Corban Villa

(As of Apr 2, 2024)

Undergraduate Student
New York University Abu Dhabi
Computer Science and Cybersecurity

Contact
corban.villa@nyu.edu
corbanvilla.com

Research Interests
- Large Language Models privacy and security
- Industrial control system compilers and cybersecurity
- Reverse engineering and binary analysis

Education

New York University, Abu Dhabi Expected 2025
B.Sc. in Computer Science, minor in Mathematics

Professional Experience

Research Assistant Apr. 2023 - Present
Modern Microprocessors Architecture Lab
- Conducting research to evaluate the efficacy of modern fuzzers on Industrial Control System (ICS) applications, 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 May 2023 - Present
Cyber Security and Privacy Lab
- 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.

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