Navid Emamdoost

(+1) 612-666-7976 | emamd001@umn.edu | LinkedIn | GitHub

Experience

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

- **Kernel Memory Management**
  Developed and maintained kernel **memory management** features to provide reliable, secure and cost-efficient kernel for Google infrastructure and Cloud.
- **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 for the **Centipede** fuzzing engine. Implemented a new feature for the **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**
  Implemented a dynamic loading library for **Rust** that allows any module to be exported to **WebAssembly** and then instantiated at runtime by a wasm binary. It liberated the wasm binary from having a copy of commonly used library routines.

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

- **Animation Generation Software**
  Implemented video in-lining, image background, and text/image overlay features using **ffmpeg**.

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**. Discovered over **200** vulnerabilities, including Use-After-Free, Null-Pointer-Dereference, and Memory Leaks, resulting in over **40 CVEs**. 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. Modified GNU **Assembler** and the NaCl validator to implement a more efficient instruction padding scheme, while ensuring security policy conformance. Formally proved the validator's correctness in **Coq**.
- **Binary Mutation for Test Analysis**
  Developed a **static binary rewriting** framework to implement binary mutation for comprehensive test suite assessment, demonstrating its feasibility in closed source applications.

Education

PhD, Computer Science |*University of Minnesota* 2021

Selected Publications

- **Navid Emamdoost**, Qiushi Wu, Kangjie Lu, and Stephen McCamant. "Detecting Kernel Memory Leaks in Specialized Modules with Ownership Reasoning" *Published in NDSS Symposium 2021.*
- Qiushi Wu, Aditya Pakki, **Navid Emamdoost**, Stephen McCamant, and Kangjie Lu. "Understanding and Detecting Disordered Error Handling with Precise Function Pairing" *Published in USENIX Security Symposium 2021.*

Technologies and Languages

- **Languages:** C, C++, Python, Rust, C#.
- **Technologies:** LLVM, Google Cloud Platform, Docker, Qemu, git, gcc, gdb, Valgrind, IDA, PostgreSQL, MySQL.
- **Other:** Fuzzing, Static Analysis, Symbolic Execution, Dataflow analysis, Malware Analysis.