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 | Homepage: link | Lab: CompSec at SNU

About Me

I'm proficient in Python and C languages. I led and developed R2Z2 project that automatically has discovered 34 new rendering bugs in Chromium browser. I was recruited as a software engineering intern at **Google** in 2022 summer through R2Z2 project. During the 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 led and developed CrFuzz project for finding 272 new vulnerabilities in popular open-source programs including FFmpeg and Ghostscript. I'm leading the "Iframe-based Attack through Rendering Bug" project that has proposed **a new type of vulnerability** in browsers and found 3 new vulnerabilities in Chrome and Firefox.

Research Interests

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

Experience

- **Google, Chrome Rendering Team**, San Francisco, CA (May 2022 - August 2022)

  Sofware Engineerning Intern: finding rendering regression bugs in Chrome
  Mentor: Philip Rogers

Publications

- **SpecDoctor: Differential Fuzz Testing to Find Transient Execution Vulnerabilities**

  Jaewon Hur, Suhwan Song, Sunwoo Kim, and Byoungyoung Lee
  In Proceedings of the 2022 ACM SIGSAC 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
  In 31st USENIX Security Symposium (SEC), Aug 2022

- **R2Z2: Detecting Rendering Regressions in Web Browsers through Differential Fuzz Testing**

  Suhwan Song, Jaewon Hur, Sunwoo Kim, Philip Rogers, and Byoungyoung Lee
  In Proceedings of the 44th International Conference on Software Engineering (ICSE), Aug 2022

- **DifuzzRTL: Differential Fuzz Testing to Find CPU Bugs**

  Jaewon Hur, Suhwan Song, Dongup Kwon, Eunjin Baek, Jangwoo Kim, and Byoungyoung Lee
  In 2021 IEEE Symposium on Security and Privacy (SP), Aug 2021

- **CrFuzz: Fuzzing Multi-Purpose Programs through Input Validation**

  Suhwan Song, Chengyu Song, Yeongjin Jang, and Byoungyoung Lee
  In Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (FSE), Aug 2020

Invited Talk

- **Google Tech Talk: Finding Rendering Bugs in Browsers** [video]

  Presenter: Suhwan Song
  Virtual meeting hosted by Google. Aug 12, 2020

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-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.

Projects

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

Education

Seoul National University Mar 2019 - Present
Seoul, South Korea

M.S/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

Technical Skills

Languages

- *Knowledgeable:* C, Python
- *Have an experience with:* C++, Go