2018 IEEE Cybersecurity Development Conference (SecDev 2018)

Cambridge, Massachusetts, USA
30 September – 2 October 2018

IEEE Catalog Number: CFP18H06-POD
ISBN: 978-1-5386-7663-9

****** 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:	CFP18H06-POD
ISBN (Print-On-Demand):	978-1-5386-7663-9
ISBN (Online):	978-1-5386-7662-2

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

2018 IEEE Secure Development Conference

SecDev 2018

Table of Contents

Message from the SecDev 2018 General Chair ix

Message from the SecDev 2018 Program Chairs x

2018 SecDev Program Committee xi

SecDev 2018 Keynote Abstracts xiii

Paper Session 1: Best Practices of Security

BP: Formal Proofs, the Fine Print and Side Effects 1
Toby Murray (University of Melbourne) and Paul van Oorschot (Carleton University)

BP: DECREE: A Platform for Repeatable and Reproducible Security Experiments 11
Lok Yan (Air Force Research Laboratory), Benjamin Price (MIT Lincoln Laboratory), Michael Zhivich (MIT Lincoln Laboratory), Brian Caswell (Lunge Technologies), Christopher Eagle (Naval Postgraduate School), Michael Frantzen (Kudu Dynamics), Holt Sorenson (Google Inc.), Michael Thompson (Naval Postgraduate School), Timothy Vidas (Secureworks), Jason Wright (Thought Networks), Vernon Rivet (MIT Lincoln Laboratory), Samuel Colt VanWinkle (MIT Lincoln Laboratory), and Clark Wood (MIT Lincoln Laboratory)

BP: Security Concerns and Best Practices for Automation of Software Deployment Processes: An Industrial Case Study 21
Vaishnavi Mohan (Deloitte Analytics Institute), Lotfi ben Othmane (Iowa State University), and Andre Kres (IBM)

Paper Session 2: Data Access Security

Tyche: A Risk-Based Permission Model for Smart Homes 29
Amir Rahmati (Samsung Research America-Stony Brook University), Earlence Fernandes (University of Washington), Kevin Eykholt (University of Michigan), and Atul Prakash (University of Michigan)

Detecting Leaks of Sensitive Data Due to Stale Reads 37
Will Snavely (Software Engineering Institute), William Klieber (Software Engineering Institute), Ryan Steele (Software Engineering Institute), David Svoboda (Software Engineering Institute), and Andrew Kotov (Software Engineering Institute)

Transforming Code to Drop Dead Privileges 45
Xiaoyu Hu (BitFusion.io), Jie Zhou (University of Rochester), Spyridoula Gravani (University of Rochester), and John Criswell (University of Rochester)

Paper Session 3: Secure Coding and Analysis

Checked C: Making C Safe by Extension 53
Archibald Samuel Elliott (University of Washington), Andrew Ruef (University of Maryland), Michael Hicks (University of Maryland), and David Tarditi (Microsoft Research)

SGL: A Domain-Specific Language for Large-Scale Analysis of Open-Source Code 61
Darius Foo (SourceClear, Inc.), Ming Yi Ang (SourceClear, Inc.), Jason Yeo (SourceClear, Inc.), and Asankhaya Sharma (SourceClear, Inc.)

A Lingua Franca for Security by Design 69
Alexander van den Berghe (KU Leuven), Koen Yskout (KU Leuven), Riccardo Scandariato (Chalmers and Göteborg University), and Wouter Joosen (KU Leuven)

Paper Session 4: Software and System Development

BP: Integrating Cyber Vulnerability Assessments Earlier into the Systems Development Lifecycle: A Methodology to Conduct Early-Cycle Cyber Vulnerability Assessments 77
Sonja Glumich (Air Force Research Laboratory), Juanita Riley (Air Force Research Laboratory), Paul Ratazzi (Air Force Research Laboratory), and Amanda Ozanam (Air Force Research Laboratory)

Light-Touch Interventions to Improve Software Development Security 85
Charles Weir (Lancaster University), Lynne Blair (Lancaster University), Ingolf Becker (University College London), Angela Sasse (University College London), and James Noble (Victoria University of Wellington)

Paper Session 5: Vulnerability Assessment

Towards Understanding the Adoption of Anti-Spoofing Protocols in Email Systems 94
Hang Hu (Virginia Tech), Peng Peng (Virginia Tech), and Gang Wang (Virginia Tech)

There's a Hole in the Bottom of the C: On the Effectiveness of Allocation Protection 102
Ronald Gil (MIT CSAIL), Hamed Okhravi (MIT Lincoln Laboratory), and Howard Shrobe (MIT CSAIL)

