Boyou Zhou

Security Researcher

- bobzhou@bu.edu
- +EMAIL-TO-ASK
- cv.boyouz.com
- linkedin.com/in/boyou-zhou-87272480
- github.com/byzhou
- @byzhou41

Education

PhD in Computer Engineering

Boston University

2013 - 2019

BSc in Communication Engineering

Southeast University

2009 - 2013

Languages

- Chinese (Native)
- English (Professional)

Interests

- Hiking
- Swimming
- Cooking

Career Profile

Summary I am a Ph.D Student in Integrated Circuits & System Group of Electrical and Computer Engineering in Boston University. My research interests are Computer System Security. My target graduation time is Jan 2019.

Experiences

Research Assistant

2013 - Present

Boston University

Current research work I am currently working on the hardware-assisted Control Flow Integrity (CFI). CFI enforce the program execution path consistent with the static analytical results, which provides protection for the programs from attacks like ROP (Return-oriented Programming). We focus on the RISCV evaluation platform to engineer CFI components for research community.

Internship

2016

Qualcomm

Internship work I implemented a Digital Signal Processing Module in the chip design. I modeled my signal processing in Python with the builder design pattern. My model brought the flexibility into parameter changing and future developments. In addition to designing the models, I also provided the websites for documenting the tools during the developments. Meanwhile, I designed a tool for Verilog automatic connection using Python and other scripting languages.

Internship

2014,2015

Analog Devices Inc.

Internship work I mainly explored the Real Number Modeling in chip modeling and also board module modeling. I used Verilog, Verilog-ams, and SystemVerilog to module the current and voltage behaviors.

Projects

My past projects and related publications During my $5\ ^1/_4$ year graduate school years, I have worked on a variety of projects related to security system design. Below is the listed work and publications.

Hardware Performance Counter Malware Detection - **BEST PAPER in AsiaCCS 2018** To evaluate the feasibility of malware detection using Hardware Performance Counters (HPC), I measured the HPC traces on programs and malware, including 1k malware and 1k benignware. To perform the measurements,

I use Rabbitmq to orchestra the commnunications in a cluster of machines. I performed data analysis on these HPC values using various machine learning algorithms, such as K Nearest Neighbors (KNN), Decision Tree (DT), Multilayer Perceptrons (MLP), Naive Bayes, AdaBoost and Random Forest (RF). By applying these machine learning algorithms, I evaluated the robustness of malware detection using these algorithms in cross-validations.

Gate Classification Through Near-IR Imaging - We propose optical backside imaging in Hardware Trojan Detection. We engineer optical structures in standard cells to expose different response in various gates. These response functions as the feature vectors for distinguish different gates. After the fabrication, we use machine learning algorithms to classify among different gates. Any modifications or replacement to these cells can be easily detected through optical imaging.

Hardware Assisted Encryption Acceleration - I implemented AES, RSA, SHA cryptographic algorithms on FPGA and measured the speed of calculations.

Skills & Proficiency

Python

C/C++

Verilog/Verilog-ams/System-Verilog

HTML & JAVASCRIPT & CSS

Bash & Perl & Any Other Scripting