4th International KLEE Workshop on Symbolic Execution

Workshop Introduction

Cristian Cadar

Department of Computing
Imperial College London

Imperial College London

15-16 April'24
Lisbon, Portugal

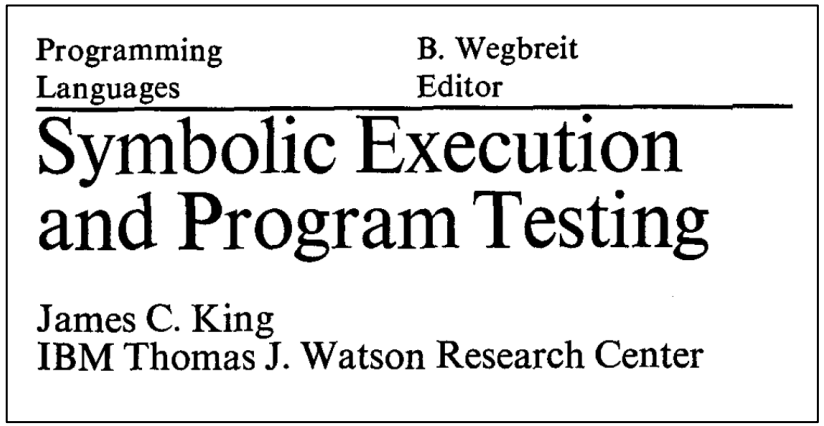
KLEE

KLEE Workshop 2024

Program Attending Call for Contributions Organisation Sponsors Series

Following three successful KLEE workshops, which have brought together over 400 participants from six continents spanning academia, industry and government, one of the main goals of KLEE'24 is to get together symbolic execution researchers, KLEE developers and KLEE users to exchange ideas, understand each other's interests and needs, and discuss the evolution of symbolic execution technology.