BP: Profiling Vulnerabilities on the Attack Surface 110
Christopher Theisen (North Carolina State University), Hyunwoo Sohn (North Carolina State University), Dawson Tripp (North Carolina State University), and Laurie Williams (North Carolina State University)

Tutorial Session

Tutorial: Building Secure and Trustworthy Blockchain Applications .120
Chengjun Cai (City University of Hong Kong), Huayi Duan (City University of Hong Kong), and Cong Wang (City University of Hong Kong)

Tutorial: Principles and Practices of Secure Crypto Coding in Java .122
Sazzadur Rahaman (Virginia Tech), Na Meng (Virginia Tech), and Danfeng (Daphne) Yao (Virginia Tech)

Tutorial: Secure Coding Practices, Automated Assessment Tools and the SWAMP .124
Elisa Heymann (University of Wisconsin-Madison) and Barton Miller (University of Wisconsin-Madison)

Tutorial: Secure Your Things: Secure Development of IoT Software with Frama-C .126
Allan Blanchard (Inria), Nikolai Kosmatov (CEA, List), and Frédéric Loulergue (Northern Arizona University)

Tutorial: Continuous Verification of Critical Software .128
Mike Dodds (Galois Inc.), Stephen Magill (Galois Inc.), and Aaron Tomb (Galois Inc.)

Tutorial: DeepState: Bringing Vulnerability Detection Tools into the Development Cycle .130
Peter Goodman (Trail of Bits, Inc.), Gustavo Grieco (Trail of Bits, Inc.), and Alex Groce (Northern Arizona University)

Tutorial: Parry and RIPOSTE: Honing Cybersecurity Skills with Challenge-Based Exercises .132
Fabian Monrose (University of North Carolina at Chapel Hill) and Jan Werner (University of North Carolina at Chapel Hill)

Practitioners' Session 1: Enterprise Threat Modeling

Scalable Static Analysis to Detect Security Vulnerabilities: Challenges and Solutions .134
François Gauthier (Oracle Labs), Nathan Keynes (Oracle Labs), Nicholas Allen (Oracle Labs), Diane Corney (Oracle Labs), and Padmanabhan Krishnan (Oracle Labs)

Applied Threat Driven Security Verification .135
Danny Dhillon (Dell) and Vishal Mishra (Dell)

Rethinking Secure DevOps Threat Modeling: The Need for a Dual Velocity Approach .136
Altaz Valani (Security Compass)

Automating Threat Intelligence for SDL .137
Raghudeep Kannavara (Intel Corporation), Jacob Vangore (Olivet Nazarene University), William Roberts (Olivet Nazarene University), Marcus Lindholm (Intel Corporation), and Priti Shrivastav (Intel Corporation)

Practitioners' Session 2: New Security Needs and Approaches

Reducing Attack Surface via Executable Transformation .138
Sukarno Mertoguno (Office of Naval Research), Ryan Craven (Office of Naval Research), Daniel Koller (Office of Naval Research), and Matthew Mickelson (The MITRE Corporation)

Designing Secure and Resilient Embedded Avionics Systems .139
Jason H. Li (Intelligent Automation Inc.), Douglas Schafer (Air Force Research Laboratories), David Whelihan (MIT Lincoln Laboratory), Stefano Lassini (GE Aviation Systems), Nicholas Evancich (Intelligent Automation Inc.), Kyung Joon Kwak (Intelligent Automation Inc.), Michael Vai (MIT Lincoln Laboratory), and Haley Whitman (MIT Lincoln Laboratory)

Data Integrity: Recovering from Ransomware and Other Destructive Events .140
Tim McBride (National Institute of Standards and Technology), Anne Townsend (The MITRE Corporation), Michael Ekstrom (The MITRE Corporation), Lauren Lusty (The MITRE Corporation), and Julian Sexton (The MITRE Corporation)

Securing Wireless Infusion Pumps .141
Andrea Arbelaez (National Institute of Standards and Technology), Sallie Edwards (The MITRE Corporation), Kevin Littlefield (The MITRE Corporation), Sue Wang (The MITRE Corporation), and Kangmin Zheng (The MITRE Corporation)

Best Practice for Developing Secure and Trusted Enterprise Storage & Computing Products .142
Xuan Tang (Dell)

Experiment: Sizing Exposed Credentials in GitHub Public Repositories for CI/CD .143
Hasan Yasar (Software Engineering Institute , Carnegie Mellon University)

Author Index .145