

# **2019 IEEE Cybersecurity Development (SecDev 2019)**

**McLean, Virginia, USA  
25 – 27 September 2019**



**IEEE Catalog Number: CFP19H06-POD  
ISBN: 978-1-5386-7290-7**

**Copyright © 2019 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:	CFP19H06-POD
ISBN (Print-On-Demand):	978-1-5386-7290-7
ISBN (Online):	978-1-5386-7289-1

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2019 IEEE Secure Development (SecDev) SecDev 2019

## Table of Contents

Message from the General Chairs	viii
Organizing Committee	ix
Steering Committee	x
Practitioner Session Committee	xi
Poster and Tool Demo Program Committee	xii
Research and Tutorial Program Committee	xiii
Sponsors	xiv

## Tutorials

Tutorial: A Practical Introduction to Formal Development and Verification of High-Assurance Software with SPARK	1
<i>Benjamin M. Brosgol (AdaCore), Claire Dross (AdaCore), and Yannick Moy (AdaCore)</i>	
Tutorial: Deploying Secure Multi-Party Computation on the Web Using JIFF	3
<i>Kinan Dak Albab (Boston University), Rawane Issa (Boston University), Andrei Lapets (Boston University), Peter Flockhart (Boston University), Lucy Qin (Boston University), and Ira Globus-Harris (Boston University)</i>	

## Cryptography and Understanding Insecure Code

Start Your ENGINES: Dynamically Loadable Contemporary Crypto	4
<i>Nicola Tuveri (Tampere University) and Billy Bob Brumley (Tampere University)</i>	
On the Universally Composable Security of OpenStack	20
<i>Kyle Hogan (Massachusetts Institute of Technology), Hoda Maleki (Augusta University), Reza Rahaeimehr (University of Connecticut), Ran Canetti (Boston University), Marten van Dijk (University of Connecticut), Jason Hennessey (Boston University, NetApp), Mayank Varia (Boston University), and Haibin Zhang (University of Maryland)</i>	
A Qualitative Investigation of Insecure Code Propagation from Online Forums	34
<i>Wei Bai (University of Maryland), Omer Akgul (University of Maryland), and Michelle L. Mazurek (University of Maryland)</i>	
CryptoAPI-Bench: A Comprehensive Benchmark on Java Cryptographic API Misuses	49
<i>Sharmin Afrose (Virginia Tech), Sazzadur Rahaman (Virginia Tech), and Danfeng (Daphne) Yao (Virginia Tech)</i>	

## Security in Lower-Levels of Abstraction

- Detecting Callback Related Deep Vulnerabilities in Linux Device Drivers .62.....  
*Tuba Yavuz (University of Florida)*
- Downright: A Framework and Toolchain for Privilege Handling .76.....  
*Remo Schweizer (Zurich University of Applied Sciences) and Stephan Neuhaus (Zurich University of Applied Sciences)*
- System-Level Framework for Logic Obfuscation with Quantified Metrics for Evaluation .89.....  
*Vivek V. Menon (University of Southern California), Gaurav Kolhe (University of Southern California), Andrew Schmidt (University of Southern California), Joshua Monson (University of Southern California), Matthew French (University of Southern California), Yinghua Hu (University of Southern California), Peter A. Beerel (University of Southern California), and Pierluigi Nuzzo (University of Southern California)*

## Data and Information

- Polymorphic Relaxed Noninterference .101.....  
*Raimil Cruz (University of Chile) and Eric Tanter (University of Chile)*
- Exploitation Techniques and Defenses for Data-Oriented Attacks .114.....  
*Long Cheng (Clemson University, USA), Hans Liljestrand (Aalto University, Finland), Md Salman Ahmed (Virginia Tech, USA), Thomas Nyman (Aalto University, Finland), Trent Jaeger (Pennsylvania State University, USA), N. Asokan (Aalto University, Finland), and Danfeng (Daphne) Yao (Virginia Tech, USA)*
- Role-Based Ecosystem for the Design, Development, and Deployment of Secure Multi-Party Data Analytics Applications .129.....  
*Andrei Lapets (Boston University), Kinan Dak Albab (Boston University), Rawane Issa (Boston University), Lucy Qin (Boston University), Mayank Varia (Boston University), Azer Bestavros (Boston University), and Frederick Jansen (Boston University)*

## Practitioner Papers

- Effective Static Analysis Enforcement in Complex Cloud Native Dockerized Systems .141.....  
*Abhishek Pathak (Cisco), Kaarthik Sivakumar (Cisco), Jin Sheng (Cisco), Anlu Yan (Cisco), and Mazhar Haque (Cisco)*
- Using Rules Engine in the Automation of System Security Review .142.....  
*Abdulrahman A. Alnaim (Saudi Aramco)*
- OpenOSC: Open Source Object Size Checking Library With Built-in Metrics .143.....  
*Yongkui Han (Cisco Systems), Pankil Shah (Cisco Systems), Van Nguyen (Cisco Systems), Ling Ma (Cisco Systems), and Richard Livingston (Cisco Systems)*

With Great Abstraction Comes Great Responsibility: Sealing the Microservices Attack Surface .144.....  
*Chien-An Chen (Palo Alto Networks)*

Multi-Cluster Visualization and Live Reporting of Static Analysis Security Testing (SAST) Warnings .145.....  
*Abhishek Pathak (Cisco Systems), Kaarthik Sivakumar (Cisco Systems),  
Mazhar Haque (Cisco Systems), and Prasanna Ganesan (Cisco Systems)*

Development Cycle Estimation Modeling .146.....  
*Samuel Denard (Texas Tech University), Susan Mengel (Texas Tech  
University), Atila Ertas (Texas Tech University), and Stephen  
Ekwaro-Osire (Texas Tech University)*

## **Networking**

Self-Authenticating Traditional Domain Names .147.....  
*Paul Syverson (U.S. Naval Research Laboratory) and Matthew Traudt  
(U.S. Naval Research Laboratory)*

Compositional Testing of Internet Protocols .161.....  
*Kenneth L. McMillan (Microsoft Research) and Lenore D. Zuck  
(University of Illinois at Chicago)*

**Author Index 175.** .....