2nd International KLEE Workshop on Symbolic Execution

Workshop Introduction

Cristian Cadar

Department of Computing

Imperial College London

Imperial College London

10-11 June 2021
Online

1st International KLEE Workshop on Symbolic Execution

19-20 April, 2018 • London, United Kingdom

Tweets by @kleesymex

kleesymex @kleesymex

Save the date! 1st International KLEE

1st International KLEE Workshop

- 19-20 April 2018 at Imperial College London
- 82 participants from academia, industry and government
  - Had to close registration early due to capacity constraints
- Dozen different countries across three continents
- Sponsored by EPSRC, Baidu, Bloomberg, Fujitsu, Huawei, Imperial College
- Three academic keynotes (Khurshid, Orso, Roychoudhury)
- Two industry keynotes (Ghosh – Fujitsu, Li – Baidu)
- 17 regular talks and 5 posters
- Lunches, coffee breaks, and pub
- Fantastic feedback post-workshop

2nd International KLEE Workshop

- ~~14-15 September 2020, London, UK~~
- ~~22-23 April 2021, London UK~~

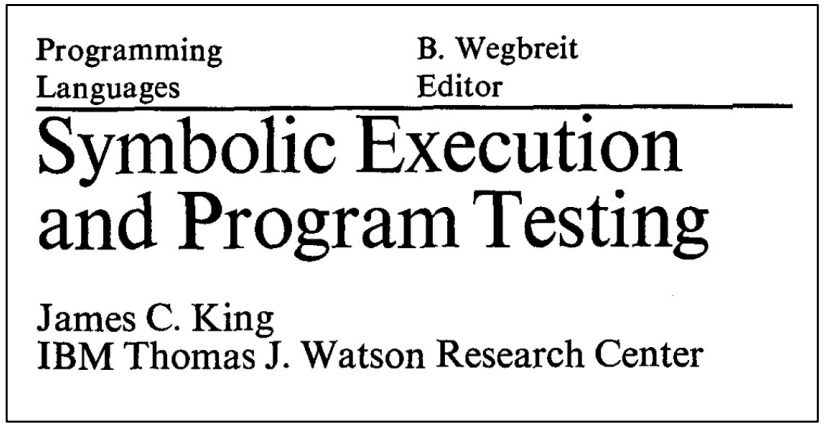
Image by Karen Arnold (public domain)

2nd International KLEE Workshop

- ~~14-15 September 2020, London, UK~~
- ~~22-23 April 2021, London UK~~
- 10-11 June 2021, Online

Image by Nick Youngson, Alpha Stock Images (CC-BY-SA 3.0)

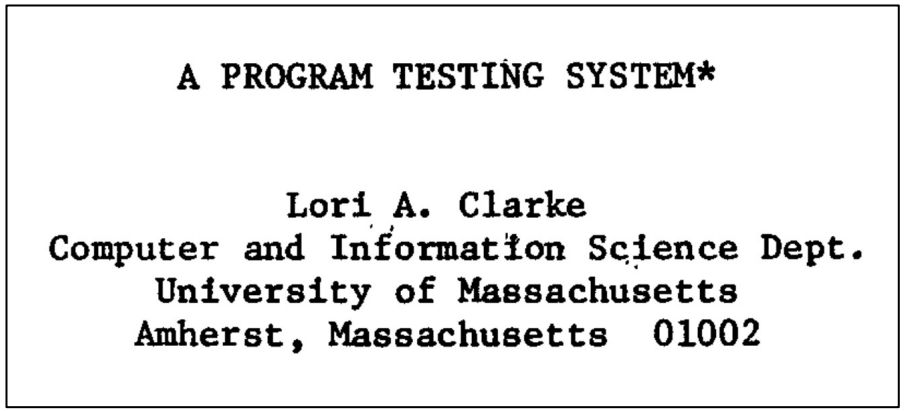
Symbolic Execution: A Bit of History: 1975-76


