Maryam Rostamipoor

mrostamipoor@cs.stonybrook.edu | https://www.linkedin.com/in/maryam-rostamipoor/ |
https://github.com/mrostamipoor| Port Jefferson, NY | (631) 428-5243

EDUCATION

Stony Brook University — Stony Brook, NY
PhD in Computer Science | GPA: 3.91/4.0 — 2026

Stony Brook University — Stony Brook, NY
MS in Computer Science| GPA: 3.91/4.0 — 2023

Amirkabir University of Technology — Tehran, Iran
MS in Information Security Engineering| GPA: 17.73/20 — 2013

Shiraz University of Technology — Shiraz, Iran
B.E. in Computer Engineering| GPA: 16.64/20 — 2011

TECHNICAL SKILLS

- **Monitoring and Analysis Tools**: Angr, Strace, SysDig
- **Programming Languages**: Rust, Go, Python, Java, C, HTML, JavaScript, CSS, Rest API
- **Tools:** Burp Suite, Acunetix, Nessus, Metasploit, Web Inspect, sqlmap
- **Development Tools**: Visual Studio Code, Eclipse, Git
- **Operating Systems:** Windows, Linux
- **Typesetting:** LaTeX, Microsoft Word, Microsoft Excel, Microsoft PowerPoint
- **Databases**: Microsoft SQL Server, MySQL
- **Security Technologies/Concepts:** Authentication, Cryptography, Authorization, VPN, DDoS, DoS, Threat detection, Malware, PKI and SSL/TLS, IDS
- **Cloud Platforms or Security Equipment:** Amazon Web Services (AWS), Container, Kubernetes, Spin, Cloudflare Workers, Firewall, WAF, HSM

EXPERIENCES

Stony Brook University — Stony Brook, NY
Research Assistant at Hexlab| Advisor: Dr. Michalis Polychronakis — Feb. 2021 - Current

- Developing an innovative protection-based secret management system for Kubernetes, this solution prevents secret leakage and addresses the limitations of existing access control mechanisms by aligning with the MITRE ATT&CK framework's Kubernetes matrix.
- Developed a method called 'LeakLess', designed to safeguard selective sensitive data against **Data-only** attacks as well as speculative execution attacks that exploit side-channel vulnerabilities. This approach specifically protects confidential information in cloud-based serverless environments. 'LeakLess' is implemented using the safe Rust programming language within the Spin framework. Spin leverages the Wasmtime runtime for executing WebAssembly functions, ensuring robust security and efficient performance.
- Developed Confine, a Linux binary analysis tool, to automatically extract system call arguments values and generate Seccomp profiles. Confine is implemented using Python and the angr binary analysis platform.

Sadad Electronic Payment Company
Senior Web Application Security Engineer — May 2018 - Feb. 2021

- Identified and remediated critical vulnerabilities in the company's web and mobile applications through penetration testing, resulted in a significant risk reduction. Enforced security hardening measures on web servers, improving security posture, and configuring HSM.
- Provided security guidance to the development team, implemented secure coding practices, enhanced application security, and conducted a comprehensive audit of the WAF configuration identified potential misconfigurations and mitigated them effectively.

APA Research Center of Amirkabir University of Technology
Researcher and Senior Web Application Security Engineer — Feb. 2017 - May 2018

- Performed black/gray box penetration testing on customers' web and mobile applications, APIs, utilizing OWASP web application security guidelines and industry-standard methodologies to identify and report vulnerabilities.
- Conducted research and assessment of security benchmarks (CIS) for web servers and operating systems, resulting in a set of well-documented best practices for other companies to improve their security posture.

- Collaborated with a team of researchers to conduct in-depth research on Pure-Call Oriented Programming (PCOP) and co-authored a published paper on the topic. Presented poster of the final research project on the performance of Palladium-Technetium catalysts in fuel cells.

Stock Exchange Organization
Senior Web Application Security Engineer Dec. 2015 - Feb. 2017

- Performed black/gray box penetration testing on the organization and its dependent companies' web applications, and APIs based on OWASP web application security guidelines, resulting in a significant reduction in the risk of a security breach for sensitive trading data and securing the APIs.
- Successfully hardened 54 CentOS Linux servers within one month by developing and implementing a comprehensive security hardening program, including documentation and a custom script to automatically detect and audit security misconfiguration.

PHD COURSE PROJECTS

System Security (C Programming) Fall 2021

- Implemented a multi-threaded version of ROP-defender using Intel Pin, developed defense against Return-Oriented Programming attacks.
- Created a tool for transparent application functionality extension, ensuring seamless functionality augmentation.
- Developed real-world scenario exploits, encompassing stack-based overflow, data-only, return-2-libc, and ROP exploits.

Network Security (Go Programming) Spring 2021

- Designed and implemented a passive Network Monitoring tool.
- Developed a specialized detection tool to identify and counteract passive DNS poisoning attacks.
- Implemented a plugboard proxy to fortify the security of publicly accessible network services, adding an extra layer of encryption.

Operating Systems (C Programming) Spring 2021

- Implemented a file system, a customized CPU profiler, and a distributed shared memory mechanism.
- Developed a special cryptographic system call for Linux security.

Visualization (Python and JavaScript Programming) Spring 2022

- Developed an interactive dashboard comparing democracy levels in countries based on global (selected as a **star project**).

AWARDS and HONORS

- Graduate Assistance in Areas of National Need (**GAANN**) Fellowship Award Aug. 2023
- Graduate Students in **STEM** Leadership & Life Design Fellowship Award Aug. 2023
- **3rd** Place in Presentation on Innovative Techniques, SU-CTF Nov. 2016
- **1st** among all M.Sc. students at Amirkabir University of Technology Sep. 2013
- Ranked **35th** in the National University Entrance Examination for Graduate Schools May 2011
- Top **0.8%** Nation-wide entrance exam of Iranian Universities Jul. 2007

SELECTED PUBLICATIONS

- **Maryam Rostamipoor**, Seyedhamed Ghavamnia, and Michalis Polychronakis, LeakLess: Selective Data Protection against Memory Leakage Attacks for Serverless Environments, Under Major Revision in NDSS 2025.
- **Maryam Rostamipoor**, Seyedhamed Ghavamnia, and Michalis Polychronakis, Confine: Fine-grained System Call Filtering for Container Attack Surface Reduction, Published in the Computers & Security Journal, 2023.
- AliAkbar Sadeghi, Salman Niksefat, **Maryam Rostamipoor**, Pure-Call Oriented Programming (PCOP): chaining the gadgets using call instructions, Published in the Journal of Computer Virology and Hacking Techniques, May 2017.

TEACHING AND MENTORIN EXPERIENCES

Stony Brook University, Stony Brook, NY Spring 2022

Operating Systems teaching Assistant| Instructor: Erez Zadok

- Conducted grading for assignments and exams to evaluate student performance.
- Provided valuable support during office hours to address student queries and concerns.

Mentorship, Daniel Kogan, undergraduate student

- Actively mentoring him in applying LeakLess approach on top of **Cloudflare Workerd** (open-sourced Cloudflare Workers).

PRESENTATIONS AND POSTERS

- **LeakLess: Selective Data Protection against Memory Leakage Attacks for Serverless Environments** presented at Graduate Research Day (GRD) 2024, Stony Brook University. Program Details