

Proceedings

BAR 2021

**Workshop on
Binary Analysis Research**

February 21, 2021
Virtual

Published by the





Internet Society
11710 Plaza America Drive
Suite 400
Reston, VA 20190

Copyright © 2021 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, 11710 Plaza America Drive, Suite 400, Reston, VA 20190 USA, tel. +1 703 439 2120, fax +1 703 326 9881, ndss@elists.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) 1-891562-69-X

Additional copies may be ordered from:



Internet Society
11710 Plaza America Drive
Suite 400
Reston, VA 20190
tel +1 703.439.2120
fax +1 703.326.9881
<http://www.internetsociety.org>

Table of Contents

Organizing Committee

Binary Analysis

SN4KE: Practical Mutation Testing at Binary Level

Mohsen Ahmadi, Pantea Kiaei, Navid Emamdoost

Short Paper: Declarative Demand-Driven Reverse Engineering

Yihao Sun, Jeffrey Ching, Kristopher Micinski

PyPANDA: Taming the PANDAmorium of Whole System Dynamic Analysis

Luke Craig, Andrew Fasano, Tiemoko Ballo, Tim Leek, Brendan Dolan-Gavitt, William Robertson

Effects of Precise and Imprecise Value-Set Analysis (VSA) Information on Manual Code Analysis

Laura Matzen, Michelle A Leger, Geoffrey Reedy

Binary Fuzzing

JMPscare: Introspection for Binary-Only Fuzzing

Dominik Maier, Lukas Seidel

icLibFuzzer: Isolated-context libFuzzer for Improving Fuzzer Comparability

Yu-Chuan Liang, Hsu-Chun Hsiao

Embedded Systems

Is Your Firmware Real or Re-Hosted? A case study in re-hosting VxWorks control system firmware

Abraham A. Clements, Logan Carpenter, William A. Moeglein, Christopher Wright

Dinosaur Resurrection: PowerPC Binary Patching for Base Station Analysis

Uwe Müller, Eicke Hauck, Timm Welz, Jiska Classen, Matthias Hollick

Polypyus – The Firmware Historian

Jan Friebertshäuser, Florian Kosterhon, Jiska Classen, Matthias Hollick

Organizing Committee

Program Chair

Brendan Dolan-Gavitt, *New York University*

Program Committee

Yan Shoshitaishvili, *Arizona State University*

Xinyu Xing, *Penn State University*

Andrea Lanzi, *University of Milan*

Lorenzo Cavallaro, *King's College London*

Sophia d'Antoine, *Margin Research*

Tim Bryant, *Vector 35*

Taegy Kim, *Purdue University*

Sébastien Bardin, *CEA LIST*

Zhiqiang Lin, *Ohio State University*

Antonio Bianchi, *Purdue University*

Maverick Woo, *Carnegie Mellon University*

Daniele Cono D'Elia, *Sapienza University of Rome*

Sarah Zennou, *Airbus*

Konrad Rieck, *TU Braunschweig*

Ruoyu "Fish" Wang, *Arizona State University*

Edward J. Schwartz, *Carnegie Mellon University*

Martina Lindorfer, *TU Wien*

Mariano Graziano, *Cisco Talos*

Christophe Hauser, *Information Sciences institute, University of Southern California*

Juan Caballero, *IMDEA Software Institute*

Aurélien Francillon, *EURECOM*

Grant Hernandez, *Qualcomm*

Alexei Bulazel, *Independent Security Researcher*