Symbolic Execution
A Bit of History: 1975-76

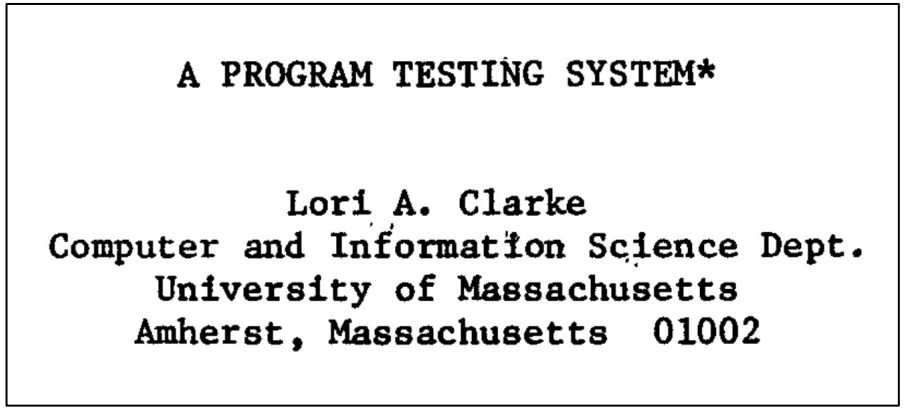


Programming Languages — B. Wegbreit Editor

Symbolic Execution and Program Testing

James C. King
IBM Thomas J. Watson Research Center

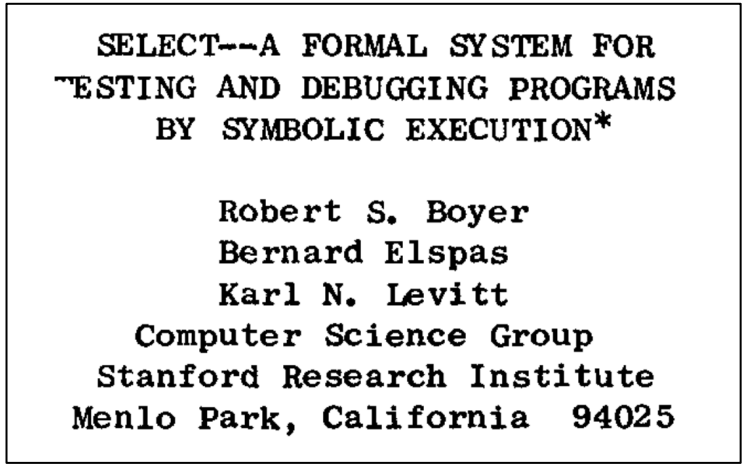
Symbolic execution of PL/I programs



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

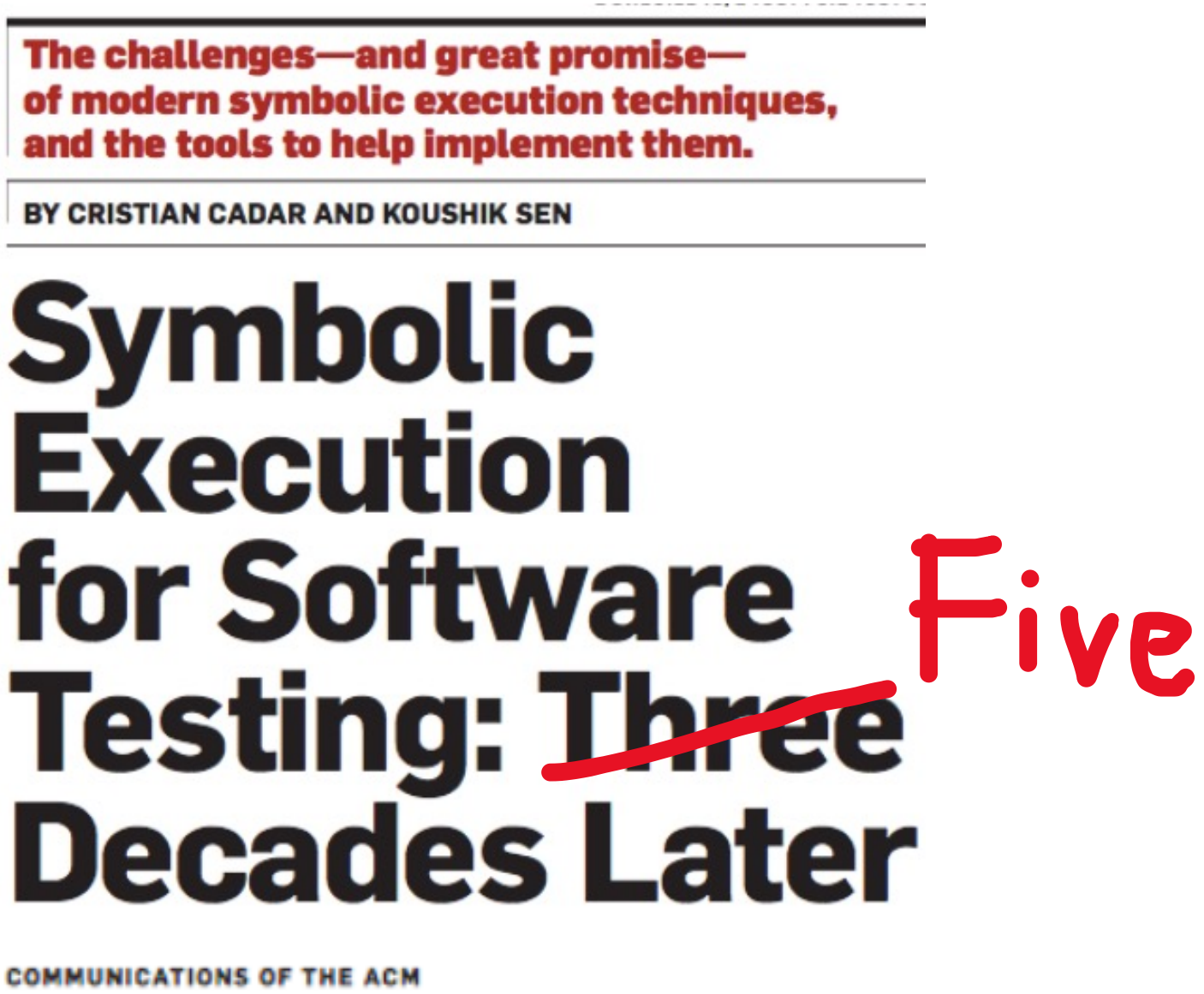
Koushik Sen
Computer Science Department
University of Illinois at Urbana-Champaign
ksen@cs.uiuc.edu

