

# **2016 IEEE Cybersecurity Development (SecDev 2016)**

**Boston, Massachusetts, USA  
3-4 November 2016**



**IEEE Catalog Number: CFP16H06-POD  
ISBN: 978-1-5090-5590-6**

**Copyright © 2016 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:	CFP16H06-POD
ISBN (Print-On-Demand):	978-1-5090-5590-6
ISBN (Online):	978-1-5090-5589-0

**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

# 2016 IEEE Cybersecurity Development

## SecDev 2016

### Table of Contents

Message from the General Chair.....	ix
Message from the Program Chair.....	xi
Message from the Tutorial Chair.....	xii
Committees.....	xiii
Invited Talks.....	xv
Sponsors.....	xviii

---

#### **Towards More Secure Systems**

You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users.....	3
<i>Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek</i>	
Toward Semantic Cryptography APIs.....	9
<i>Soumya Indela, Mukul Kulkarni, Kartik Nayak, and Tudor Dumitras</i>	
Operational Security Log Analytics for Enterprise Breach Detection.....	15
<i>Zhou Li and Alina Oprea</i>	

#### **Exploring Secure Design**

Hints for High-Assurance Cyber-Physical System Design.....	25
<i>Lee Pike</i>	
Design Space Exploration for Security.....	30
<i>Eunsuk Kang</i>	
Static Analysis Alert Audits: Lexicon & Rules.....	37
<i>David Svoboda, Lori Flynn, and Will Snively</i>	
The Seven Turrets of Babel: A Taxonomy of LangSec Errors and How to Expunge Them.....	45
<i>Falcon Momot, Sergey Bratus, Sven M. Hallberg, and Meredith L. Patterson</i>	
Software Security Investment: The Right Amount of a Good Thing.....	53
<i>Chad Heitzenrater and Andrew Simpson</i>	

## Lightning Talks

A Case for Combining Industrial Pragmatics with Formal Methods .....	63
<i>Eric L. McCorkle</i>	
Avoiding Insecure C++ — How to Avoid Common C++ Security Vulnerabilities .....	65
<i>Aaron Ballman and David Svoboda</i>	
Dependency-Based Attacks on Node.js .....	66
<i>Brian Pfretzschner and Lotfi ben Othmane</i>	
Maintaining Authorization Hook Placements Across Program Versions .....	67
<i>Nirupama Talele, Divya Muthukumaran, Frank Capobianco, Trent Jaeger, and Gang Tan</i>	
MOSAIC: A Platform for Monitoring and Security Analytics in Public Clouds .....	69
<i>Alina Oprea, Ata Turk, Cristina Nita-Rotaru, and Orran Krieger</i>	
Secure Coding for Real-Time Embedded Systems: Cert Run-Time Profile for Ada .....	71
<i>Mable Benjamin</i>	
Secure MPC for Analytics as a Web Application .....	73
<i>Andrei Lapets, Nikolaj Volgushev, Azer Bestavros, Frederick Jansen, and Mayank Varia</i>	
Secure Multiparty Computation for Cooperative Cyber Risk Assessment .....	75
<i>Kyle Hogan, Noah Luther, Nabil Shear, Emily Shen, David Stott, Sophia Yakoubov, and Arkady Yerukhimovich</i>	
Towards Building Practical Secure Multi-party Databases .....	77
<i>Yuzhe Tang and Wenqing Zhuang</i>	

## Security Enforcement Techniques

Security Guarantees for the Execution Infrastructure of Software Applications .....	81
<i>Frank Piessens, Dominique Devriese, Jan Tobias Mühlberg, and Raoul Strackx</i>	
Applying the Opacified Computation Model to Enforce Information Flow Policies in IoT Applications .....	88
<i>Amir Rahmati, Earlence Fernandes, and Atul Prakash</i>	
Certified Lightweight Contextual Policies for Android .....	94
<i>Mohamed Nassim Seghir, David Aspinall, and Lenka Marekova</i>	
Enforcing Content Security by Default within Web Browsers .....	101
<i>Christoph Kerschbaumer</i>	
Leveraging Data Provenance to Enhance Cyber Resilience .....	107
<i>Thomas Moyer, Karishma Chadha, Robert Cunningham, Nabil Shear, Warren Smith, Adam Bates, Kevin Butler, Frank Capobianco, Trent Jaeger, and Patrick Cable</i>	

## Secure Defenses

Self-Verifying Execution (Position Paper) .....	117
<i>Matt McCutchen, Daniel Song, Shuo Chen, and Shaz Qadeer</i>	
Code Randomization: Haven't We Solved This Problem Yet? .....	124
<i>Stephen Crane, Andrei Homescu, and Per Larsen</i>	
Automated Code Repair Based on Inferred Specifications .....	130
<i>William Klieber and Will Snively</i>	
Building Robust Distributed Systems and Network Protocols by Using Adversarial Testing and Behavioral Analysis .....	138
<i>Endadul Hoque and Cristina Nita-Rotaru</i>	

## Tutorials on Security of Web Design

Adopting Strict Content Security Policy for XSS Protection .....	149
<i>Lukas Weichselbaum, Michele Spagnuolo, and Artur Janc</i>	
Safe Client/Server Web Development with Haskell .....	150
<i>Mark Mazumder and Timothy Braje</i>	

## Tutorials on Static Analysis Techniques

How to Find and Fix Software Vulnerabilities with Coverity Static Analysis .....	153
<i>Bill Baloglu</i>	
Auditing Code for Security Vulnerabilities with CodeSonar .....	154
<i>David Vitek</i>	

## Tutorials on Dynamic Testing Techniques

Continuous Fuzzing with libFuzzer and AddressSanitizer .....	157
<i>Kosta Serebryany</i>	
Using Dr. Fuzz, Dr. Memory, and Custom Dynamic Tools for Secure Development .....	158
<i>Derek Bruening and Qin Zhao</i>	

## Tutorials on Security Engineering

Beyond errno: Error Handling in "C" .....	161
<i>David Svoboda</i>	
Codiscope SecureAssist™ — The Developer's Security Assistant .....	162
<i>Nivedita Murthy</i>	

## **Tutorials on Secure Development Operations**

Software Vulnerabilities, Defects, and Design Flaws: A Technical Debt Perspective .....	165
<i>Robert L. Nord and Ipek Ozkaya</i>	
Secure DevOps Process and Implementation .....	166
<i>Hasan Yasar and Kiriakos Kontostathis</i>	
<b>Author Index</b> .....	167