Proceedings

# BAR 2018

# Workshop on
# Binary Analysis Research

February 18, 2018
San Diego, California

*Published by the*

Internet Society

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

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) 1-891562-50-9

*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**

**Miscellaneous**

**Reverse Engineering**

# Program Committee Chairs’ Message

Much of the software that powers our modern society is binary software. That is, it ships (and is executed) in the form of a sequence of ones and zeroes, encoding machine instructions that, by accumulating individual tiny modifications to a process' memory, registers, and so on, collectively (help to) power such human accomplishments as the internet, same-day delivery of online-ordered packages, and the launching of sports cars at nearby planetary bodies.

However, binary software is hard to understand. This leads to an embarrassingly ineffective ability to identify flaws in binaries through principled means. The periodic identification and exploitation of such flaws in widely-deployed systems wreak significant amounts of havok on our society. The complexity of binaries also makes the automatic repair of such flaws difficult to accomplish, to say nothing simply of automatic understanding (for example, for interoperability) of the programs themselves. As a society, and as a scientific field, we must push toward a better solution.

Fortunately, heroes still exist in our world. On February 18th, around 70 such heroes gathered at the Catamaran in San Diego to discuss this challenge facing our society: ideas, techniques, and tools to accomplish the automatic analysis of binary programs. This inaugural instance of the Binary Analysis Research workshop was a success from the perspective of the academic, industry, and scientific communities. First, let's view this success through some numbers:

- 24 Program Committee members were recruited to help organize the workshop. These included prominent researchers from the academic (i.e., professors), industry, and enthusiast (i.e., students and hackers) communities.
- 22 papers were submitted to the paper sessions of the workshop. Of these, 2 papers had nothing to do with binaries. Of the remaining 20, the Program Committee painstakingly selected 8.
- 45 people specifically specified on their registrations that they were attending BAR. Since attendants to the NDSS workshops were free to wander between workshops, this is not a faithful representation of actual attendance. The official count, sometime during the paper sessions, was 58. Anecdotally, at one point, we filled all but the front row of seats, which would (anecdotally) put us somewhere around 70 attendees.
- Of the 8 presentations, we had 3 or 4 awesome technical issues requiring the swapping of laptops, and so forth. A Nintendo Switch HDMI adapter finally came to the rescue and allowed the projector to work with USB-C video output.
- The workshop concluded with a 3-hour discussion session focused on binary analysis tooling, with representatives from 9 binary analysis tools.

The workshop discussion (and other discussions in the breaks during the BAR and, afterwards, at actual bars) allowed the developers of otherwise-competing products to come together to chat and commiserate in camaraderie. In a field with some strong egos, the discussion was friendly, supportive, and very productive. Importantly, it yielded a number of concrete outcomes that the community would like to see from the workshop:

- A better collaboration point for our community, such as a mailing list.
- An abstraction language for implementing support for environmental interaction (such as syscalls).
- Standardization of terminology used in binary analysis papers and techniques.
- Standardization of artifact storage.
- A yearly edition of BAR.
- An "off-cycle" version, such as a workshop for Practical Understanding of Binaries halfway through the year between BAR instances.
- A common area to document differences and similarities between binary analysis engines, to help newcomers and experts alike in understanding what tools are geared toward what purposes.
- Some sort of tool-agnostic automated binary analysis CTF. Since BAR 2018, Rode0day (https://rode0day.mit.edu/) has launched to fill this void!

The common theme in these ideas is that the binary analysis community wants to have more collaboration and a more coherent direction. So, let's do it! Hop on the mailing list, come to PUB (when it happens) and BAR 2019 (if it happens), and help make some of these undertakings a reality! Be the heroes of binary analysis, and let's push the state of the art ever forward!

**Yan Shoshitaishvili and Ruoyu “Fish” Wang**
**Program Committee Chairs, BAR 2018**

# 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*