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



Five

KLEE

CREST

BINSEC

SymCC

Miasm

PathGrind

PyExZ3

SymDroid

jCUTE

TRITON

Otter

CUTE

SAGE

Savior

SymJS

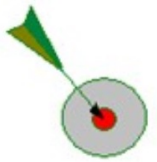
Jalangi2

Symbolic PathFinder

Manticore

angr

BinSE



DART

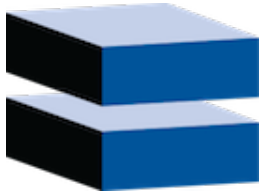
Kite

LDSE

Pex

Rubyx

JDart



S²E

CATG

CiVL

Mayhem

KLOVER

Impact in Research & Industry

- Two test of time awards
- 4000+ citations to first KLEE paper
- 280+ publications and systems building upon KLEE
  - https://klee-se.org/publications/
  - From many different research communities: testing, verification, systems, software engineering, programming languages, security, etc.

- Sponsors of KLEE Workshops:
  - Baidu, Bloomberg, Fujitsu, Google, Huawei, Qualcomm, Samsung, Trail of Bits
- Companies using/experimenting w/ KLEE:
  - **Baidu**: KLEE'18, IEEE S&P'20
  - **Fujitsu**: PPoPP'12, CAV'13, ICST'15, IEEE SW'17, KLEE'18
  - **Google**: 2x KLEE'21
  - **Hitachi**: CPSNA'14, ISPA'15, EUC'16, KLEE'21
  - **Intel**: WOOT'15
  - **NASA Ames**: NFM'14
  - **Samsung**: 2x KLEE'18
  - **Trail of Bits**: https://blog.trailofbits.com/, KLEE'22
  - **etc.**

