3rd International KLEE Workshop on Symbolic Execution

Workshop Introduction

Cristian Cadar

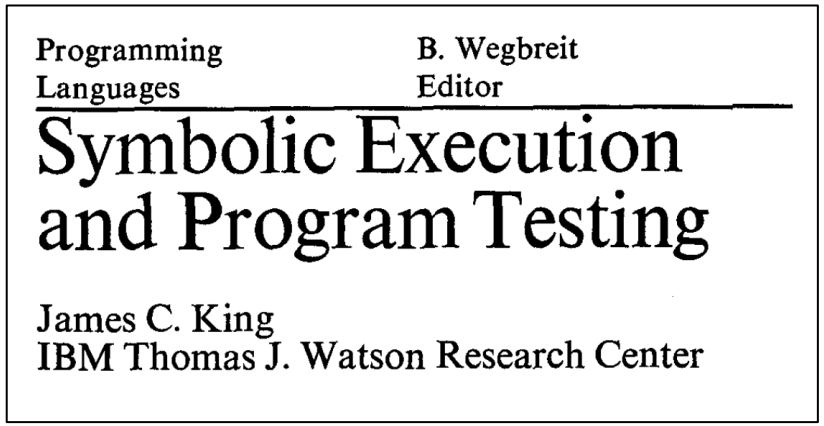
Department of Computing

Imperial College London

Imperial College London

15-16 September 2022
London, UK and Online

Symbolic Execution
A Bit of History: 1975-76

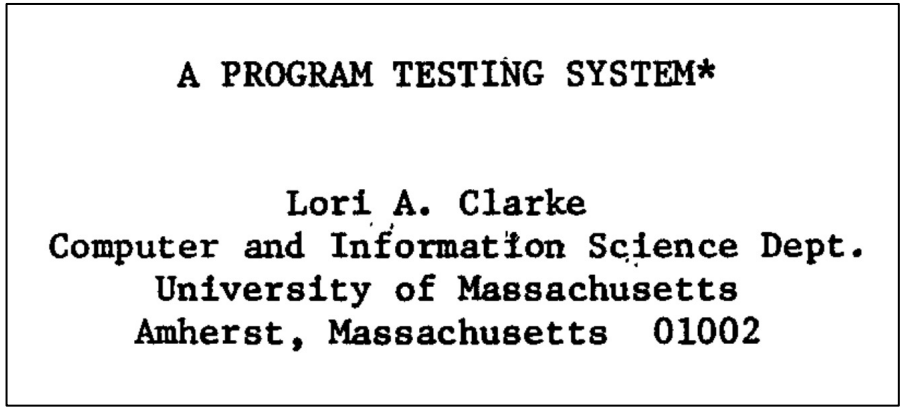


Programming Languages — B. Wegbreit Editor

Symbolic Execution and Program Testing

James C. King
IBM Thomas J. Watson Research Center

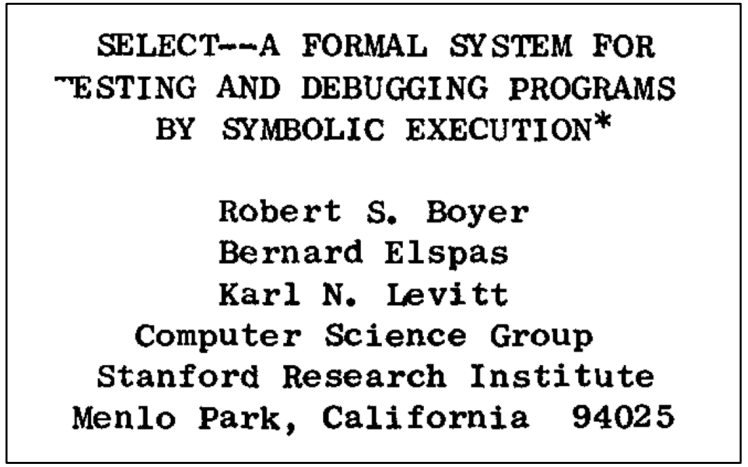
Symbolic execution of PL/I programs



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

Symbolic Execution
A Bit of History: 2005

Symbolic Execution for Software Testing: Three Decades Later

Mixed concrete-symbolic execution /

(dynamic symbolic execution, concolic execution, whitebox fuzzing…)

Concurrent with a revolution in SAT & SMT solving

DART: Directed Automated Random Testing

Patrice Godefroid Nils Klarlund
Bell Laboratories, Lucent Technologies
{god,klarlund}@bell-labs.com

