

Binary Analysis Research Workshop 2021 (BAR 2021)

Online
21 February 2021

ISBN: 978-1-7138-3762-6

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2021) by The Internet Society
All rights reserved.

Printed with permission by Curran Associates, Inc. (2021)

For permission requests, please contact The Internet Society
at the address below.

The Internet Society
11710 Plaza America Drive, Suite 400
Reston, VA 20190
U.S.A.

Phone: (703) 439-2120
Fax: (703) 326-9881

www.internetsociety.org

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
Email: curran@proceedings.com
Web: www.proceedings.com

Table of Contents

Organizing Committee

Binary Analysis

- 1 SN4KE: Practical Mutation Testing at Binary Level
Mohsen Ahmadi, Pantea Kiaei, Navid Emamdoost
- 10 Short Paper: Declarative Demand-Driven Reverse Engineering
Yihao Sun, Jeffrey Ching, Kristopher Micinski
- 17 PyPANDA: Taming the PANDAmonium of Whole System Dynamic Analysis
Luke Craig, Andrew Fasano, Tiemoko Ballo, Tim Leek, Brendan Dolan-Gavitt, William Robertson
- 31 Effects of Precise and Imprecise Value-Set Analysis (VSA) Information on Manual Code Analysis
Laura Matzen, Michelle A Leger, Geoffrey Reedy

Binary Fuzzing

- 43 JMPscare: Introspection for Binary-Only Fuzzing
Dominik Maier, Lukas Seidel
- 51 icLibFuzzer: Isolated-context libFuzzer for Improving Fuzzer Comparability
Yu-Chuan Liang, Hsu-Chun Hsiao

Embedded Systems

- 62 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
- 74 Dinosaur Resurrection: PowerPC Binary Patching for Base Station Analysis
Uwe Müller, Eicke Hauck, Timm Welz, Jiska Classen, Matthias Hollick
- 85 Polypyus – The Firmware Historian
Jan Friebertshäuser, Florian Kosterhon, Jiska Classen, Matthias Hollick