

2022 IEEE Secure Development Conference (SecDev 2022)

**Atlanta, Georgia, USA
18 – 20 October 2022**



**IEEE Catalog Number: CFP22H06-POD
ISBN: 978-1-6654-7183-1**

**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:	CFP22H06-POD
ISBN (Print-On-Demand):	978-1-6654-7183-1
ISBN (Online):	978-1-6654-7182-4

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 Secure Development Conference (SecDev) **SecDev 2022**

Table of Contents

Message from the General Chairs	viii
Message from the Program Chairs	x
Organizing Committee	xi
Program Committee	xii
Steering Committee	xiii
Reviewers	xiv
Sponsors	xv

Tutorials

Tutorial: LLVM for Security Practitioners	1
<i>John Criswell (University of Rochester), Ethan Johnson (University of Rochester), and Colin Pronovost (University of Utah)</i>	
Tutorial: Analyzing, Exploiting, and Patching Smart Contracts in Ethereum	3
<i>Jens-Rene Giesen (University of Duisburg-Essen, Germany), Sebastien Andreina (NEC Laboratories Europe, Germany), Michael Rodler (University of Duisburg-Essen, Germany), Ghassan O. Karame (Ruhr University of Bochum, Germany; NEC Laboratories Europe, Germany), and Lucas Davi (University of Duisburg-Essen, Germany)</i>	
Tutorial: Threat Modeling of Cloud-Based Solutions	5
<i>Lotfi Ben Othmane (University of North Texas, Denton, USA), Heinrich Gantenbein (Microsoft Industry Solutions, St. Paul, USA), Hasan Yasar (Carnegie Mellon University, Pittsburgh, USA), Simone Curzi (Microsoft Industry Solutions, Perugia, Italy), Altaz Valani (Security Compass, Toronto, Canada), Arun Prabhakar (Boston Consulting Group, Toronto, Canada), and Robert Cuddy (HCL Technologies, Aliso Viejo, USA)</i>	

Research Session #1: Security Evaluation

How far are German Companies in Improving Security Through Static Program Analysis Tools?	7
<i>Goran Piskachev (Fraunhofer IEM), Stefan Dziwok (Fraunhofer IEM), Thorsten Koch (Fraunhofer IEM), Sven Merschjohann (Fraunhofer IEM), and Eric Bodden (Paderborn University and Fraunhofer IEM)</i>	

A Comparative Study of Log4Shell Test Tools	16
<i>Douglas Everson (Clemson University, USA), Ashish Bastola (Clemson University, USA), Rajat Mittal (Clemson University, USA), Siddheshwar Munde (Clemson University, USA), and Long Cheng (Clemson University, USA)</i>	
Evaluating Text Augmentation for Boosting the Automatic Mapping of Vulnerability Information to Adversary Techniques	23
<i>Emmanouil Gionanidis (DataWise Data Engineering LLC, USA), Petros Karvelis (University of Ioannina, Greece), George Georgoulas (DataWise Data Engineering LLC, USA), Konstantinos Stamos (DataWise Data Engineering LLC, USA), and Purvi Garg (Hive Pro Inc., USA)</i>	

Research Session #2: Hardware Supported Security

Towards Cryptographically-Authenticated in-Memory Data Structures	30
<i>Setareh Ghorshi (University of Waterloo, Canada), Lachlan J. Gunn (Aalto University, Finland), Hans Liljestrand (University of Waterloo, Canada), and N. Asokan (University of Waterloo, Canada)</i>	
Salsa: SGX Attestation for Live Streaming Applications	45
<i>Tobias Cloosters (University of Duisburg-Essen, Germany), Sebastian Surminski (University of Duisburg-Essen, Germany), Gerrit Sangel (University of Duisburg-Essen, Germany), and Lucas Davi (University of Duisburg-Essen, Germany)</i>	
Position Paper: Towards a Hybrid Approach to Protect Against Memory Safety Vulnerabilities.....	52
<i>Kaled Alshmrany (The University of Manchester, UK), Ahmed Bhayat (The University of Manchester, UK), Franz Brauße (The University of Manchester, UK), Lucas Cordeiro (The University of Manchester, UK), Konstantin Korovin (The University of Manchester, UK), Tom Melham (The University of Oxford, UK), Mustafa A. Mustafa (The University of Manchester, UK), Pierre Olivier (The University of Manchester, UK), Giles Reger (The University of Manchester, UK), and Fedor Shmarov (The University of Manchester, UK)</i>	

Practitioner Session #1

From Lemons to Peaches: Improving Security ROI Through Security Chaos Engineering	59
<i>Kelly Shortridge (Product Technology, Fastly, USA)</i>	
Industrial Strength Static Detection for Cryptographic API Misuses	61
<i>Ya Xiao (Virginia Tech, USA), Yang Zhao (Oracle Labs, Australia), Nicholas Allen (Oracle Labs, Australia), Nathan Keynes (Oracle Labs, Australia), Danfeng Yao (Virginia Tech, USA), and Cristina Cifuentes (Oracle Labs, Australia)</i>	
Framework to Assess Policy Driven Security Misconfiguration Risks in Cloud Native Application	63
<i>Kanchanjot Kaur Phokela (Accenture Labs, India), Kapil Singi (Accenture Labs, India), Kuntal Dey (Accenture Labs, India), Vikrant Kaulgud (Accenture Labs, India), and Adam P. Burden (Accenture, Singapore)</i>	

Secure Development Workflows in CI/CD Pipelines	65
<i>Pranshu Bajpai (Motorola Solutions Inc.) and Adam Lewis (Motorola Solutions Inc.)</i>	

A Hierarchical Database of One Million Websites	67
<i>Jack B. Harrison (Virginia Tech National Security Institute), Joseph R. Harrison (Virginia Tech National Security Institute), Madison G. Boswell (Virginia Tech National Security Institute), and Alan J. Michaels (Virginia Tech National Security Institute)</i>	

Research Session #3: Software Security

What are the Practices for Secret Management in Software Artifacts?	69
<i>Setu Kumar Basak (North Carolina State University, USA), Lorenzo Neil (North Carolina State University, USA), Bradley Reaves (North Carolina State University, USA), and Laurie Williams (North Carolina State University, USA)</i>	

How Do Developers Follow Security-Relevant Best Practices When using NPM Packages?	77
<i>Md Mahir Asef Kabir (Virginia Tech, USA), Ying Wang (Northeastern University, China), Danfeng Yao (Virginia Tech, USA), and Na Meng (Virginia Tech, USA)</i>	

Uncovering Product Vulnerabilities with Threat Knowledge Graphs	84
<i>Zhenpeng Shi (Boston University, USA), Nikolay Matyunin (Honda Research Institute Europe GmbH, Germany), Kalman Graffi (Honda Research Institute Europe GmbH, Germany), and David Starobinski (Boston University, USA)</i>	

Design and User Study of a Constraint-Based Framework for Business Logic Flaw Discovery	91
<i>Carmen Cheh (Advanced Digital Sciences Center, Singapore and Singapore University of Technology and Design, Singapore), Nicholas Tay (Singapore University of Technology and Design, Singapore), and Binbin Chen (Singapore University of Technology and Design, Singapore)</i>	

Author Index	101
---------------------------	------------