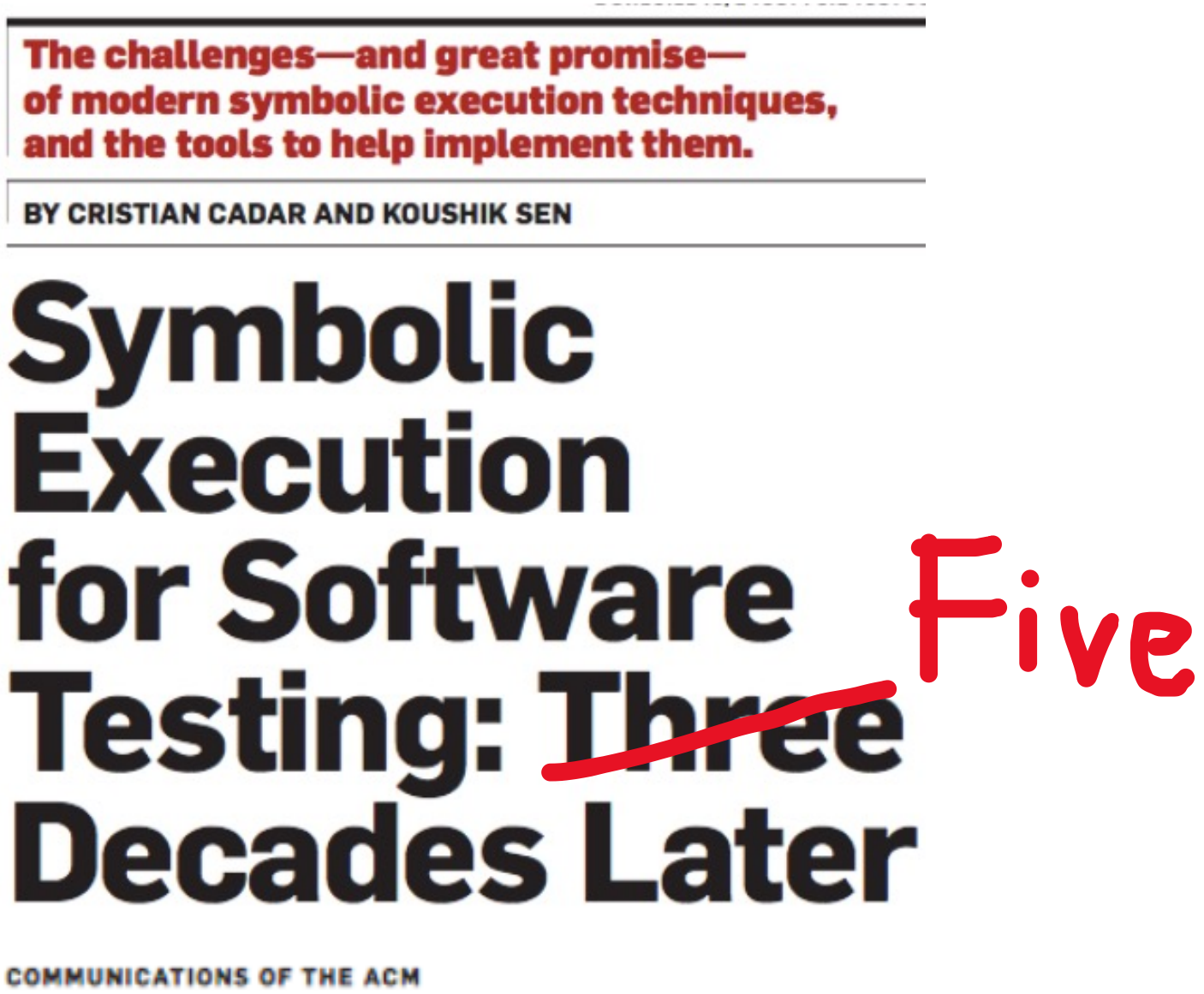
Koushik Sen
Computer Science Department
University of Illinois at Urbana-Champaign
ksen@cs.uiuc.edu

Execution Generated Test Cases: How to Make Systems Code Crash Itself

Cristian Cadar and Dawson Engler*

Computer Systems Laboratory
Stanford University
Stanford, CA 94305, U.S.A.

