Corban Villa

(As of Aug 27, 2024)

Undergraduate Student and Researcher
Computer Science and Cybersecurity
New York University Abu Dhabi

Contact
+1 (801) 380-6244
corban.villa@nyu.edu

Personal Site · GitHub · LinkedIn

Research Interests

- Security & Privacy.
- Machine Learning Security.
- Critical Infrastructure Security.

Education

New York University Abu Dhabi Expected, May 2025
B.Sc. in Computer Science. Minor in Mathematics. GPA 3.8/4.

- Capstone: Investigating Attacks and Defenses Enabling Resilient O-RAN Deployments.

Professional Experience

Research Assistant May '23 - 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.

Research Assistant Apr. '23 - Present
Modern Microprocessors and 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.

Publications

Mapping and Bypassing of Safety Guardrails in Text-to-Image Models — USENIX '25 (Targeting)
Corban Villa, Shujaat Mirza, Christina Pöpper.

ICS-QUARTZ: Scan Cycle-Aware and Vendor-Agnostic Fuzzing for Industrial Control Systems — NDSS '25 (Round 2)
Corban Villa, Constantine Doumanidis, Hithem Lamri, Prashant Hari Narayan Rajput, Michail Maniatakos.

Media talks Privacy: Unraveling a Decade of Privacy Discourse around the World — PETS '24 (Published)
Shujaat Mirza, Corban Villa, Christina Pöpper.
- Awarded as the Andreas Pfitzmann Best Student Paper Runner-Up.

Research

CodexLeaks: Privacy Leaks from Code Generation Language Models in GitHub Copilot — USENIX '23 (Published)
Conducted experiments with StarCoder to evaluate the privacy implications of GitHub Copilot and other code generation models.

Community Service

PETS '25 Artifact Evaluator

SheCanML Workshop — April '24
Empower high school women through Machine Learning (ML). Introduce students to the basics of ML in an interactive and fun setting, uncovering exciting paths in tech and AI.

ACNS Volunteer — March '24
Volunteer to host the ACNS conference at NYU Abu Dhabi.

Container Security Workshop — Oct. '19
Saintcon 2019 Docker Security red-team and blue-team challenges.

Teaching & Mentorship

Cybersecurity Student Group — Aug. 2023 - Present
Introduced the first cybersecurity student interest group to promote interest in cybersecurity among students.

The Gazelle Web Chief — Aug. 2022 - Present
Leading a team of student developers for the student newspaper.

Private Programming Tutoring for Kids — Jun. 2023 - Present
Provide private tutoring ranging from programming games with scratch, encrypting messages with primitive ciphers, and intercepting messages with Wireshark.

Presentations

ICS-QUARTZ: Scan Cycle-Aware and Vendor-Agnostic Fuzzing for Industrial Control Systems — May '24
Center for Cyber Security (CCS): Cybersecurity Seminar Series, Abu Dhabi.

Vulnerabilities

CVE-2024-6876 — Reported April '24
Out-of-bounds memory vulnerability for open-source ICS library.