Qiuchen Yan

https://www-users.cs.umn.edu/~yanxx297/ Email: yanxx297@umn.edu
https://github.com/yanxx297 Mobile: +1-651-235-4138

EDUCATION

University of Minnesota, Twin Cities Minneapolis, MN
Ph.D. in Computer Science, GPA 3.60 Sep. 2014 – May 2021 (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

SKILLS

Programming Languages: C/C++, Python, OCaml, Java, X86 assembly
Systems & Tools: FuzzBALL, S2E, Intel Xed, DWARF, VEX, Git, QEMU

RESEARCH PROJECTS

Linux Kernel Vulnerability Verification by Symbolic Execution 2018 – present
Build a hybrid verification system with Syzkaller and symbolic execution tool.
- Explored Linux kernel with symbolic execution tools (S2E and FuzzBALL.)
- Implement new features (tracing, constraints optimization) for S2E

Loop Summarization for Symbolic Execution 2014 – 2015, 2018 – present
Implemented new features in FuzzBALL (symbolic execution tool based on Valgrind front end) to replace loops with polynomials whenever feasible. 3000 lines of OCaml code.

Fast & Automatic Emulator Testing System 2015 – 2018
Improved the performance of an automated CPU emulator testing system.
- Modified the x86 assembly test generator to create test aggregations (multiple tests and code to save outputs and reset state for all tests.) 3000 lines of Python code. Decode tested instructions by Intel Xed.
- Tested 39,685 historical versions of QEMU, 200 times faster.

Binary Level Type Inference by Static Analysis 2013 – 2014
Built a static signedness inference system that achieves 96% true positive rate on GNU core utilities.
- Translated binaries to data flow graphs in static single assignment form, and divide it to signed and unsigned parts based on data flow and heuristics.
- Built with Valgrind front end and libdwarf. 10,000 lines of C/C++ code.

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

COURSE PROJECTS

Reproduce the Lucky Thirteen attack 2014
Implemented a timing side channel attack to the TLS protocol. C, Shell script, POSIX.

Sybil attack study 2014
Surveyed about the Sybil attack in online social network and its state-of-art defense approaches, and collected data from real world Sybil communities in Sina Weibo. Weibo API for C/C++.

Encrypted address book for Android 2012
Designed and implemented an Android address book app that can send encrypted contact info via text message. Java(back-end), XML(front-end.)

SERVICE

- Presented my work on The 14th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE’18)
- Guest lectures on security related courses at the University of Minnesota.
- Co-advised an undergraduate student on a relevant project