Qiuchen Yan

http://www-users.cs.umn.edu/∼yanxx297/

Email : yanxx297@umn.edu
Mobile : +1-651-235-4138

Education

University of Minnesota, Twin Cities — Minneapolis, MN
Ph.D. in Computer Science; GPA: 3.60 — *May 2014 – 2019 (anticipated)*
Master of Science in Computer Science; GPA: 3.625 — *Sep. 2012 – May 2014*

Shandong University of Science and Technology — Qingdao, China
Bachelor of Engineering in Computer Science; GPA: 3.65 — *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, I 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 SSA form Vine IR.
- Parse debug information using libdwarf.
- Based on heuristics and debug information other than variable types, infer whether the variables are signed or unsigned using minimum cut.

Publication

Qiuchen Yan, Stephen McCamant, "Fast PokeEMU: Scaling Generated Instruction Tests Using Aggregation and State Chaining" The 14th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE'18)

Qiuchen Yan, Stephen McCamant, "Conservative Signed/Unsigned Type Inference for Binaries using Minimum Cut" Technical report

Qiuchen Yan, Stephen McCamant, "Automatic Emulator Testing Made Faster" Poster presented at University of Minnesota CS&E's Eleventh Biennial Research Showcase & Open House

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