

Proceedings

**BAR 2018**

**Workshop on  
Binary Analysis Research**

February 18, 2018  
San Diego, California

*Published by the*





---

**Internet Society**  
**1775 Wiehle Avenue**  
**Suite 201**  
**Reston, VA 20190-5108**

---

Copyright © 2018 by the Internet Society.  
All rights reserved.

This volume is published as a collective work. The Internet Society owns the copyright for this publication and the copyrights to the individual papers are retained by their respective author[s].

Address your correspondence to: NDSS Program Manager, Internet Society, 1775 Wiehle Avenue, Suite 201, Reston, Virginia 20190-5108, U.S.A., tel. +1 703 439 2120, fax +1 703 326 9881, [ndss@isoc.org](mailto:ndss@isoc.org).

*The papers included here comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interest of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors or the Internet Society.*

ISBN Number (Digital Format) 1-891562-50-9

*Additional copies may be ordered from:*



**Internet Society**  
1775 Wiehle Avenue  
Suite 201  
Reston, VA 20190-5108  
tel +1 703.439.2120  
fax +1 703.326.9881  
<http://www.internetsociety.org>

## **Table of Contents**

### **Software Testing**

INSTRIM: Lightweight Instrumentation for Coverage-guided Fuzzing

*Chin-Chia Hsu, Che-Yu Wu, Hsu-Chun Hsiao (National Taiwan University) and Shih-Kun Huang (National Chiao Tung University)*

Avatar<sup>2</sup>: A Multi-Target Orchestration Platform

*Marius Muench, Dario Nisi, Aurélien Francillon and Davide Balzarotti (Eurecom)*

DeepState: Symbolic Unit Testing for C and C++

*Peter Goodman (Trail of Bits) and Alex Groce (Northern Arizona University)*

Saluki: Finding Taint-style Vulnerabilities with Static Property Checking

*Ivan Gotovchits, Rijnard Van Tonder and David Brumley (Carnegie Mellon University)*

### **Miscellaneous**

The Effect of Instruction Padding on SFI Overhead

*Navid Emamdoost and Stephen McCamant (University of Minnesota)*

Predictable Packet Processing with PathMiner

*John Sonchack and Jonathan Smith (University of Pennsylvania)*

### **Reverse Engineering**

Evolving Exact Decompilation

*Eric Schulte, Jason Rucht, Matt Noonan, David Ciarletta and Alexey Loginov (GramaTech, Inc)*

Towards Generic Deobfuscation of Windows API Calls

*Vadim Kotov and Michael Wojnowicz (Cylance Inc)*

## **Program Committee Chairs**

Yan Shoshitaishvili, *Arizona State University*  
Ruoyu “Fish” Wang, *University of California, Santa Barbara*

## **Program Committee**

Davide Balzarotti, *EURECOM*  
Tiffany Bao, *Carnegie Mellon University*  
Antonio Bianchi, *UC Santa Barbara*  
Sang Kil Cha, *KAIST*  
Thanassis Avgerinos, *ForAllSecure*  
Brendan Dolan-Gavitt, *New York University*  
Thomas Dullien, *Google*  
Manuel Egele, *Boston University*  
Alessandro Di Federico, *Politecnico di Milano*  
Taesoo Kim, *Georgia Institute of Technology*  
Tim Leek, *MIT Lincoln Labs*  
Zhiqiang Lin, *UT Dallas*  
David Melski, *Grammatech*  
Tavis Ormandy, *Google*  
William Robertson, *Northeastern University*  
Michalis Polychronakis, *Stony Brook University*  
Christopher Salls, *UC Santa Barbara*  
Giovanni Vigna, *UC Santa Barbara*  
Jordan Wiens, *Vector35*  
Michal Zalewski, *Google*  
Chao Zhang, *Tsinghua University*  
Mingwei Zhang, *Intel Labs*