Maryam Rostamipoor

Software Security Researcher
Port Jefferson, NY

✉ mrostamipoor@cs.stonybrook.edu
Personal Website
LinkedIn GitHub

Education

- **Ph.D. in Computer Science** *2021-2025*
  Stony Brook University, NY GPA: 3.91/4.0
- **Master in Computer Science** *2021-2024*
  Stony Brook University, NY GPA: 3.91/4.0
- **Master in Information Security Engineering** *2011-2013*
  Amirkabir University of Technology, Iran GPA: 17.73/20
- **Bachelor in Computer Engineering** *2007-2011*
  Shiraz University of Technology, Iran GPA: 16.64/20

Skills

- **Programming Languages**: Rust, Go, Python, Java, C.
- **Program Analysis Techniques**: Taint Tracking, Control Flow, Data Flow, Static & Dynamic Instrumentation.
- **Security & Analysis Tools**: CodeQL, angr, Ghidra, strace, ltrace, Objdump, sysdig, Burp Suite, Nessus, SQLMap, Acunetix, AppScan.
- **Cloud & DevOps Tools**: Docker, Kubernetes, AWS (Lambda, API Gateway), Git, CI/CD.
- **Container Security**: Seccomp, AppArmor, RBAC Hardening, Kubernetes Secrets Management.
- **Security Concepts**: Penetration Testing, Vulnerability Management, Cryptography, Authentication, Authorization, VPNs, DDoS Mitigation, Malware Protection, SSL/TLS, Firewalls, WAF.
- **Web Development & AI**: Python (Django, Flask), REST APIs, HTML, CSS, JavaScript, Prompt Engineering for LLMs.
- **Soft Skills**: Critical Thinking, Problem Solving, Self-Learning, Presentation, Adaptability.

Experience

- **Research Assistant at Hexlab, Stony Brook University** *Feb 2021 - now*
  Advisor: Dr. Michalis Polychronakis Stony Brook, NY
  - *Vulnerability Analysis (Ongoing)*: Analyzing software vulnerabilities using taint analysis in CodeQL to track sensitive data flow and identify vulnerable code patterns.
  - *KubeKeeper*: Designed and developed a solution to protect Kubernetes Secrets from leakage due to excessive permissions. The system automatically encrypts Secrets and ensures only explicitly authorized Pods can access decrypted secrets. It operates transparently, requiring no changes to existing infrastructure or application code.
  - *LeakLess*: Designed and developed a practical approach to mitigate memory disclosure vulnerabilities—including transient execution attacks—in serverless environments. LeakLess uses selective in-memory encryption for developer-annotated sensitive data and is implemented in Rust for safety and performance.
  - *Confine*: Developed a Linux binary analysis tool that automatically extracts system call argument values and generates Seccomp profiles. The tool was implemented in Python using the Angr platform.
- **Sadad Electronic Payment Company** *May 2018 - Feb 2021*
  Head of Software Security Team Tehran, Iran
  - Led a team of 3 security engineers, providing mentorship and training while ensuring thorough verification of findings and effective prioritization of remediations.
  - Identified and remediated critical vulnerabilities through penetration testing, improved server security via hardening and HSM configuration.
  - Guided development team on secure coding standards, audited WAF configurations to enhance security.
- **APA Research Center of Amirkabir University of Technology** *Feb 2017 - May 2018*
  Researcher and Senior Web Application Security Engineer Tehran, Iran
  - Performed black-box and gray-box penetration testing on customers' web applications, mobile applications, and APIs, following OWASP guidelines and industry-standard methodologies to identify and report vulnerabilities.
  - Conducted research and assessment of security benchmarks (CIS) for web servers and operating systems, developing a set of well-documented best practices that improved security posture for multiple organizations.
  - Collaborated on research into Pure-Call Oriented Programming (PCOP) and co-authored a published paper.
- **Stock Exchange Organization** *Dec 2015 - Feb 2017*
  Senior Web Application Security Engineer Tehran, Iran
  - Performed black/gray box penetration testing on web applications and APIs for the organization and its dependent companies, following OWASP guidelines. This work resulted in a significant reduction in the risk of security breaches for sensitive trading data.
  - Hardened 54 CentOS Linux servers within one month by developing and implementing a comprehensive security hardening program. Created a custom script to automatically detect and audit security configurations.

Publications

- **Maryam Rostamipoor**, Aliakbar Sadeghi, and Michalis Polychronakis. *"KubeKeeper: Protecting Kubernetes Secrets Against Excessive Permissions"*. In Proceedings of the 10th IEEE European Symposium on Security & Privacy (EuroS&P), 2025.
- **Maryam Rostamipoor**, Seyedhamed Ghavamnia, and Michalis Polychronakis. *"LeakLess: Selective Data Protection against Memory Leakage Attacks for Serverless Environments"*. In Proceedings of the Network and Distributed System Security Symposium (NDSS), February 2025, San Diego, CA.
- **Maryam Rostamipoor**, Seyedhamed Ghavamnia, and Michalis Polychronakis. *"Confine: Fine-grained System Call Filtering for Container Attack Surface Reduction"*. Computers & Security Journal, vol. 132, September 2023.
- AliAkbar Sadeghi, Salman Niksefat, **Maryam Rostamipoor**. *"Pure-Call Oriented Programming (PCOP): chaining the gadgets using call instructions"*, Journal of Computer Virology and Hacking Techniques, vol. 14, pp. 139–156, May 2018.

PhD Course Projects

- **System Security (C Programming)** *Fall 2021*
  - Developed a multi-threaded version of ROP-defender using Intel Pin to defend against Return-Oriented Programming (ROP) attacks.
  - Created a tool for transparent application functionality extension, ensuring seamless functionality augmentation.
  - Developed real-world scenario exploits, including 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 (Source code).
  - Developed a specialized detection tool to identify and counteract passive DNS poisoning attacks (Source code).
  - Implemented a plugboard proxy to fortify the security of publicly accessible network services, adding an extra layer of encryption (Source code).
- **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 across countries using global datasets, selected as a star project (Source code | Video).

Awards and Honors

- Awarded the **Catacosinos Fellowship** for academic excellence and research potential. *Apr. 2025*
- Awarded the **2025 Internet Society NDSS Fellowship**. *Jan. 2025*
- Selected for the **2025 CRA-WP Grad Cohort for Women & IDEALS**. *Jan. 2025*
- 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*

Teaching Experience

- **Teaching Assistant, Operating Systems** *Instructor: Dr. Erez Zadok*
  Stony Brook University Spring 2022
- **Web Application Penetration Testing Instructor** *2015-2020*

Mentorship Experience

- **Undergraduate Research Projects** *Spring 2023 - Fall 2024*
  Stony Brook University
  - Mentored Daniel Kogan in applying LeakLess to enhance security on **Cloudflare Workerd** (open-source Cloudflare Workers).
  - Mentored Jie Chen in working with Kubernetes third-party applications, focusing on learning how to identify and mitigate excessive RBAC permissions to follow the principle of least privilege.