Shenglong YAO

Tel: +852-46409081 / Email: shenglyao2-c@my.cityu.edu.hk

GitHub: https://github.com/James-yaoshenglong / Personal Website: https://james-yaoshenglong.github.io/home

Education Background

City University of Hong Kong

Bachelor of Science in Computer Science Expected May 2023

- Major GPA: **4.20/4.3**, CGPA: **4.08/4.3**
- HKSAR Government Scholarship (4 quota per year for whole CS Department)
- Dean's List of College of Engineering 2019-2020 SemA, 2019-2020 SemB, 2020-2021 SemA, 2020-2021 SemB

Research Experience

Front-end Secure Framework against Malicious Browser Extensions Dec 2021~ Present

- Research Area: Browser Security, Front-end Security
- Motivation and Contribution
  - Browser extension introduces potential risks due to escalated privileges
  - Assuming security of browser sandbox and untrusting browser extension and web content from the Internet
  - Providing a front-end secure framework to mitigate potential attack from malicious browser extension and unauthorized privacy API access
  - Enhancing our solution's compatibility to popular front-end framework like Vue and reducing its deployment cost in development process
  - Potential front-end encryption integration with end-to-end privacy survey platform
- Role in the Research: Project Member
  - Deploying our WebEnclave solution to front-end framework like Vue
  - Seeking potential extension of WebEnclave to defense other data leak channels such as UI Spoofing and clipboard hijacking
  - Designing better authorization mechanism to authorize user trusted extensions

Fuzzing Evaluation Benchmark and Selection Guideline Aug 2021~ Present

- Research Area: Fuzzing, Bug Detection Analysis
- Motivation and Corresponding Contribution
  - Current fuzzing benchmark methods do not well consider the difficulty difference between different bugs fuzzed, which is an important metric nevertheless
  1. Providing a novel bug construction and insertion method to construct a fair ground-truth corpora of bugged program with diverse bug difficulty
  2. Evaluating various fuzzing methods with the corpora according to our self-defined evaluation difficulty metrics for exploration and exploitation
  - Current fuzzing benchmark methods cannot provide a selection guideline for different targets to fuzzing
  1. Providing a guideline of fuzzing method selection for different application scenario according to our evaluation metrics
- Role in the Research: Collaborator
  - Designing and implementing the bug insertion and corpora construction process with dynamic program analysis and compile-time bug insertion
  - Defining reasonable metrics for evaluating exploitation difficulty of a bug
  - Evaluating various fuzzing methods by experiments with constructed corpora

App Novel Problem Detection from App Review Jun 2020~Jun 2021

- Under Research Mentoring Scheme of CS Department, Supervised by Dr. Jacky KEUNG
- Research Area: Nature Language Processing, Topic Modeling

- Motivation and Contribution
    - App reviews are important for developers to detect novel problems in App
    - Manual inspection of thousands of App reviews is labor-intensive
    - Provided an improved automated framework based on TF-IDF Text Model and BTM Topic Modeling to detecting novel problems from app reviews with better performance
- Role in the Research: Project Principal

Work Experience

Full Time Research / Technical Assistant

Department of Computer Science, City University of Hong Kong Jul 2021~Present

- Supervised by Prof. Cong WANG
- Participating in the research projects mentioned previously
- Working as the **team leader** of **CITYFHK CTF Team**
    - Organized CITYF 21 CTF competition of City University (question setting, platform deployment and management)
    - Leaded the team to get Rank 6 in PwC's HackaDay 2021
    - Leaded the team to get Rank 9 in Tertiary Institution Category of Hong Kong Cyber Security New Generation Capture the Flag (CTF) Challenge 2021

Selected Courses

Cybersecurity Courses

- CS4293: Topics on Computer Security (ongoing)
- CS4296: Cloud Computing (ongoing)
- Software Analysis (ongoing, provided by Peking University Online)
- GE2338: Internet Applications and Security (A+)
- Cybersecurity Infrastructure Configuration (Certificate of Completion, provided by Palo Alto Networks Academy)

Artificial Intelligence Courses

- CS4186: Computer Vision and Image Processing (ongoing)
- Machine Learning (Completion, instructed by Andrew Ng on Coursera)

Computer Science Core Courses

- CS2115: Computer Organization (A+)
- CS3103: Operating System (A+)
- CS3201: Computer Networks (A+)
- CS3402: Database Systems (A+)
- CS4335: Design and Analysis of Algorithms (A+)

Extracurricular Activities

AWS Educate Student Ambassador

1st batch of AWS Educate Student Ambassadors in Hong Kong Jan 2022~Present

- Learning the AWS Cloud Fluency Course of AWS Educate
- Promoting AWS Service to university students

Skills & Qualification

- **Programming Language**: C/C++, Java, Python, JavaScript
- **Hacking**: Master proficient skills in binary exploitation (PWN) and web hacking
- **Back-end Operation**: Good Knowledge of Linux, Cloud Computing and Server / Container Management
- **Artificial Intelligence**: Good knowledge of Machine Learning and Deep Learning, Competition experience in data wrangling and model training
- **ML & Security**: Knowledge in Machine Learning Robustness and Adversarial Attack
- **Program Analysis**: Skills in common static and dynamic software analysis tools such as Intel Pin and LLVM

References

Prof. Cong, Wang

Professor, IEEE Fellow
Department of Computer Science, City University of Hong Kong
Phone: +852 34422010
E-mail: congwang@cityu.edu.hk
Prof. Wang is my current research supervisor of my research assistant position at Department of Computer Science, City University of Hong Kong