SUHWAN SONG / Ph.D Student

Dept. of Electrical and Computer Engineering
Seoul National University
South Korea

Phone: (+82) 10-3093-8556 | Mail: sshkeb96@snu.ac.kr | Lab: CompSec at SNU

ABOUT ME

I have extensive experience in software testing and security. I led **CrFuzz**, uncovering 272 vulnerabilities in major open-source projects such as FFmpeg and Ghostscript, and developed **R2Z2**, which identified 34 rendering bugs in Chrome and is now used internally by Google's Chrome team. During the Google Ph.D internship, I productized a tool to find rendering regression bugs in Chrome automatically and the tool is currently used internally by Chrome rendering team. I subsequently led **Metamong**, detecting 19 render-update bugs in Chrome and Firefox, and I am currently researching iframe vulnerabilities, having discovered 5 new browser security issues.

RESEARCH INTERESTS

I am interested in **software engineering** and **computer security** in general. In particular, my research focus is in **software testing**, e.g., fuzzing systems to find software bugs.

PUBLICATIONS

- **Metamong: Detecting Render-update Bugs in Web Browsers through Fuzzing**
  Suhwan Song, and Byoungyoung Lee
  ACM Symposium on the Foundations of Software Engineering (FSE) 2023

- **R2Z2: Detecting Rendering Regressions in Web Browsers through Differential Fuzz Testing**
  Suhwan Song, Jaewon Hur, Sunwoo Kim, Philip Rogers, and Byoungyoung Lee
  IEEE/ACM International Conference on Software Engineering (ICSE) 2022

- **SpecDoctor: Differential Fuzz Testing to Find Transient Execution Vulnerabilities**
  Jaewon Hur, Suhwan Song, Sunwoo Kim, and Byoungyoung Lee
  ACM Conference on Computer and Communications Security (CCS) 2022

- **FuzzOrigin: Detecting UXSS vulnerabilities in Browsers through Origin Fuzzing**
  Sunwoo Kim, Young Min Kim, Jaewon Hur, Suhwan Song, Gwangmu Lee, and Byoungyoung Lee
  USENIX Security Symposium (Security) 2022

- **DifuzzRTL: Differential Fuzz Testing to Find CPU Bugs**
  Jaewon Hur, Suhwan Song, Dongup Kwon, Eunjin Baek, Jangwoo Kim, and Byoungyoung Lee
  IEEE Symposium on Security and Privacy (SP) 2021

- **CrFuzz: Fuzzing Multi-Purpose Programs through Input Validation**
  Suhwan Song, Chengyu Song, Yeongjin Jang, and Byoungyoung Lee
  ACM Symposium on the Foundations of Software Engineering (FSE) 2020

EXPERIENCE

- **Google, Chrome Rendering Team, San Francisco, CA (May 2022 - August 2022)**
  Sofware Engineerning Intern: finding rendering regression bugs in Chrome
  Mentor: Philip Rogers

INVITED TALK

- **Towards Reliable Computer Systems with Fuzz and Differential Testing**
  UNIST. Apr 16, 2025

- **Google Tech Talk: Finding Rendering Bugs in Browsers**
  Virtual meeting hosted by Google. Aug 12, 2020

PROJECTS

Development of an Automotive Security Vulnerability-based Threat Analysis System Mar 2024 – Current
South Korean Ministry of Trade, Industry and Energy (MOTIE)

- Improving test coverage collection latency and data encryption performance for automotive threat analysis.
- Target: Electronic Control Unit (ECU) in automotive systems

Finding regression rendering bugs in Chrome [Internship] May 2022 – Aug 2022
Google

- Productionize a tool to automatically find rendering regression bugs in Chrome before users are affected
- Target: Chrome browser

Research on library fuzzing input vector extension Feb 2021 – Dec 2021
SAMSUNG Research, Samsung Electronics Co., Ltd.

- Design a fuzzer which addresses an insufficient execution environment in library fuzzing
- Target: Samsung Tizen library

Research on fuzzing performance enhancement using deep learning Jan 2019 – Sep 2020
Agency for Defense Development (ADD)

- Design a fuzzer which can explore the higher code coverage than AFL
- Target: C/C++ open-sourced software programs

REPORTED VULNERABILITIES (SELECTED)

CVE-2022-4025: [$3000] Chrome: the contents of iframe is placed outside of iframe when CSS “column-width” is defined in main frame.

CVE-2023-7281: [$1000] Chrome: Chromium illegally paints outside of iframe when using -webkit-box-reflect.

CVE-2023-7013: Chrome: Chromium illegally paints outside of iframe when using -webkit-box-reflect.

CVE-2022-28286: [$500] Firefox: Firefox incorrectly draws outside of iframe because table cell contents overflow table bounds.

CVE-2022-45420: [$500] Firefox: iframe contents can be arbitrarily drawn outside of iframe due to wrong stacking context.

EDUCATION

Seoul National University Mar 2019 - Present
Seoul, South Korea

Ph.D. in Electrical and Computer Engineering (Advisor: Byoungyoug Lee)

Pusan National University Mar 2015 - Feb 2019
Busan, South Korea

B.S. Electrical and Computer Engineering

TEACHING ASSISTANT

Programming Methodology (430.211) Spring 2025
Seoul National University

Systems Programming Spring 2022, Spring 2023
Samsung Electronics Co., Ltd.

System Programming (430.658) Fall 2022
Seoul National University

Cyber Security and Blockchain (M2177.006300) Spring 2020, Fall 2020, Fall 2021, Fall 2022
Seoul National University

Introduction to Data Structures (430.217) Fall 2020, Spring 2021
Seoul National University