

MARIA KHODAK

vesna.my · maria.a.khodak@gmail.com · (215) 390-0815

RESEARCH INTERESTS

Graph theory, offensive security, cloud security, reverse engineering, machine learning model supply chain security, program analysis, software exploit mitigations, vulnerability discovery

EDUCATION

Dartmouth College

Hanover, NH

PhD Computer Science

Advised by Sergey Bratus and Christophe Hauser

Sep 2025 - Present

Rensselaer Polytechnic Institute

Troy, NY

BS Computer Science

Aug 2019 - May 2022

PROJECTS

Explainable Cloud Attack Path Discovery via Reinforcement Learning and Datalog *Python, Datalog*

Designed and implemented a reinforcement learning agent in Python to model adversarial network exfiltration scenarios, representing cloud networks and principals as directed graphs representing varying security risk levels.

Wyze Camera Vulnerability Security Analysis *Binary Ninja*

Ongoing independent vulnerability research and security analysis on the Wyze Cam Outdoor v2, Wyze Cam v4, and Wyze Lock Bolt v2, examining firmware, network communications, and authentication mechanisms.

GraphLeak

<https://vesnafvr.github.io/GraphLeak/>

An interactive visualization of data poisoning attacks using graph representations on sample machine learning training datasets. The program ingests a csv file of edges and displays the corresponding graph with various statistics. Then, the user can poison (ie remove or add) nodes and compare the resulting graph by ingesting it again.

Network Poisoner *Python, Gephi*

<https://github.com/vesnafvr/network-poisoner>

A program that poisons and alters training networks of machine learning data. The program intakes a csv file and outputs a poisoned version of the csv. The data is then input into Gephi in order to produce before and after snapshots of the effect of data poisoning.

Mandarin Project *Unity, C#, Python*

<https://cisl.rpi.edu/research/projects/mandarin-project>

A cognitive learning environment that leverages cognitive and mixed reality technology to immerse students in a sample of Chinese culture, practice daily tasks, and get help from intelligent agents.

WORK EXPERIENCE

Cigna

Remote

Security Engineer, Cigna Information Protection

July 2022 - July 2026

- Found and provided solutions for security vulnerabilities to internal and external customers through penetration testing engagements, documenting findings with accompanying proof-of-concepts and steps for remediation.
- Spearheaded machine learning testing to harden security posture for internal applications that use generative AI by demonstrating vulnerabilities such as data poisoning to organization leadership.
- Created and implemented a password management system in order to distribute credentials effectively for penetration testing operations.
- Independently conducted post-incident testing on internal applications, identifying and remediating vulnerabilities such as session token mismanagement, insecure credential handling, and broken access control.
- Led an organization-wide migration to Insomnia as an alternative to Postman for API testing to comply with internal security policies.
- Participated in comprehensive application security reviews, ensuring evaluations encompassed third-party and open-source applications, aligning with industry best practices.
- Implemented a Response Checker script to check decommissioned company site activity.
- Created and presented weekly reports for vulnerability occurrence metrics and remediation plans to organization leadership.

Cognitive and Immersive Research Laboratory
Undergraduate Researcher

Troy, NY
Nov 2019 - Dec 2021

- Researched cultural sites for usage in the panoramic scene system.
- Created 2 language learning games using Python and Javascript.
- Created panoramic waypoints and portals for language learning games using C#.
- Tested and modified simulated Chinese dialogues using C#.

SPEAKING ENGAGEMENTS

PathQuarry: Watching RL Agents Discover Cloud Privilege Escalation	Summercon 2026
Be Not Afraid: AppSec Solutions for ML Vulnerabilities	No Hat 2025
Poison in the Wires: Interactive Network Visualization of Data Attacks	SecTor 2025
	No Hat 2025
	Ekoparty 2025
	DistrictCon 2026
Good Models Gone Bad: Visualizing Data Poisoning with Networks	Insomni'Hack 2025

CERTIFICATIONS

Automated Reverse Engineering	Binary Ninja June 2025
GIAC Machine Learning Engineer (GMLE)	SANS Institute June 2025
Practical Junior Penetration Tester (PJPT)	TCM Security January 2025
GIAC Web Application Penetration Tester (GWAPT)	SANS Institute January 2024

SKILLS

Security Tools:	Burp Suite, Linux, Metasploit, Wireshark, Nmap, Binary Ninja
Programming Languages:	Python, C++, Bash
Natural Languages:	English, Russian, French, Mandarin Chinese