A Bit of History



KLEE

CREST

BINSEC

SymCC

Miasm

PathGrind

PyExZ3

SymDroid

jCUTE

TRITON

Otter

CUTE

SAGE

Savior

SymJS

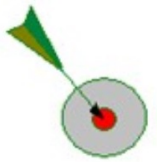
Jalangi2

Symbolic PathFinder

Manticore

angr

BinSE



DART

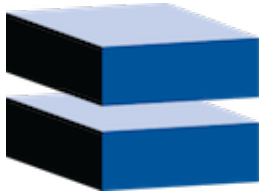
Kite

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

13+ years since open-sourced

9 releases

2400+ commits

Active community

100+ contributors to codebase incl. subprojects

400+ subscribers to mailing list

580+ public forks of KLEE repository

2000+ stars on GitHub

Academic Impact & Interest

- SIGOPS Hall of Fame Award (KLEE paper)
- CCS Test of Time Award (EXE paper)
- 3700+ citations to original KLEE paper
- 250+ 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 & 3rd KLEE workshops:

  Baidu, Bloomberg, Fujitsu, Google, Huawei, Qualcomm, Samsung, Trail of Bits

- Two industry keynotes to the first KLEE Workshop (and two more now!):
  - 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..**
- High percentage of 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.

KLEE Workshop 2018

Organization Sponsors

- 80+ participants from academia, industry and government
- 12 different countries across three continents
- Sponsored by EPSRC, Baidu, Bloomberg, Fujitsu, Huawei, Imperial College London
- 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

1st International KLEE Workshop on Symbolic Execution

19-20 April, 2018 • London, United Kingdom

Tweets by @kleesymex

kleesymex @kleesymex

Save the date! 1st International KLÉE

- 200+ participants from academia and industry
- 34 different countries across **six continents**
- Sponsored by Bloomberg, Samsung, Google and Imperial College London
- Keynote from Chao Wang
- 24 regular talks
- Great feedback post-workshop
- Huge support for a future in-person event

2nd International KLEE Workshop on Symbolic Execution

10-11 June, 2021 • Online

Tweets by @kleesymex

kleesymex Retweeted

KLEE Workshop 2022

3rd International KLEE Workshop on Symbolic Execution

15–16 September 2022 • London, UK and Online

Tweets from @kleesymex

kleesymex
@kleesymex · Sep 7

Participants

- 125+ participants, with ~65 onsite and ~60 online
- 29 different countries across 5 continents

- Good mix of industry and academia:
  - Around 58% academia, 36% industry, 6% other

- More registrations than participants:
  - Several participants could unfortunately not get a visa on time
  - Others had their flights/trained cancelled
  - Some will join late, this afternoon

Participants' interests (online only)

Program

- 4 keynotes: 2 from academia, 2 from industry
  - Jan Strejček, Masaryk University
  - Peter Goodman, Trail of Bits
  - Sébastien Bardin, CEA LIST, Université Paris-Saclay
  - Vitaly Chipounov, Cyberhaven

Program (cont.)

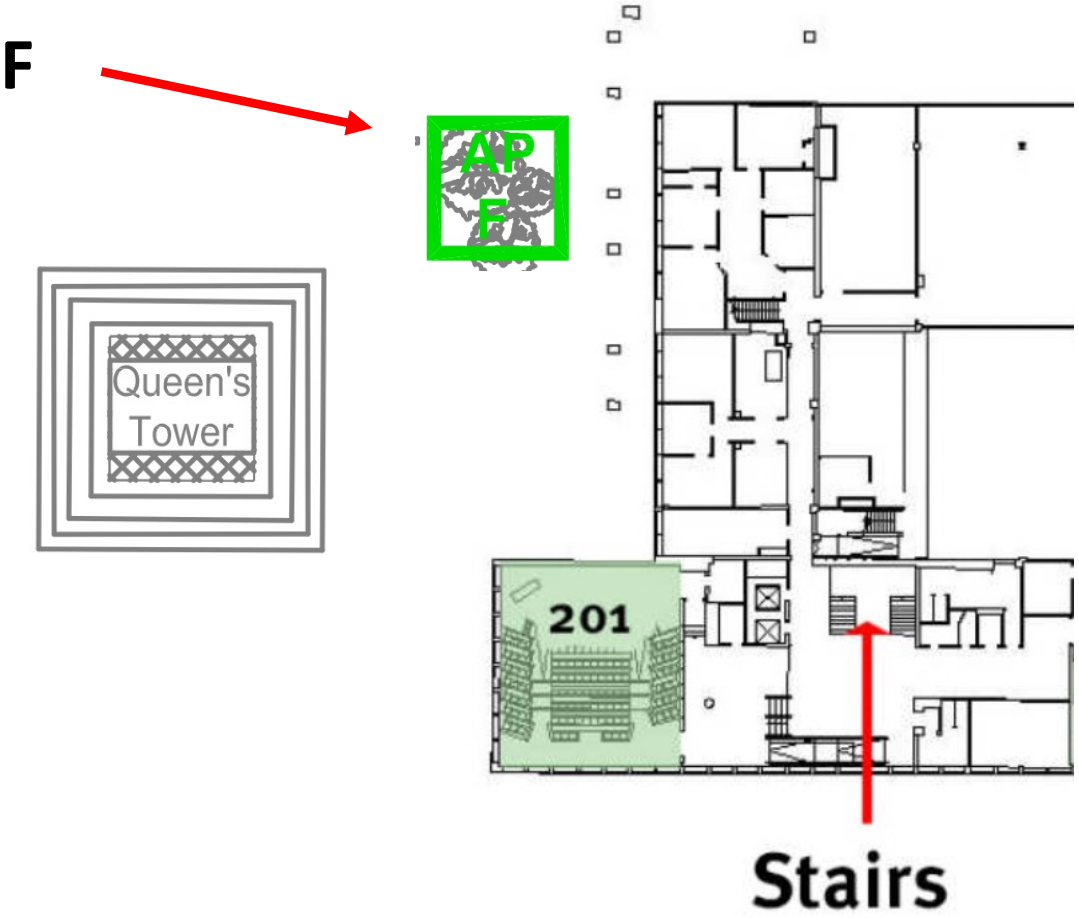
- 20 regular presentations, grouped into 7 sessions
- 10 posters, presented in two poster sessions and outside the lecture hall, with additional questions on Discord: #posters