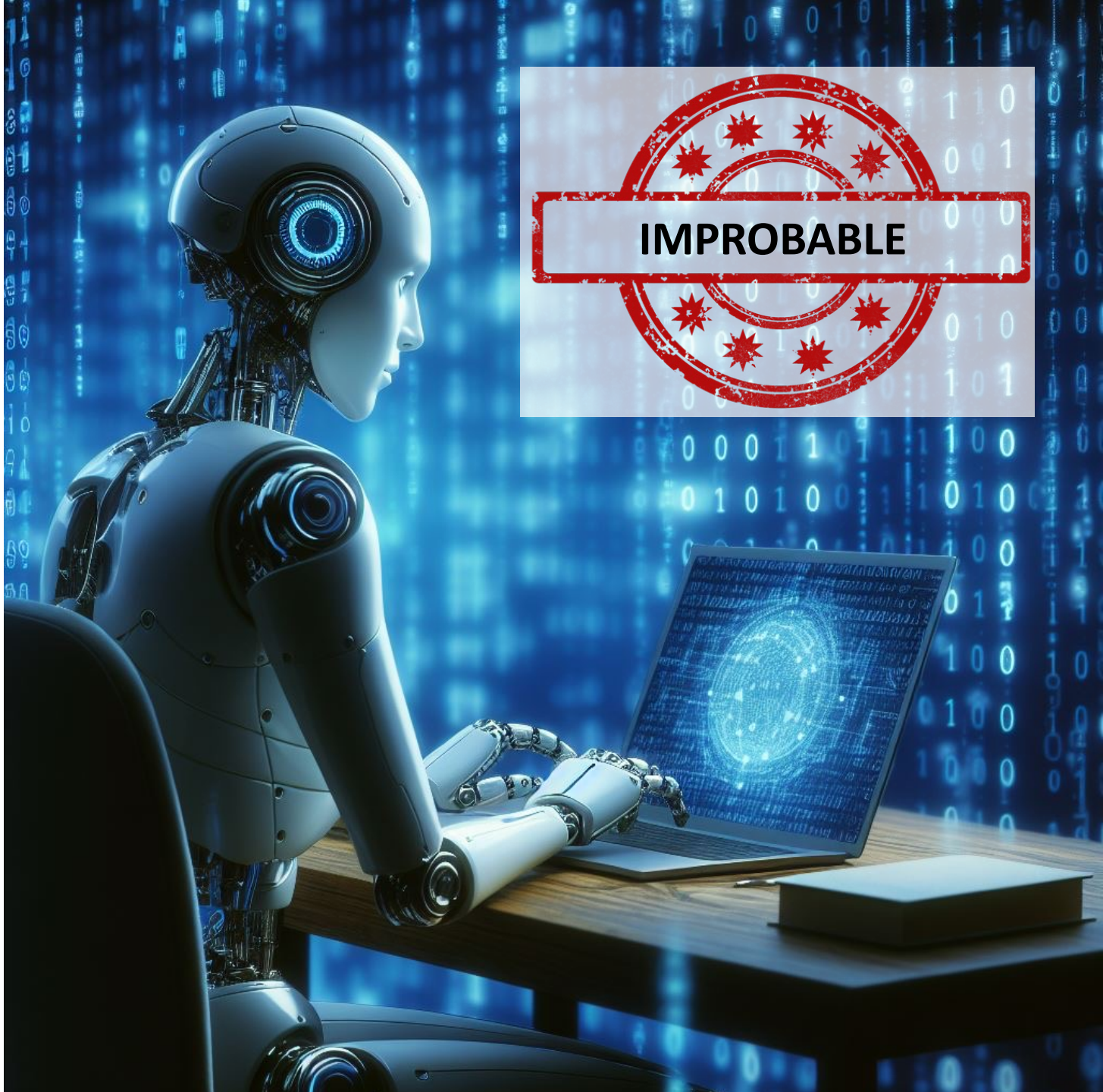
Great mix of academia & industry participants at KLEE workshops

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.

Impact of Generative AI: Two Possible Futures



AI-assisted Software Engineering

Accelerated shift from code writing to code reviewing

Program analysis techniques such as symbolic execution will become even MORE IMPORTANT

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

Active project

15 years since open-sourced

11 releases

2700+ commits

Active community

100+ contributors to codebase incl. subprojects

450+ subscribers to mailing list

650+ public forks of KLEE repository

2500+ stars on GitHub

KLEE Changes since 3rd KLEE Workshop (Sep 2022)

- New web domain: https://klee-se.org/
- Released KLEE 3.0 in June 2023 and KLEE 3.1 in Feb 2024
  - Improved detection of use-after-free errors
  - Support for UBSan checks to detect more types of undefined behaviour
  - New deterministic memory allocator (“KDAlloc”)
  - Better support for seeding, execution tree, and pointer resolution
  - Support for concrete inline assembly
  - Support for newer LLVM versions
  - Overhaul of CI and build scripts
  - Bug fixes, optimisations, refactorings, test cases, documentation, …
  - …

Still need your help!

