, USA), Mert D. Pesé (Clemson University, USA), and Long Cheng (Clemson University, USA)</i>	
Catamaran: User Privacy Violation Detection in Mobile Logging	16
<i>Chenxi Hou (New Jersey Institute of Technology, USA), Chun Jie Chong (New Jersey Institute of Technology, USA), Zhihao Yao (New Jersey Institute of Technology, USA), and Hui Peng (Google Inc., USA)</i>	
Comparison of Fully Homomorphic Encryption and Garbled Circuit Techniques in Privacy-Preserving Machine Learning Inference	29
<i>Kalyan Cheerla (University of North Texas), Lotfi Ben Othmane (University of North Texas), and Kirill Morozov (University of North Texas)</i>	

Privacy-Preserving Medical Risk Assessment Using Homomorphic Encryption	37
<i>Raushan Kumar Pandit (University of North Texas, USA), Kirill Morozov (University of North Texas, USA), and Cihan Tunc (University of North Texas, USA)</i>	

Aiding Secure Development

Catching Common Vulnerabilities with Code Language Models	45
<i>Syafiq Al Atiiq (Lund University, Sweden), Christian Gehrman (Lund University, Sweden), Karim Khalil (Lund University, Sweden), and Kevin Dahlén (Lund University, Sweden)</i>	
SoK: Understanding CI/CD Security: A Comprehensive Review of Architecture, Attacks, and Defenses	58
<i>Ryan Zmuda (Riverside Research, USA), Russell Graves (Riverside Research, USA), Michael Shepherd (Riverside Research, USA), and Scott Brookes (Riverside Research, USA)</i>	
PathFix: Automated Program Repair with Expected Path	69
<i>Xu He (Geroge Mason University, USA), Shu Wang (Palo Alto Networks, USA), and Kun Sun (Geroge Mason University, USA)</i>	
Secure Development of a Hooking-Based Deception Framework Against Keylogging Techniques ...	82
<i>Md Sajidul Islam Sajid (Towson University, USA), Shihab Ahmed (Towson University, USA), and Ryan Sosnoski (Towson University, USA)</i>	
Secure and Policy-Aware Serverless Pipelines for Automated Data Governance on Google Cloud....	92
<i>WY Chen (Independent Researcher, USA)</i>	

Security Analysis and Design

User and Entity Behavior Analytics (UEBA) Enhanced Security Anomaly Detection in Enterprise DevSecOps Platforms	94
<i>Adam Jordan (Texas Tech University, USA ; Shell Information Technology International Inc., USA) and Yong Chen (Texas Tech University, USA)</i>	
Behind the Curtain: A Server-Side View of Web Session Security	105
<i>Simone Bozzolan (Università Ca' Foscari Venezia, Italy), Stefano Calzavara (Università Ca' Foscari Venezia, Italy), Florian Hantke (CISPA Helmholtz Center for Information Security, Germany), and Ben Stock (CISPA Helmholtz Center for Information Security, Germany)</i>	
Time for Actions: A Longitudinal Study of the GitHub Actions Marketplace	118
<i>Narong Chaiwut (Stony Brook University, USA) and Nick Nikiforakis (Stony Brook University, USA)</i>	
SoK: A Practical Guideline and Taxonomy to LLVM's Control Flow Integrity	129
<i>Sabine Houy (Umeå University), Bruno Kreyssig (Umeå University), Timothée Riom (Umeå University), Alexandre Bartel (Umeå University), and Patrick McDaniel (University of Wisconsin - Madison)</i>	

On the Readiness of Enterprise-Scale Log Analysis Solutions Against Advanced Persistent Threats	142
<i>Tanmoy Sarkar Pias (Virginia Tech, United States ; Contributed equally), Wenjia Song (Virginia Tech, United States ; Contributed equally), Tahmina Sultana Priya (Virginia Tech, United States), Sahil Dudani (Virginia Tech, United States), Randy Marchany (Virginia Tech, United States), Brad Tilley (Virginia Tech, United States), Lingxiang Wang (Independent Researcher, United States), and Danfeng Daphne Yao (Virginia Tech, United States)</i>	

Attack and Vulnerability Analysis

Navigating the Patchwork: Investigating the Availability & Consistency of Security Advisories	145
<i>Ronald E. Thompson (Tufts University, USA), Luke Boshar (Tufts University, USA), Eugene Y. Vasserman (Kansas State University, USA), and Daniel Votipka (Tufts University, USA)</i>	
Obfusc8: LLM-Augmented PowerShell Obfuscation	156
<i>Kwangyun Keum (Samsung Research America, America), Dheeraj Kumar (Samsung Research America, America), Bogdan Barchuk (Samsung Research America, America), Sai Chand Boyapati (Samsung Research America, America), Rohit Deopura (Samsung Research America, America), and Amir Rahmati (Stony Brook University)</i>	
Exploiting Intent-Flow State Vulnerabilities in Intent-Based Networking	169
<i>Angela Yan (Purdue University), Jiwon Kim (Purdue University), Benjamin E Ujcich (Georgetown University), and Dave Jing Tian (Purdue University)</i>	

Hardware Supported Security

CAROT: A Secure RISC-V ECU with Trusted Execution and Moving Target Defense	176
<i>Ahmer Raza (Clemson University, USA) and Zhenkai Zhang (Clemson University, USA)</i>	
Understanding Minimal-Time Attacks on Reinforcement Learning Agents	186
<i>Veena Krish (Stony Brook University, USA) and Amir Rahmati (Stony Brook University, USA)</i>	
Hardware Security Benchmarks for Open-Source SystemVerilog Designs	196
<i>Jayden Rogers (North Carolina A&T), Niyaz Shakeel (University of North Carolina at Chapel Hill), Xiao Tan (University of North Carolina at Chapel Hill), Samantha Espinosa (University of North Carolina at Chapel Hill), Divya Mankani (University of North Carolina at Chapel Hill), Cade Chabra (University of North Carolina at Chapel Hill), Kaki Ryan (University of North Carolina at Chapel Hill), and Cynthia Sturton (University of North Carolina at Chapel Hill)</i>	

PV-Bit: Private Verification of FPGA Bitstreams Via Bitstream Equivalence Checking 204
Ali Asgar Sohangpurwala (Graf Research Corporation, USA), Daniel Gibson (Graf Research Corporation, USA), Scott Harper (Graf Research Corporation, USA), Jonathan Graf (Graf Research Corporation, USA), and Timothy Dunham (Graf Research Corporation, USA)

Author Index 215