Corban Villa

+1 (801) 380 6244 | corban.villa@nyu.edu | github.com/corbanvilla

Education

Computer Science, B.S., 3rd-Year, NYU Abu Dhabi

Relevant Courses: Network Security (graduate), Penetration Testing and Vulnerability Analysis, Computer Security, Operating Systems, Computer Systems Organization, Algorithms, Data Structures.

Technical Skills

Tools: GDB, Binary Ninja, PANDA.re, Wireshark, Git, Docker, Kubernetes, Ansible, VMWare, QEMU, Pandas, Fuzzbench.

Experience: Reading and generating LLVM Intermediate Representation (IR), running and evaluating fuzzers, modifying compilers, reverse-engineering assembly, conducting vulnerability assessments, attacking network protocols.

Programming Languages: Python, Rust, C/C++, TypeScript.

Work Experience

Research Assistant, Modern Microprocessors Architecture Lab — NYU Abu Dhabi (May 2023 - Current)

- Conducting research to evaluate the efficacy of modern fuzzers on Industrial Control System (ICS) applications, in order to improve overall security and reliability, under the direct supervision of Mihalis Maniatakos, PhD.
- Orchestrate project strategy and operations as the first author, in collaboration with other lab members.
- Modify a Rust-based compiler for ICS programs to add code coverage instrumentation, callbacks, better source navigation, and programmatically inject both bugs and memory taints (for dynamic analysis with PANDA.re).
- Leverage Fuzzbench and compiler described above to evaluate fuzzers on the widely used ICS libraries.
- Provide assessments of methodology, experimentation, and argumentation for paper proposals to top conferences during weekly lab review meetings.
- Assist lab researchers with paper writing, revisions, experiment configurations, and troubleshooting.

Research Assistant, Cyber Security and Privacy Lab — NYU Abu Dhabi (Apr. 2023 - Current)

- Conducting research to evaluate the security and privacy implications of Large Language Models (LLM), under the direct guidance of Program Head of Computer Science Christina Pöpper, PhD.
- Developed and conducted additional experiments on a recent paper, to evaluate how a blind membership inference (BlindMI) attack generalizes to LLMs featuring differing architectures (see Section 9).
- Collaborating with Christina Pöpper and her PhD candidates to develop a research project proposal for a directed study research class, investigating malicious advertisements in chatbots.

Blockchain Developer Intern — Owl Protocol (Dec. 2021 - Aug. 2022)

- Lead interns through smart contract development process, creating open-source libraries on Ethereum.
- Build smart contracts to decode CBOR (RFC 8949) and cryptographically verify data integrity via Merkle trees.

Software Engineer Intern — Zahlen Solutions (Contractor for HPE) (Jul. 2019 - Oct. 2021)

- Worked for Hewlett Packard Enterprise (HPE), communicating directly with project managers and software engineers to design, build and implement internal applications and APIs which aggregate customer data.
- Implemented log aggregation tools and filtering systems to alert on errors, security threats, and other issues.
- Reverse-engineered legacy black-box applications to enhance performance, reduce costs, and boost efficiency.

Projects

Senior Web Chief — The Gazelle (University Newspaper) (Aug. 2022 - Current)

- Spearheaded a team of Computer Science undergraduates to enhance server infrastructure and codebase.
- Mentored team members in learning and applying React, TypeScript, and MySQL for effective web development.
- Achieved a 90% reduction in infrastructure costs and 20x improvement for full-page load speed.