- Lots of open issues
- Lots of suggested projects
- Need better documentation
- Need maintainer for KLEE Web

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 KLEE

KLEE Workshop 2021 Program Attending Call for Presentations Organization Sponsors Series

- 200+ online 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

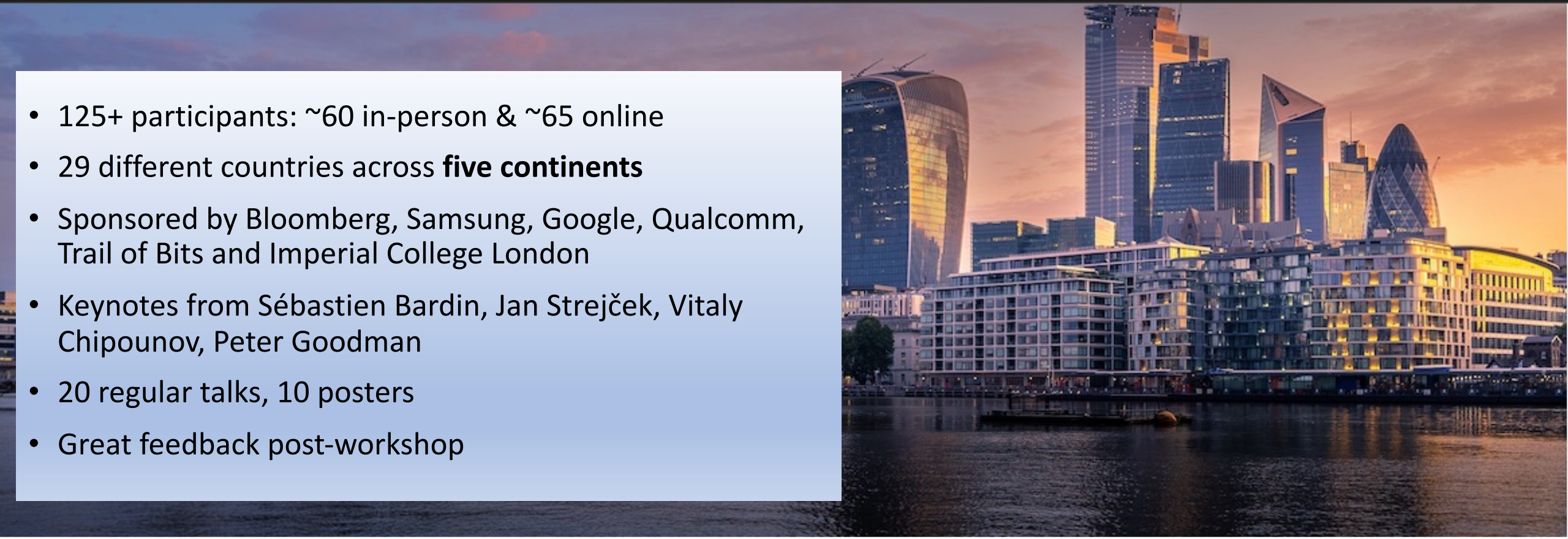
10-11 June, 2021 • Online

Tweets by @kleesymex

kleesymex Retweeted

KLEE Workshop 2022

Program ▾ Attending ▾ Call for Contributions ▾ Organisation Sponsors Venue ▾ Series ▾



- 125+ participants: ~60 in-person & ~65 online
- 29 different countries across **five continents**
- Sponsored by Bloomberg, Samsung, Google, Qualcomm, Trail of Bits and Imperial College London
- Keynotes from Sébastien Bardin, Jan Strejček, Vitaly Chipounov, Peter Goodman
- 20 regular talks, 10 posters
- Great feedback post-workshop

3rd International KLEE Workshop on Symbolic Execution

15–16 September 2022 • London, UK and Online

Tweets from @kleesymex

kleesymex
@kleesymex · Sep 7

KLEE Workshop 2024

Program Attending Call for Contributions Organisation Sponsors Series

4th International KLEE Workshop on Symbolic Execution

15–16 April 2024 • Lisbon, Portugal • Co-located with ICSE 2024

In-person, co-located with ICSE

- In-person workshop
- First time co-located with a conference

- Trade-offs:
  + Co-located with ICSE and other events
  + Facilitates and minimizes travel
  + Reaches out to a different region
  + Benefits from the conferences' organization infrastructure
  – High price difference £50/day vs €150-250/day
  – Tied to a single community
- Looking forward to your feedback at the end of the workshop

Participants

- 68 registrations
- From 17 different countries across 5 continents
- Good mix of academia, industry and research labs
  - Around 60% academia, 40% industry/research labs/government
  - Similar mix to previous workshops
- More registrations than participants:
  - Several people could unfortunately not get a visa on time
  - Some people are also attending other concurrent events

Program

Three keynotes: 1 from academia, 1 from industry, 1 mixed

- **Tevfik Bultan (**UCSB)
- **Tomasz Kuchta**, (Samsung)
- **Corina Pasareanu** (NASA Ames and CMU)

Program (cont.)

