

2021 IEEE Secure Development Conference (SecDev 2021)

**Virtual Conference
18 – 20 October 2021**



IEEE Catalog Number: CFP21H06-POD
ISBN: 978-1-6654-3171-2

**Copyright © 2021 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:	CFP21H06-POD
ISBN (Print-On-Demand):	978-1-6654-3171-2
ISBN (Online):	978-1-6654-3170-5

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

2021 IEEE Secure Development Conference (SecDev) **SecDev 2021**

Table of Contents

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

Tutorial Track A

Tutorial: The Correctness-by-Construction Approach to Programming Using CoC	1
<i>Ina Schaefer (TU Braunschweig, Germany), Tobias Runge (TU Braunschweig, Germany), Loek Cleophas (TU Eindhoven, The Netherlands; Stellenbosch University, South Africa), and Bruce W. Watson (Stellenbosch University, South Africa)</i>	
Tutorial: Investigating Advanced Exploits for System Security Assurance	3
<i>Salman Ahmed (Virginia Tech, USA), Long Cheng (Clemson University, USA), Hans Liljestrand (University of Waterloo, Canada), N. Asokan (University of Waterloo, Canada), and Danfeng (Daphne) Yao (Virginia Tech, USA)</i>	
Tutorial: A Lightweight Web Application for Software Vulnerability Demonstration	5
<i>David Lee (Augusta University, USA), Brandon Steed (Augusta University, USA), Yi Liu (University of Massachusetts Dartmouth, USA), and Onyeka Ezenwoye (Augusta University, USA)</i>	
Hands-on Tutorial: How Exploitable is Insecure C Code?	7
<i>David Svoboda (Carnegie Mellon University, USA)</i>	

Tutorial Track B

Tutorial: LLVM for Security Practitioners	9
<i>John Criswell (University of Rochester), Ethan Johnson (University of Rochester), and Colin Pronovost (University of Rochester)</i>	
Tutorial: Sandboxing (Unsafe) C Code with RLBox	11
<i>Shravan Narayan (UC San Diego), Craig Disselkoen (UC San Diego), and Deian Stefan (UC San Diego)</i>	

Tutorial: Making C Programs Safer with Checked C	13
<i>Jie Zhou (University of Rochester), Michael Hicks (University of Maryland and Correct Computation, Inc.), Yudi Yang (University of Rochester), and John Criswell (University of Rochester)</i>	

Session I: Security/Threat Analysis

Analyzing OpenAPI Specifications for Security Design Issues	15
<i>Carmen Cheh (Singapore University of Technology and Design, Singapore) and Binbin Chen (Singapore University of Technology and Design, Singapore)</i>	
Compressing Network Attack Surfaces for Practical Security Analysis	23
<i>Douglas Everson (Clemson University, USA) and Long Cheng (Clemson University, USA)</i>	
Automated Threat Analysis and Management in a Continuous Integration Pipeline	30
<i>Laurens Sion (KU Leuven, Belgium), Dimitri Van Landuyt (KU Leuven, Belgium), Koen Yskout (KU Leuven, Belgium), Stef Verreydt (KU Leuven, Belgium), and Wouter Joosen (KU Leuven, Belgium)</i>	

Session II: Secure Development

Towards Improving Container Security by Preventing Runtime Escapes	38
<i>Michael Reeves (Sandia National Laboratories), Dave (Jing) Tian (Purdue University), Antonio Bianchi (Purdue University), and Z. Berkay Celik (Purdue University)</i>	
Developers Are Neither Enemies Nor Users: They Are Collaborators	47
<i>Partha Das Chowdhury (University of Bristol, UK), Joseph Hallett (University of Bristol, UK), Nikhil Patnaik (University of Bristol, UK), Mohammad Tahaai (University of Bristol, UK), and Awais Rashid (University of Bristol, UK)</i>	
Shhh!: 12 Practices for Secret Management in Infrastructure as Code	56
<i>Akond Rahman (Tennessee Tech University, USA), Farhat Lamia Barsha (Tennessee Tech University, USA), and Patrick Morrison (IBM, USA)</i>	

Session III: Security Focused Designs

Android Remote Unlocking Service Using Synthetic Password: A Hardware Security-Preserving Approach	63
<i>Sungmin Lee (Seoul National University, South Korea), Yoonkyo Jung (Seoul National University, South Korea), Jaehyun Lee (Seoul National University, South Korea), Byoungyoung Lee (Seoul National University, South Korea), and Ted "Taekyoung" Kwon (Seoul National University, South Korea)</i>	
Enclave-Based Secure Programming with JE	71
<i>Aditya Oak (TU Darmstadt), Amir M. Ahmadian (KTH Royal Institute of Technology), Musard Balliu (KTH Royal Institute of Technology), and Guido Salvaneschi (University of St.Gallen)</i>	

Towards Zero Trust: An Experience Report	79
<i>Jason Lowdermilk (Chip Scan, Inc.) and Simha Sethumadhavan (Chip Scan, Inc.)</i>	

Session IV: Formal Verification

Layered Formal Verification of a TCP Stack	86
<i>Guillaume Cluzel (AdaCore & ENS de Lyon), Kyriakos Georgiou (AdaCore & University of Bristol), Yannick Moy (AdaCore), and Clément Zeller (Oryx Embedded)</i>	

Vivienne: Relational Verification of Cryptographic Implementations in WebAssembly	94
<i>Rodothea Myrsini Tsoupidi (KTH Royal Institute of Technology, Sweden), Musard Balliu (KTH Royal Institute of Technology, Sweden), and Benoit Baudry (KTH Royal Institute of Technology, Sweden)</i>	

Author Index	103
---------------------------	------------