Table of Contents

Message from the Organizers
Organizing Committee
Program Committee

Session 1
Dissecting American Fuzzy Lop - A FuzzBench Evaluation
   Andrea Fioraldi, Alessandro Mantovani (EURECOM), Dominik Maier (TU Berlin),
   Davide Balzarotti (EURECOM)

Fine-Grained Coverage-Based Fuzzing
   Bernard Nongpoh, Marwan Nour, Michaël Marcozzi, Sébastien Bardin (Université
   Paris-Saclay, CEA, List)

Session 2
First, Fuzz the Mutants
   Alex Groce, Goutamkumar Kalburgi (Northern Arizona University), Claire Le Goues,
   Kush Jain (Carnegie Mellon University), Rahul Gopinath (Saarland University)

Generating Test Suites for GPU Instruction Sets through Mutation and Equivalence
Checking
   Shoham Shitrit, Sreepathi Pai (University of Rochester)

Session 3
Fuzzing Configurations of Program Options
   Zenong Zhang (University of Texas at Dallas), George Klees (University of
   Maryland), Eric Wang (Poolesville High School), Michael Hicks (University of
   Maryland), Shiyi Wei (University of Texas at Dallas)

NSFuzz: Towards Efficient and State-Aware Network Service Fuzzing
   Shisong Qin (Tsinghua University), Fan Hu (State Key Laboratory of Mathematical
   Engineering and Advanced Computing), Bodong Zhao, Tingting Yin, Chao Zhang
   (Tsinghua University)

datAFLow: Towards a Data-Flow-Guided Fuzzer
   Adrian Herrera (Australian National University and Defence Science and
   Technology), Mathias Payer (EPFL), Antony Hosking (Australian National
   University)
Message from the Organizers: Introducing our Pre-Registration-based Publication Process

It is our great pleasure to welcome you to the 1st International Workshop on Fuzzing (FUZZING 2022), co-located with NDSS in San Diego, CA, USA on 24 April 2022. This workshop is the first of its kind, presenting the drafts of registered reports that were accepted as part of the first stage in a two-stage publication process.

FUZZING 2022 introduces to our community a novel preregistration-based publication process that consists of two main stages; In the first stage, the program committee (PC) evaluates all submissions based on: (i) the significance and novelty of the hypotheses or techniques and (ii) the soundness and reproducibility of the methodology specified to validate the claims or hypotheses—but explicitly not based on the strength of the (preliminary) results. These draft registered reports are presented and improved at the FUZZING 2022 workshop in San Diego. After the workshop, the final versions of the registered reports are re-checked and approved by the PC. In the second stage, the PC and the Artifact Evaluation Committee (AEC), chaired by Yannic Noller, check whether the experimental methodology as laid out by the authors was correctly followed. We are excited to announce that the outcome of this stage will be published in the ACM Transactions on Software Engineering and Methodology (TOSEM) via the Preregistration track, subject to approval by the TOSEM Board.

By shifting the focus away from the results and back to the innovations, key claims, and the evaluation methodology, we can minimize the temptation to overclaim. Also, it will provide early feedback before time is spent following a possibly unsound evaluation methodology, which would lead to rejection only when all the work is already done, or the request for more experiments when all the work has concluded. This way, we hope the reviewer’s focus shifts from gatekeeping to providing productive feedback, aiming to ensure the best study design possible.

The main objectives of our new publication process are:

- **Fairness.** By asking reviewers to evaluate the study design rather than the final article, we can prevent some types of subconscious bias, such as publication bias (where authors are inclined to publish only positive results selectively), confirmation bias (where reviewers might give more credence to results that support their own views), and impact bias (where reviewers might give novel results more consideration).

- **Reproducibility.** By requesting prospective authors to specify a precise experiment protocol and consulting an AEC, reproducibility becomes a first-class citizen of the reviewing process. We request authors to provide the final artifact to ensure that other researchers can build on these results. Current authors would receive early feedback on the soundness and reproducibility of the proposed evaluation methodology, while future authors would have clear instructions on reproducing the results.

- **Support.** In this first-of-its-kind joint venture between academia and industry, we are pledging our support with the required infrastructure and resources, if needed. This is provided by Google’s fuzzer benchmarking platform and service, FuzzBench. Our aims are to reduce the barrier to entry, to facilitate a sound experimental evaluation, to maximize reproducibility, and to facilitate innovations towards a more secure open-source software ecosystem.
The purpose of the FUZZING 2022 workshop is two-fold. On the one hand, authors can get early feedback on their proposed research. On the other hand, reviewers can discuss community expectations, e.g., for a sound empirical evaluation. As part of the workshop, we organize a fishbowl where the participants can discuss their experience with Stage 1 of the publication process and provide feedback and suggestions for improvement.

The FUZZING 2022 Program Committee selected seven drafts of registered reports for the technical program of the workshop from a pool of nine submissions. Each submission received at least three reviews, and after discussion among reviewers, one additional meta-review. For each submission, the reviewers jointly decided to give one of four scores: A submission could be accepted without revision, with minor revision, and with major revisions, or it could be rejected. All accepted drafts have been published in the NDSS companion proceedings. After the FUZZING workshop, the authors will submit the revised versions of the registered reports to the ACM TOSEM Preregistration track to confirm the requested revision. For continuity, we are planning to invite the same reviewers for confirmation. Once the registered report is in-principle accepted, the experimentation period has officially commenced. When the experiments are finalized, authors of confirmed reports will be able to submit the full technical paper with all results for journal publication. If the PC and AEC confirm that the agreed-upon experimental protocol has been followed, any deviations from the protocol have been explained, and the results have been properly interpreted, the full paper is accepted for journal publication.

The workshop will also feature two exciting keynotes from well-known members of the community: one from Andreas Zeller (CISPA Helmholtz Center for Information Security) on “Fuzzing: A Tale of Two Cultures” and the other from Abhishek Aarya (Google) on “The Evolution of Fuzzing in Finding the Unknowns”.

We would like to take the opportunity to thank the program committee, the artifact evaluation committee, our keynote speakers, the NDSS workshop chairs, as well as all of the authors who submitted papers. We also thank ACM TOSEM Editor in Chief Mauro Pezze for his openness towards our initiative and the productive discussions in support of our endeavour. Without everyone’s generous support, our journey would not be possible.

We hope to see interactive sessions between researchers and practitioners and hope to provide a stimulating forum for exchanging and developing new ideas in fuzzing. We wish all of you an enjoyable workshop.

Marcel Böhme
MPI for Security and Privacy
Germany
marcel.boehme@acm.org

Cristian Cadar
Imperial College
London
United Kingdom
c.cadar@imperial.ac.uk

Baishakhi Ray
Columbia University
United States of America
rayb@cs.columbia.edu

László Szekeres
Google
United States of America
lszekeres@google.com
Organizing Committee

Marcel Böhme, MPI-SP and Monash University
Cristian Cadar, Imperial College London
Baishakhi Ray, Columbia University
László Szekeres, Google

Program Committee

Cornelius Aschermann, Facebook
Sang Kil Cha, KAIST
Brendan Dolan-Gavitt, New York University
Alastair Donaldson, Imperial College London
Renáta Hodován, University of Szeged
Thorsten Holz, CISPA
Caroline Lemieux, Microsoft Research and UBC
Martin Nowak, Imperial College London
Van-Thuan Pham, The University of Melbourne
John Regehr, University of Utah
Konstantin Serebryany, Google
Willem Visser, AWS and Stellenbosch University
Qian Zhang, University of California, Los Angeles
Chengyu Zhang, East China Normal University