- 20 regular presentations, grouped into 7 sessions
- 7 posters, presented in a poster sessions and in the lunch area

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

Recording

The workshop is 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 (see https://klee-se.org/publications/)

Talk Format

- Each talk has a 22-minute slot
  - 16 minutes for the talk itself
  - 6 minutes for Q&A and switch-over
- Each poster has a 5-minute presentation slot
  - No Q&A but posters will be displayed in the lunch area
- All presentations (except keynotes) will be displayed from a single machine, to minimise switch-over time

Sessions and Session Chairs

MONDAY

1. State Merging & Posters: Alessandro Orso
2. Grammars, Concurrency, Mocking & Constraints: Abhik Roychoudhury
3. Binary Analysis: Daniel Schemmel

TUESDAY

4. Test Input Generation: Sergey Mechtaev
5. Program Repair: Martin Nowack
6. Taming Path Explosion and Non-determinism: Frank Busse
7. Coverage and Memory Errors: Julien Vanegue

Session chairs will be assisted by Daniel, Frank or Martin with the slides setup

Q&A

Ask lots of questions during the workshop!

- That's one of the main reasons for having the workshop in the first place!

Protocol:

- Just raise your hand to ask a question
- Session chair or speaker should repeat it before answering it

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

https://discord.gg/5MrmZ9TN

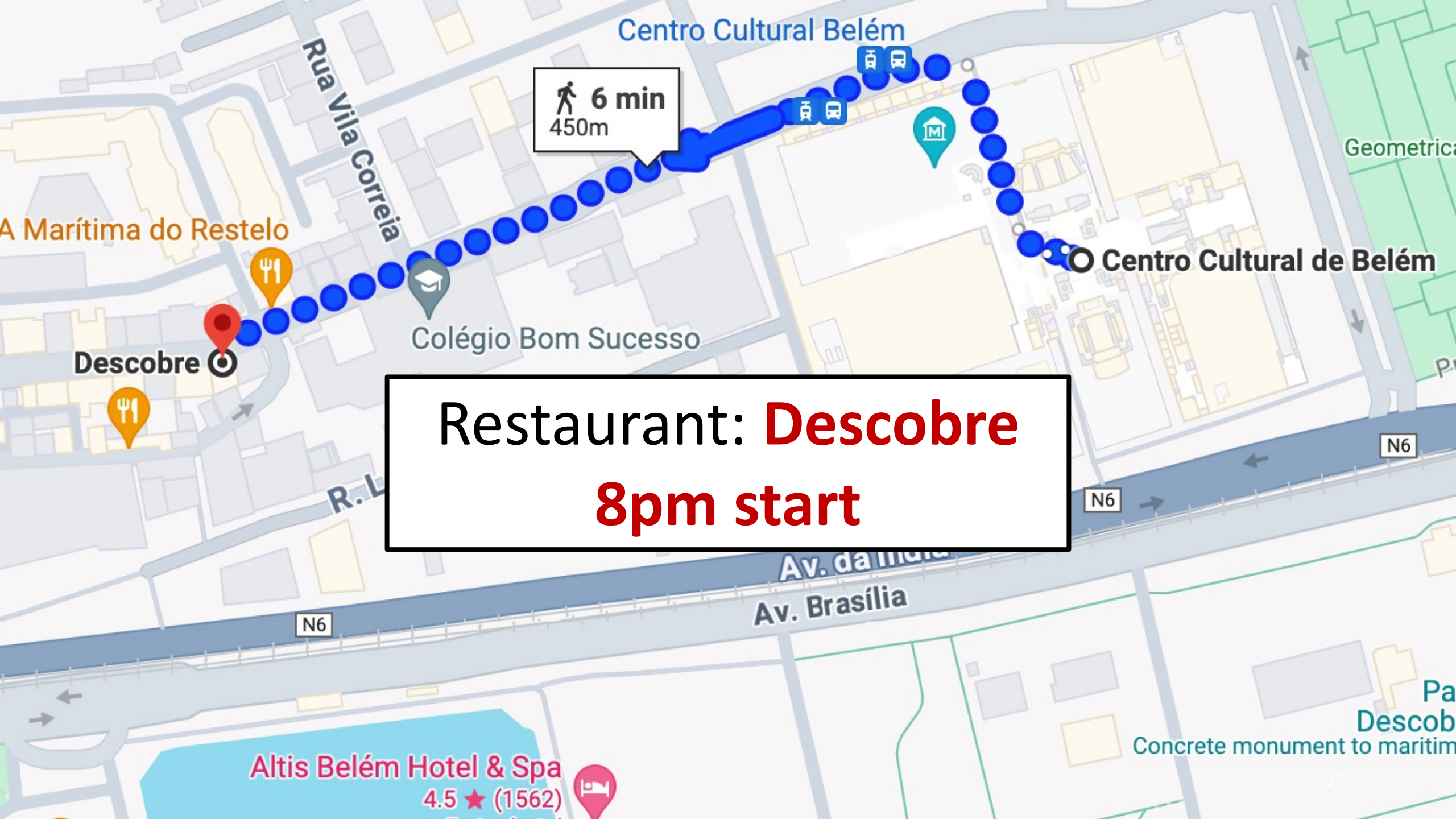
KLEE T-Shirts and Stickers

- If you haven't picked up a KLEE T-shirt, see us during the lunch break
- If you have requested a specific size via the survey, tell us
