Corban Villa

(As of Jan 29, 2025)

Computer Science and Cybersecurity
New York University Abu Dhabi
Website · GitHub · LinkedIn

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

Education

08.21–Present **New York University Abu Dhabi** Expected, May '25.
B.Sc. in Computer Science. Minor in Applied Mathematics. GPA: 3.85/4.

- Capstone: Investigating Attacks and Defenses Enabling Resilient O-RAN. Advised by Christina Pöpper.

Research Experience

04.23–Present **Cyber Security and Privacy Lab, NYU Abu Dhabi**
Student Research Assistant
Advisor: Christina Pöpper

- **Directed Study:** Proposed and led investigation introducing novel timing side-channel and jailbreaking attacks in text-to-image (T2I) models. Publication at USENIX Security'25. Disclosed vulnerability to OpenAI.
- **Capstone Project:** Produced a comprehensive graph-based threat model, synthesized with related work, to evaluate the research potential of O-RAN cellular infrastructure.
- **Student Research:** Designed and conducted a user study (n=50) to evaluate machine translations of security-related news articles. Publication at PETS'24.
- **Student Research:** Constructed experiments to evaluate how membership inference attacks can be generalized to various code generation model architectures, thereby leaking user privacy details from the training corpus.

05.23–Present **Modern Microprocessors and Architecture Lab, NYU Abu Dhabi**
Student Research Assistant
Advisor: Michail Maniatakos

- **Directed Study:** Led investigation to introduce novel bug injection for Industrial Control System (ICS) software and used to compare state-of-the-art fuzzers.
- **Student Research:** Introduced an ICS fuzzer that outperforms state-of-the-art by 15× in executions per second, proposed scan cycle-aware fuzzing, and discovered a CVE. Modify Rust-based ICS compiler to introduce code coverage and address sanitizer for program fuzzing. Publication at NDSS'25. Disclosed CVE-2024-6876.
- **Student Research:** Designed a lab for the undergraduate System Security course, incorporating fuzzing ICS programs to reproduce and exploit a known vulnerability.

Presentations

09.24 **Exposing the Guardrails: Reverse-Engineering and Jailbreaking Safety Filters in DALL·E Text-to-Image Pipelines**
Center for Cyber Security: Cybersecurity Seminar Series, NYU Abu Dhabi.

05.24 **ICSQuartz: Scan Cycle-Aware and Vendor-Agnostic Fuzzing for ICS**
Center for Cyber Security: Cybersecurity Seminar Series, NYU Abu Dhabi.

10.18 **Bluetooth: From Basics to Vulnerabilities.**
Security Advisory and Incident Network Team Conference, USA.

Publications

USENIX'25 (A/R: 19%) **Exposing the Guardrails: Reverse-Engineering and Jailbreaking Safety Filters in DALL·E Text-to-Image Pipelines**
Corban Villa, Shujaat Mirza, Christina Pöpper.

NDSS'25 (A/R: 17%) **ICSQuartz: Scan Cycle-Aware and Vendor-Agnostic Fuzzing for Industrial Control Systems**
Corban Villa, Constantine Doumanidis, Hithem Lamri, Prashant H. N. Rajput, Michail Maniatakos.

PETS'24 (A/R: 21%) **Media talks Privacy: Unraveling a Decade of Privacy Discourse around the World**
Shujaat Mirza, **Corban Villa**, Christina Pöpper.
- Awarded as the Andreas Pfitzmann Best Student Paper Runner-Up.

Publications (In Preparation)

CCS'25 **SoK: Systematizing O-RAN Security: A Graph-Based Approach to Threat Mapping and Vulnerability Analysis**
Syed Khandker, **Corban Villa**, Evangelos Bitsikas, Aanjhan Ranganathan, Christina Pöpper.

CCS'25 **ICSBench: An LLM-Based Bug Injection Methodology for Evaluating Industrial Control System Fuzzers**
Corban Villa, Christoforos Vasilatos, Manaar Alam, Michail Maniatakos.

Vulnerability Disclosures

09.24 **Disclosed CVE-2024-6876**
Out-of-bounds read vulnerability for an Industrial Control System library.

Teaching & Mentorship

08.24–Present **Co-Founder of Cybersecurity CTF Group, NYU Abu Dhabi**
- Co-founded cybersecurity Capture the Flag (CTF) group to promote ethical hacking.
- Led hands-on workshops for reverse engineering and buffer overflow attacks.

06.23–Present **Private Programming Tutoring for Kids**
Provided technical tutoring, including introductory game programming with Scratch, encrypting messages with primitive ciphers, and intercepting messages with Wireshark.

04.24 **SheCanML Workshop**
Developed and led a ML workshop for 35 high school women to inspire interest in STEM.

Community Service

01.25 **Artifact Evaluator, Privacy Enhancing Technologies Symposium**

08.22–Present **Senior Web Chief, The Gazelle**
- Reduced infrastructure costs by over 90% while improving page load time by 10×.
- Mentored a team of undergraduates through web development processes, including Git, server operations, threat monitoring, web frameworks, and relational databases.
- Improved site accessibility, including introducing audio-based articles.

03.24 **Conference Volunteer, Applied Cryptography and Network Security**

10.19 **Saintcon Container Security Workshop**
Proposed and led a container security workshop, including cybersecurity challenges.