

Qiuchen Yan

<http://www-users.cs.umn.edu/~yanxx297/>

Email : yanxx297@umn.edu

Mobile : +1-651-235-4138

EDUCATION

University of Minnesota, Twin Cities

Ph.D. in Computer Science; GPA: 3.60

Master of Science in Computer Science; GPA: 3.625

Minneapolis, MN

May 2014 – 2019(anticipated)

Sep. 2012 – May 2014

Shandong University of Science and Technology

Bachelor of Engineering in Computer Science; GPA: 3.65

Qingdao, China

Sep. 2008 – July 2012

PROJECTS

Fast PokeEMU

Improve the performance of PokeEMU, an automatic emulator testing tool based on FuzzBALL and KemuFuzzer.

- Modify the assembly test generator of PokeEMU for better performance.
- Port KemuFuzzer to various versions of QEMU.

Loop Summarization

Implement loop summarization algorithm on FuzzBALL. This project is supported by a grant under DARPA Cyber Grand Challenge program.

- As a countermeasure against path explosion, implement a trace based loop summarization algorithm on FuzzBALL, a symbolic execution engine written in Ocaml. The algorithm is described in “Automatic Partial Loop Summarization in Dynamic Test Generation”(ISSTA 2011)
- Build CFG dynamically.
- Evaluate the loop summarization algorithm using competition binaries from DARPA Cyber Grand Challenge

Type Inference

Infer the signedness of variables using static binary analysis.

- Disassemble binaries and translate to Vine IR.
- Generate CFG based on Vine IR.
- Access debug information using libdwarf.
- Based on debug information other than variable types, infer whether the variables are signed or unsigned using minimum cut.

ONGOING WORK

Fast PokeEMU: Scaling Generated Instruction Tests Using State Chaining

Qiuchen Yan, Stephen McCamant

Paper in preparation for submission to VEE 2018

Automatic Emulator Testing Made Faster

Qiuchen Yan, Stephen McCamant

Poster presented at University of Minnesota CS&Es Eleventh Biennial Research Showcase & Open House

TECHNICAL REPORT

Conservative Signed/Unsigned Type Inference for Binaries using Minimum Cut

Qiuchen Yan, Stephen McCamant

EXPERIENCE

DARPA Cyber Grand Challenge

In addition to the loop summarization project, contributed code for FuzzBOMB group in CGC Qualification Event.

PROGRAMMING SKILLS

Languages: C++, Python, Ocaml, X86 assembly, Javascript, PHP, SQL

Systems: Linux, Xed, DWARF, Vine