

Proceedings

BAR 2019

**Workshop on
Binary Analysis Research**

February 24, 2019
San Diego, California

Published by the





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

Copyright © 2019 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.

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) 1-891562-58-4

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

Binary Translation

B2R2: Building an Efficient Front-End for Binary Analysis

Minkyu Jung (KAIST), Soomin Kim (KAIST), HyungSeok Han (KAIST), Jaeseung Choi (KAIST), Sang Kil Cha (KAIST)

Performance, Correctness, Exceptions: Pick Three

Andrea Gussoni (Politecnico di Milano), Alessandro Di Federico (Politecnico di Milano), Pietro Fezzardi (Politecnico di Milano), Giovanni Agosta (Politecnico di Milano)

Binary Analysis and Security

CLIK on PLCs! Attacking Control Logic with Decompilation and Virtual PLC

Sushma Kalle (University of New Orleans), Nehal Ameen (University of New Orleans), Hyunguk Yoo (University of New Orleans), Irfan Ahmed (Virginia Commonwealth University)

Symbolic Path Tracing to Find Android Permission-Use Triggers

Kristopher Micinski (Haverford College), Thomas Gilray (University of Alabama, Birmingham), Daniel Votipka (University of Maryland), Michelle L. Mazurek (University of Maryland), Jeffrey S. Foster (Tufts University)

Rapid Vulnerability Mitigation with Security Workarounds

Zhen Huang (Pennsylvania State University), Gang Tan (Pennsylvania State University)

Towards Automatically Generating a Sound and Complete Dataset for Evaluating Static Analysis Tools

Aravind Machiry (UC Santa Barbara), Nilo Redini (UC Santa Barbara), Eric Gustafson (UC Santa Barbara), Hojjat Aghakhani (UC Santa Barbara), Christopher Kruegel (UC Santa Barbara), Giovanni Vigna (UC Santa Barbara)

Binary Mutation Analysis of Tests Using Reassembleable Disassembly

Navid Emamdoost (University of Minnesota), Vaibhav Sharma (University of Minnesota), Tae Byun (University of Minnesota), Stephen McCamant (University of Minnesota)

Machine Learning and Binary Analysis

Investigating Graph Embedding Neural Networks with Unsupervised Features
Extraction for Binary Analysis

*Luca Massarelli (Sapienza University of Rome), Giuseppe A. Di Luna (CINI -
National Laboratory of Cybersecurity), Fabio Petroni (Independent Researcher),
Leonardo Querzoni (Sapienza University of Rome), Roberto Baldoni (Italian
Presidency of Ministry Council)*

Enhancing Symbolic Execution by Machine Learning Based Solver Selection

*Sheng-Han Wen (National Taiwan University), Wei-Loon Mow (National Taiwan
University), Wei-Ning Chen (National Taiwan University), Chien-Yuan Wang
(National Taiwan University), Hsu-Chun Hsiao (National Taiwan University)*

A Cross-Architecture Instruction Embedding Model for Natural Language Processing-
Inspired Binary Code Analysis

*Kimberly Redmond (University of South Carolina), Lannan Luo (University of
South Carolina), Qiang Zeng (University of South Carolina)*

Organizing Committee

General Chair

Ruoyu “Fish” Wang, *Arizona State University*

Paper Sessions Chair

Antonio Bianchi, *The University of Iowa*

Discussion Sessions Chair

Brendan Dolan-Gavitt, *New York University*

Program Committee

Thanassis Avgerinos, *ForAllSecure*

Davide Balzarotti, *EURECOM*

Tiffany Bao, *Arizona State University*

Zheng Leong Chua, *National University of Singapore*

Jacopo Corbetta, *Qualcomm*

Alessandro Di Federico, *rev.ng*

Manuel Egele, *Boston University*

Sang Kil Cha, *KAIST*

Christophe Hauser, *University of Southern California*

Zhenkai Liang, *National University of Singapore*

Taesoo Kim, *Georgia Institute of Technology*

Tim Leek, *MIT Lincoln Labs*

Christopher Liebchen, *Independent Researcher*

Zhiqiang Lin, *The Ohio State University*

Aravind Machiry, *UC Santa Barbara*

David Melski, *GammaTech*

Michalis Polychronakis, *Stony Brook University*

Wil Robertson, *Northeastern University*

Brendan Saltaformaggio, *Georgia Institute of Technology*

Yan Shoshitaishvili, *Arizona State University*

Giovanni Vigna, *UC Santa Barbara*

Jordan Wiens, *Vector35*

Stefano Zanero, *Politecnico Di Milano*

Chao Zhang, *Tsinghua University*

Mingwei Zhang, *Intel Labs*

Workshop Advisor

Yan Shoshitaishvili, *Arizona State University*