Qiuchen Yan

http://www-users.cs.umn.edu/∼yanxx297/
https://github.com/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 – 2020 (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*

Research Projects

Fast & Automatic Emulator Testing System — 2015 – 2018

- Speed up an automatic emulator testing tool by 200 times by designing and implementing a novel approach to generate test cases.
- Write Python code that generate x86 assembly test cases. Also modified other components of the testing system written in C++.

Loop Summarization for Symbolic Execution — 2014 – 2015, 2018 – present

- As a countermeasure of the path explosion problem, design a extended version of a trace-based loop summarization algorithm[1] and implement it on FuzzBALL, a symbolic execution platform.
- Still under progress. Currently consists of approximately 1300 lines of code in OCaml.

Binary Level Type Inference — 2013 – 2014

- Design a binary level type inference tool that can infer the signedness of variables with 96% true positive.
- Build this tool on top of Vine and libdwarf using C++.

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, "Fast PokeEMU: Scaling Generated Instruction Tests Using Aggregation and State Chaining," Poster

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

Experience

Graduate Research Asistant, University of Minnesota — 2014 – present

Work with Stephen McCamant on several research projects. Collaborate with Pen-Chung Yew's dynamic binary translation group on the emulator testing project.

DARPA Cyber Grand Challenge — 2014 – 2015

Contributed bug checking code for FuzzBOMB group in CGC Qualification Event.

Skills

Programming Languages: C/C++, Python, OCaml, X86 assembly, Javascript, PHP, SQL

Systems & Tools: Linux, Xed (Intel Pin), DWARF, Vine, FuzzBALL

Version Control System: Git

Coursework

Introduction to Computer Security: A breadth of knowledge about software security and network security

Modern Cryptography: Introduction to widely used cryptography theories and algorithms

Machine Learning: Introduction to machine learning

Security and Privacy in Computing: A seminar discussing recent papers about security, privacy and cryptography

Academic Projects

Reproduce the Lucky Thirteen attack 2014

Implemented a timing side channel attack to the TLS protocol. Course project.

Sybil attack study 2014

Surveyed about the Sybil attack in online social network and its state-of-art defence approach and collected data from real world sybil communities in sina weibo. Course project.

Encrypted address book 2012

An Android address book app that can send encrypted contact info via text message. Bachelor final project.

Service

- Contribut code to FuzzBALL, an open source symbolic execution tool.
- Gave guest lectures on security related courses at the University of Minnesota.

References

[1] Patrice Godefroid and Daniel Luchaup. Automatic partial loop summarization in dynamic test generation. In *Proceedings of the 2011 International Symposium on Software Testing and Analysis*, ISSTA '11, pages 23–33, New York, NY, USA, 2011. ACM.