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
PhD of Science 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

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 libdward.
- Based on debug information other than variable types, infer whether the variables are signed or unsigned using minimum cut.

Loop Summarization

Implement loop summarization algorithm on FuzzBALL

- 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
- Build CFG dynamically.
- Evaluate the loop summarization algorithm using competition binaries from DARPA Cyber Grand Challenge

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.

Publications Under Submission

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

Fast PokeEMU: Scaling Generated Instruction Tests Using State Chaining
Qiuchen Yan, Stephen McCamant

Experience

University of Minnesota — Minneapolis, MN
Research Assistant — *Sep 2014 - Present*

Programming Skills

Languages: C++, Python, Ocaml, Assembly, Javascript, PHP, SQL

Systems: Linux, Xed, DWARF, Vine