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 2015 – 2018

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

- Modify the automatic test case generator of PokeEMU for better performance.
- Evaluate the improved PokeEMU by testing different versions of QEMU.

Loop Summarization for Symbolic Execution 2014 – present

Implement loop summarization algorithm on FuzzBALL as a countermeasure of the path explosion problem. This project is supported by a grant under DARPA Cyber Grand Challenge program.

- Implement a trace-based loop summarization algorithm on FuzzBALL, a symbolic execution engine written in OCaml. The original algorithm is described in “Automatic Partial Loop Summarization in Dynamic Test Generation” (ISSTA 2011)
- Evaluate the loop summarization algorithm using competition binaries from DARPA Cyber Grand Challenge

Binary Based Type Inference 2013 – 2014

Based on heuristics and debug information except variable types, infer whether the variables are signed or unsigned by computing the minimum cut of the data flow graph between the signed region and the unsigned region.

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

In addition to the loop summarization project, contributed 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

- Contributed to open source projects (FuzzBALL and PyXed.)
- Gave guest lectures on security related courses at the University of Minnesota.