Programming Languages B. Wegbreit Editor

Symbolic Execution and Program Testing

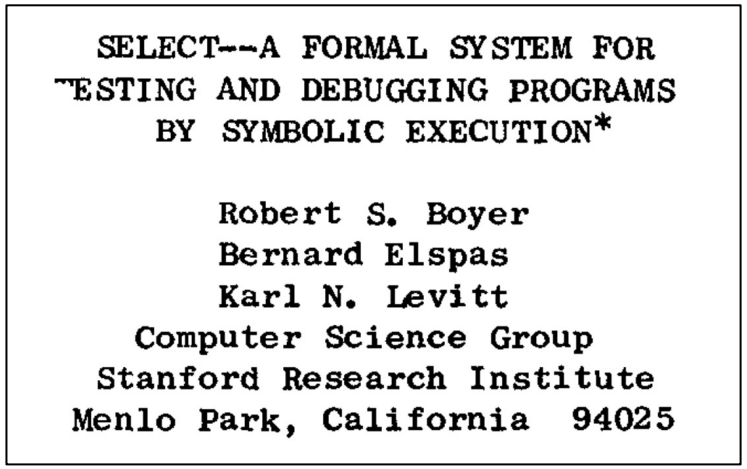
James C. King
IBM Thomas J. Watson Research Center

Symbolic execution of PL/I programs


A PROGRAM TESTING SYSTEM*

Lori A. Clarke
Computer and Information Science Dept.
University of Massachusetts
Amherst, Massachusetts 01002

Symbolic execution of Fortran programs

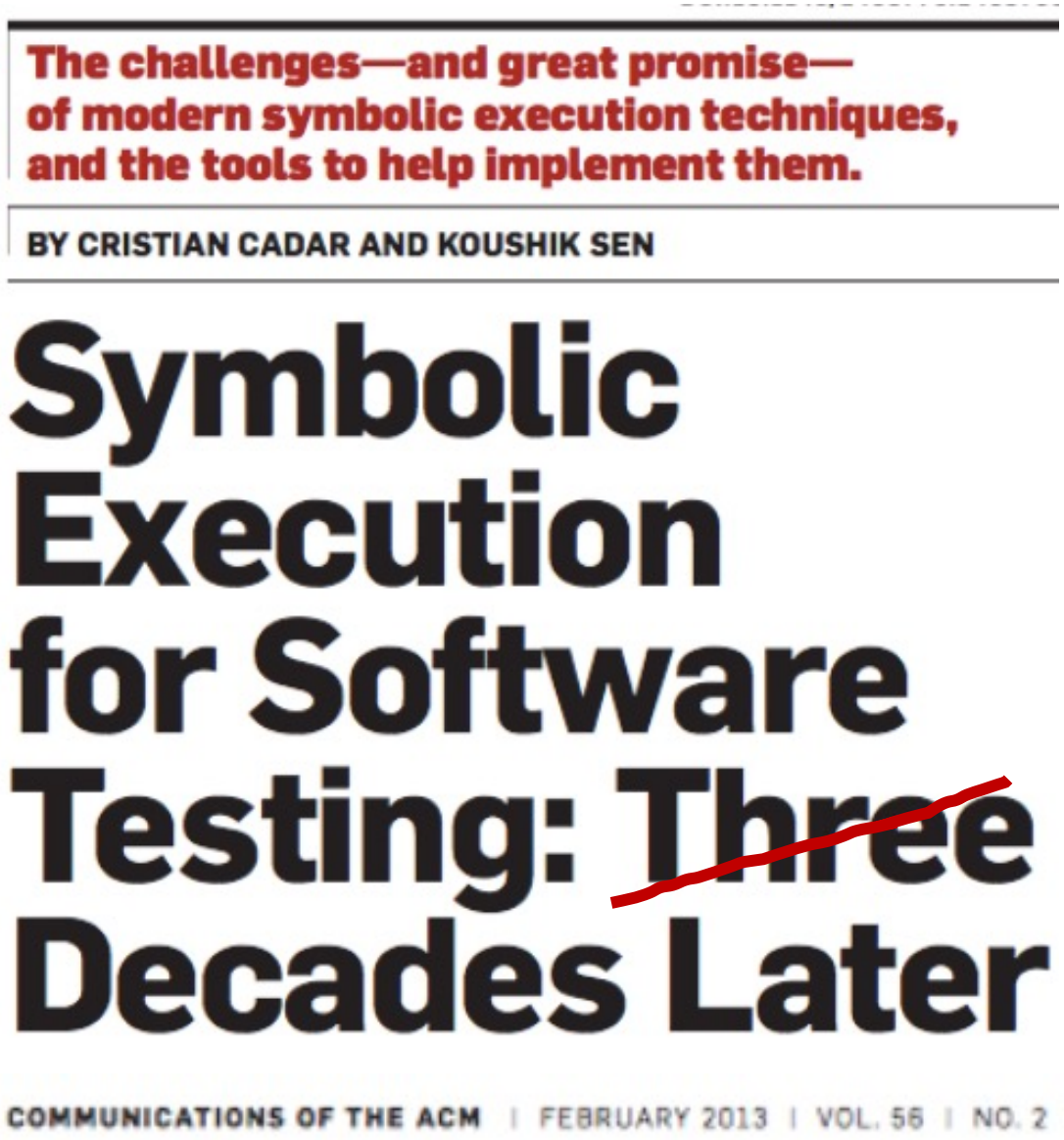

SELECT--A FORMAL SYSTEM FOR TESTING AND DEBUGGING PROGRAMS BY SYMBOLIC EXECUTION*

Robert S. Boyer
Bernard Elspas
Karl N. Levitt
Computer Science Group
Stanford Research Institute
Menlo Park, California 94025