- **A big thank you to all contributors and participants!**

Fire Alarm

In case of a fire alarm, follow exit signs and gather at assembly point

Assembly point F



Streaming and Recording

The workshop is streamed to online participants

- Speakers: please stand to the left of the podium to be seen
- We will use the podium computer for regular talks

The workshop is also recorded BUT:

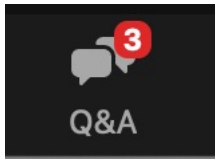
- The Q&A sessions will NOT be made available to encourage participation
- Individual talks will be made available with speaker consent via the YouTube KLEE channel

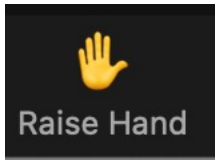
Q&A

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

In-person participants:

- You can raise your hand and ask your question
- Session chair or speaker should repeat it to make sure online participants hear it properly





Online participants:

- Please use Zoom's Q&A feature to ask and upvote questions
- Can also press the "Raise Hand" button to ask questions with voice
  - But with a large audience size, session chairs might prioritize written questions
- After each session, any unanswered questions are dismissed
- More permanent conversations should move to Discord

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

Session Chairs

- Session: Chair (online chair):
  1. Memory Modelling: Peter O'Hearn (Martin)
  2. Floating Point and Incorrectness Logic: Tomasz Kuchta (Daniel)
  3. Debug Info, Reverse Engineering and Program Repair: Martin Nowack (Frank)
  4. Symbolic Execution and Greybox Fuzzing: Frank Busse (Martin)
  5. Path Exploration: Alessandro Orso (Daniel)
  6. Precondition Inference and Driver Generation: Jonathan Bell (Martin)
  7. Models, Synthesis, Specs and New Architectures: Daniel Schemmel (Frank)
- Session chairs will be assisted by an online chair (Daniel, Frank or Martin) who will point out questions from online participants

Workshop Co-chairs

Frank Busse

Martin Nowack

Daniel Schemmel

Finances and admin:

- Hassan Patel
- Jamie Perrins

Gold sponsors

Bloomberg

SAMSUNG

Silver sponsors

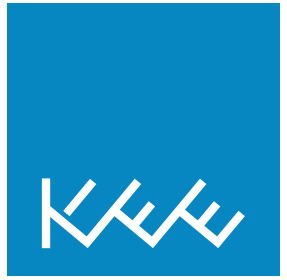
Google

Qualcomm

TRAIL OF BITS

Supported by

Imperial College London



3rd International KLEE Workshop on Symbolic Execution

Thank You

To Our Sponsors

https://srg.doc.ic.ac.uk/klee22/

@kleesymex

KLEE Community

- Martin Nowack for co-maintaining KLEE for the last many years
- Frank Busse for recently joining the maintainers team and maintaining the list of publications building up on KLEE (now at 250+)
- Prior co-maintainers Daniel Liew, Andrea Mattavelli and Daniel Dunbar
- Daniel Dunbar for starting the project back in 2007!
- Our 100+ contributors
- The entire awesome KLEE community

KLEE Workshop 2022

3rd International KLEE Workshop on Symbolic Execution

15–16 September 2022 • London, UK and Online

Tweets from @kleesymex

kleesymex
@kleesymex · Sep 7