Navid Emamdoost

(+1) 612-666-7976 | emamd001@umn.edu | Linkedin | github.com/Navidem

Work Experience

Google | Software Engineer | *Sunnyvale, CA, USA* Sep 2021, Present

- **OSS-Fuzz and ClusterFuzz Maintainer**
  Provided cloud-based fuzzing infrastructure for over 800 critical open source projects. Implemented new features like crash deduplication and supporting new fuzzing engines. Wrote new fuzzers to increase code coverage and find new bugs.
- **FuzzIntrospector Engineering Lead**
  Developed various static and dynamic code analysis techniques to evaluate the fuzzing performance and provide automated suggestions to improve the fuzzer. Integrated the FuzzIntrospector with OSS-Fuzz to improve fuzzing for hundreds of open source projects.
- **Centipede Developer**
  Implemented a new corpus prioritization approach using static code analysis to increase fuzzing coverage. Implemented a new feature for **LLVM SanitizerCoverage** to instrument the binary and extract control-flow and call graphs.

Mozilla | Software Engineer Intern | *Portland, OR, USA* Summer 2018

- **Bringing Dynamic Loading into WebAssembly**
  Designed and implemented a dynamic loading library for a **Rust** project targeting **WebAssembly**.

TruScribe | Software Engineer Intern | *Minneapolis, MN, USA* Summer 2016

- **Developing Animation Generation Software**
  Added new features like video in-lining, image background, text and image overlay to the animation generation software using **ffmpeg** library.

Research Projects

University of Minnesota | Research Assistant | *Minneapolis, MN, USA* Sep 2013 - Aug 2021

- **Automatic Semantic Error Detection in the Linux Kernel**
  Developed an **LLVM**-based static analysis tool to detect multiple classes of security bugs in the **Linux kernel** code. Found over **200** confirmed security bugs and received over **40 CVEs** for the detected vulnerabilities including **Use-After-Free**, **Null-Pointer-Dereference**, and **Memory-Leak**. Fixed the bugs by submitting patches to the Linux maintainers.
- **Software-based Fault Isolation**
  Improved runtime performance of Google Native Client (NaCl) by reducing instruction padding overhead. Changed the NaCl instruction padding in GNU **Assembler** (GAS), updated NaCl validator to enforce security policies, and proved the validator correctness in **Coq**.
- **Binary Mutation for Test Analysis**
  Evaluated the adequacy of a test suite, via **static binary rewriting**. The project demonstrated how binary mutation is effective in test quality measurement when no source-code or debugging information is available.

Education

PhD, Computer Science |*University of Minnesota* 2021

M.Sc, Computer Science |*University of Minnesota* 2016

Selected Publications

- **Navid Emamdoost**, Qiushi Wu, Kangjie Lu, and Stephen McCamant. "Detecting Kernel Memory Leaks in Specialized Modules with Ownership Reasoning" *in Proceedings of the 28th Network and Distributed System Security (NDSS) Symposium 2021.*
- Qiushi Wu, Aditya Pakki, **Navid Emamdoost**, Stephen McCamant, and Kangjie Lu. "Understanding and Detecting Disordered Error Handling with Precise Function Pairing" *To appear in Proceedings of the 30th USENIX Security Symposium (Security'21). Vancouver, Canada, August 2021.*

Technologies and Languages

- **Languages:** C, C++, Python, Rust, C#.
- **Technologies:** LLVM, Google Cloud Platform, Valgrind, OProfile, IDA Pro, PostgreSQL, MySQL.
- **Other:** Fuzzing, Symbolic Execution, Dataflow analysis, Malware Analysis.