Symbolic execution of LISP programs


1975-76

A Bit of History



The challenges—and great promise—
of modern symbolic execution techniques,
and the tools to help implement them.

BY CRISTIAN CADAR AND KOUSHIK SEN

Symbolic Execution for Software Testing: ~~Three~~ Decades Later

4+

COMMUNICATIONS OF THE ACM | FEBRUARY 2013 | VOL. 56 | NO. 2

KLEE

CREST

BINSEC

SymCC

Miasm

PathGrind

PyExZ3

SymDroid

jCUTE

TRITON

Otter

CUTE

SAGE

Savior

SymJS

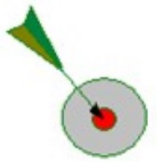
Jalangi2

Symbolic PathFinder

Manticore

angr

BinSE



DART

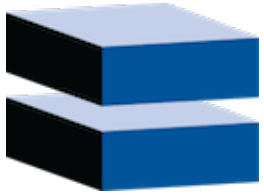
Kite

LDSE

Pex

Rubyx

JDart



S²E

CATG

CiVL

Mayhem

KLOVER

Webpage: **https://klee.github.io/**
Code: **https://github.com/klee/**
Web version: **http://klee.doc.ic.ac.uk/**

Active project

12+ years since open-sourced

8 releases

2300+ commits

400+ resolved issues

Active community

100+ contributors to codebase incl. subprojects

400+ subscribers to mailing list

490+ public forks of KLEE repository

1700+ stars on GitHub

Academic Impact & Interest

- SIGOPS Hall of Fame Award (KLEE paper)
- CCS Test of Time Award (EXE paper)
- 3200+ citations to original KLEE paper
- 200+ publications and systems building upon KLEE
  - https://klee.github.io/publications/
  - From many different research communities: testing, verification, systems, software engineering, programming languages, security, etc.

Industry Impact & Interest

- Companies sponsoring 1st & 2nd KLEE workshops: Baidu, Bloomberg, Google, Huawei, Fujitsu, Samsung
- Two keynotes in the first KLEE Workshop:
  - Fujitsu: Utilization and Evolution of KLEE-based Technologies for Embedded Software Testing at Fujitsu
  - Baidu: ConcFuzzer: A Sanitizer Guided Hybrid Fuzzing Framework Leveraging Greybox Fuzzing and Concolic Execution
- Many different companies reporting on using/experimenting with KLEE:
  - **Baidu**: [KLEE 2018], [IEEE S&P 2020]
  - **Fujitsu**: [PPoPP 2012], [CAV 2013], [ICST 2015], [IEEE Software 2017], [KLEE 2018]
  - **Google**: [2x KLEE 2021]
  - **Hitachi**: [CPSNA 2014], [ISPA 2015], [EUC 2016], [KLEE 2021]
  - **Intel**: [WOOT 2015]
  - **NASA Ames**: [NFM 2014]
  - **Samsung**: [2x KLEE 2018]
  - **Trail of Bits**: https://blog.trailofbits.com/
  - **etc.**
- Many industry participants at KLEE workshops!

KLEE and SymEx: *Beyond* Bug Finding

- Bug finding is ***extremely*** important
- But symbolic execution is applicable to ***many other*** problems!
  - Program repair
  - Verification
  - Refactoring
  - Education
  - Equivalence checking
  - Test case generation and augmentation
  - Debugging and fault localization
  - Model learning
  - Document repair
  - Reverse engineering
  - Side-channel analysis
  - Test-case reduction
  - Liveness analysis
  - Binary lifting and recompilation
  - Detecting cheating in online games

etc. etc.

2nd International KLEE Workshop on Symbolic Execution

10-11 June, 2021 • Online

Tweets by @kleesymex

kleesymex Retweeted

Participants

206 registrations!

34 countries across 6 continents!