- Otherwise, we hope we still have your size left
- We should still have plenty of stickers left

KLEE Workshop Dinner

- If you haven't filled out the survey and would still like to join for dinner, see us ASAP
- We have a few places left, but you might not get your preferred menu choices
- We will do our best to call the restaurant and accommodate a few more people, but we cannot guarantee they still have space or food

From www.descobre.com.pt/



Restaurant: **Descobre**

8pm start

Gold sponsors

Bloomberg

SAMSUNG

Supported by

Association for Computing Machinery

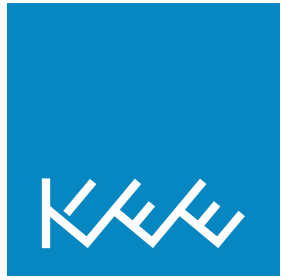
SIGSOFT

IEEE COMPUTER SOCIETY

IEEE

IEEE COMPUTER SOCIETY TCSE

Technical Committee on Software Engineering



4th International KLEE Workshop on Symbolic Execution

Thank You

To Our Sponsors

https://srg.doc.ic.ac.uk/klee24/

@kleesymex

Workshop Co-chairs

Big thanks to the ICSE'24 organisers, particularly:

- Rui Abreu
- José Borralho
- Gunel Jahangirova

Frank Busse

Martin Nowack

Daniel Schemmel

KLEE Community

- Martin Nowack for co-maintaining KLEE for the last many years
- Frank Busse for maintaining KLEE and the list of publications and systems building upon KLEE (now at 286)
- Prior co-maintainers Daniel Liew, Andrea Mattavelli and Daniel Dunbar
- Daniel Dunbar for starting the project back in'07!
- Our 100+ contributors to KLEE and its subprojects
- The entire awesome symex community

KLEE Workshop 2024

Program Attending Call for Contributions Organisation Sponsors Series

4th International KLEE Workshop on Symbolic Execution

15–16 April 2024 • Lisbon, Portugal • Co-located with ICSE 2024