Two workshop days favoring different timezones, taking into account organizers in Europe:

Day 1: better for Western Hemisphere

Day 2: better for Eastern Hemisphere

United States of America	BST-8
	BST-7
United States of America	BST-6
Canada, United States of America	BST-5
Argentina	BST-4
	BST-3
	BST-2
	BST-1
Algeria, Cameroon, Ireland, Morocco, United Kingdom	BST
Austria, Czech Republic, France, Germany, Hungary, Italy, Luxembourg, Netherlands, Poland, Portugal, Spain, Sweden, Switzerland	BST+1
Greece, Israel, Romania, Russia	BST+2
United Arab Emirates	BST+3
Pakistan	BST+4
India	BST+4.5
Bangladesh	BST+5
	BST+6
China, Singapore	BST+7
Japan, South Korea	BST+8
Australia	BST+9

Affiliations

- Good mix of academia and industry
  - Around 60% academia and 40% industry

- Good mix of career stages
  - E.g., academic researchers pre- and post-PhD in similar proportion

Participants interests

Program

- Keynote from Chao Wang, USC
- 24 regular presentations, grouped into 7 sessions:
  1) Memory Representation and Constraint Solving
  2) Testing Evolving Software and Fault Injection
  3) New Applications
  4) Mutation Testing and Fault Localization
  5) Scalability and Side Channels
  6) Model Learning and Education
  7) Extending Applicability

- A big thank you to all contributors and participants!

Organization Team

- Frank Busse (co-chair)
- Martin Nowack (co-chair)

- Timotej Kapus
- Hassan Patel
- Jamie Perrins

Gold sponsors

Bloomberg®

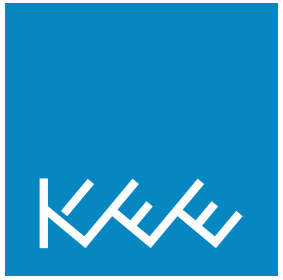
SAMSUNG

Silver sponsor

Google

Supported by

Imperial College London



2nd International KLEE Workshop on Symbolic Execution

Thank You

To Our Sponsors

https://srg.doc.ic.ac.uk/klee21/
@kleesymex

Session Chairs

- Tomasz Kuchta (Session 1)
- Alastair Reid (Session 2)
- Alex Orso (Session 3)
- Sébastien Bardin (Session 4)
- Daniel Schemmel (Session 5)
- Julien Vanegue (Session 6)
- Martin Nowack (Session 7)

KLEE Contributors

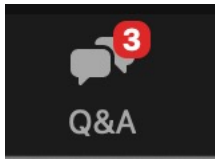
- Martin Nowack for co-maintaining KLEE for the last many years
- Prior co-maintainers Daniel Liew, Andrea Mattavelli and Daniel Dunbar
- Daniel Dunbar for starting the project back in 2007!
- Other major contributors particularly Julian Büning, Frank Busse, Jiri Slaby, Peter Collingbourne, Timotej Kapus, Gleb Popov, Hristina Palikareva
- Frank Busse for maintaining the list of publications building up on KLEE (now at 220+)
- The entire awesome KLEE community

Workshop Logistics

- Regular talks take ~12’ followed by ~3’ of Q&A
  - Session chairs will ensure that talks don’t overrun
  - Both live and pre-recorded, depending on speaker preferences
- Sessions end with a discussion with the speakers and session chair
  - Audience can ask additional questions about specific talks or the session topic

- Recording policy: the workshop is recorded BUT:
  - The Q&A and discussion sessions will NOT be made available to encourage participation
  - Individual talks will be made available with workshop permission via a YouTube KLEE channel

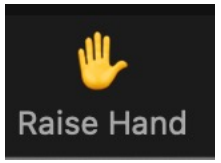
Workshop Logistics



Please use Zoom's Q&A feature to:

1) Ask questions
2) Vote on interesting questions

After each session, any unanswered questions are dismissed



You can also raise your hand to ask questions with voice:

- But with a large audience size, it makes sense to prioritize written questions

You can use Discord for more questions and to chat about other topics

Two Final Requests

- Contribute your techniques/extensions (or parts of) to the KLEE mainline
  - An achievement in itself, as the barrier for successful integration is high
  - Your technique won’t be forgotten and will be useful to others
  - New techniques could compare with your technique too

- Ask lots of questions during the workshop!
  - That’s one of the main reasons for having the workshop in the first place!

2nd International KLEE Workshop on Symbolic Execution

10-11 June, 2021 • Online

Tweets by @kleesymex

kleesymex Retweeted