Maryam Rostamipoor

Security Researcher / Engineer, San Jose, CA
mrostamipoor@cs.stonybrook.edu

Website: mrostamipoor.github.io
GitHub: github.com/mrostamipoor
LinkedIn: linkedin.com/in/maryam-rostamipoor

Summary

PhD Candidate in Computer Science and Security Researcher with 10+ years of combined research and industry experience in cloud, container, and application security. Specialized in scalable defenses against data leakage in cloud-native and serverless environments, with expertise in program analysis, vulnerability discovery, and secure software design. Proficient in Python, Go, Rust, Kubernetes, and CodeQL, with applied experience using LLMs for data flow analysis in serverless applications. Proven record of building tools for Kubernetes secret protection, serverless memory safety, and container hardening, translating cutting-edge research into practical security solutions.

Skills

- **Programming:** Python, Go, Rust, C, JavaScript
- **Machine Learning & Data Analysis:** Scikit-learn, Pandas, NumPy, Data Cleaning & Feature Engineering, Prompt Engineering (LLMs), AI-driven Automation in Security Monitoring
- **Research & Analysis Tools:** CodeQL, Angr, Ghidra, Dynamic & Static Program Analysis, Data Flow Analysis & Taint Tracking, Information Flow Control (language-based security, IFC tools)
- **Systems & Scalability:** Kubernetes (RBAC, Secrets Management, Admission Webhooks), Docker, AWS (Lambda, API Gateway, SQS, DynamoDB, S3), Serverless Computing
- **Cryptography & Data Protection:** Applied Cryptography for Data Protection & Privacy, Secure Protocols
- **Security Engineering & Testing:** Threat Modeling, Secure Software Development Lifecycle (SDLC), Application Security (SAST/DAST, code review), Penetration Testing (Web & API; Burp Suite, Nessus, SQLMap, Metasploit, WebInspect), Intrusion Detection & Anomaly Detection (system monitoring, security analytics), Hardening (Seccomp, AppArmor), Vulnerability Discovery
- **DevOps & Tools:** Git, CI/CD, Dashboarding (Python Dash, JavaScript/Plotly)

Experience

- **Research Assistant, Hexlab — Stony Brook University** *Feb 2021 – Present*
  Advisor: Dr. Michalis Polychronakis Stony Brook, NY
  - *Static Analysis for Serverless Security*: Leveraging CodeQL-based taint tracking with LLM-assisted reasoning to detect sensitive data flows in AWS Lambda. Applied ML-driven insights to configuration analysis (IAM and resource usage), uncovering systemic misconfigurations.
  - *KubeKeeper*: Designed a framework to prevent Kubernetes Secret leakage by applying encryption and fine-grained access control, eliminating insecure defaults and excessive permissions threats. Built a static analysis tool that scans Kubernetes configurations (YAML/Helm/Kustomize) pre-deployment to detect and report misconfigurations, uncovering that over 40% of real-world applications were misconfigured with secret-related risks.
  - *LeakLess*: Proposed a selective in-memory encryption approach for serverless platforms to mitigate memory disclosure and transient execution attacks. Implemented the prototype in Rust, demonstrating 91% compatibility with real-world workloads while maintaining only 2.8–8.5% overhead.
  - *Confine*: Developed an automated binary analysis tool using Angr that reduced container attack surfaces by up to 70% and neutralized 3× more Linux kernel CVEs compared to default policies, by generating application-specific system call filters.

- **Sadad Electronic Payment Company** *May 2018 – Feb 2021*
  Head of Software Security Team Tehran, Iran
  - Led and grew a 3-person security team, cutting critical vulnerability remediation time by 40% through streamlined triage and prioritization workflows.
  - Executed penetration testing and server hardening across 100+ systems, eliminating high-severity findings and deploying HSM-backed key protection for payment transactions.
  - Trained developers on secure coding standards and audited WAF rules, reducing exploitable risks in high-volume financial applications by 35%.

- **APA Research Center, Amirkabir University of Technology** *Feb 2017 – May 2018*
  Researcher & Senior Web Application Security Engineer Tehran, Iran
  - Performed black-box and gray-box penetration testing on 40+ web and mobile applications and APIs, uncovering high-risk vulnerabilities and ensuring compliance with OWASP standards.

- Assessed CIS benchmarks for servers and operating systems, creating best-practice hardening guidelines adopted by 100+ client organizations to strengthen their security posture.
- Co-authored research on Pure-Call Oriented Programming (PCOP), advancing academic understanding of exploitation techniques and attack surface reduction.

• **Stock Exchange Organization** *Dec 2015 – Feb 2017*
Senior Web Application Security Engineer Tehran, Iran
- Led penetration testing of 30+ web applications and APIs for the national stock exchange and subsidiaries, mitigating high-risk vulnerabilities in systems handling millions of daily trades.
- Hardened 54 CentOS servers in one month by designing and deploying a security baseline; developed automated auditing scripts that cut configuration review time by 70% and ensured ongoing compliance.

Education

• **Ph.D. in Computer Science** *2021 – 2026*
Stony Brook University, NY GPA: 3.91/4.0
***Thesis**: Detecting and Preventing Sensitive Data Leakage in Cloud-Native Environments*

• **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

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.

Awards and Honors

- Awarded the **Catacosinos Fellowship** for academic excellence and research potential. *Apr. 2025*
- Awarded the **Internet Society NDSS Fellowship**. *Jan. 2025*
- Selected for the **CRA-WP Grad Cohort for Women & IDEALS**. *Jan. 2025*
- Graduate Assistance in Areas of National Need **(GAANN)** Fellowship Award. *Aug. 2023*
- **1st** among all M.Sc. students at Amirkabir University of Technology. *Sep. 2013*

Selected Course Projects

- **System Security (Fall 2021):** Multithreaded ROP-defender with Intel Pin; exploit development (stack overflow, data-only, ret2libc, ROP).
- **Network Security (Spring 2021):** Passive network monitor; DNS-poisoning detector; Encrypted plugboard proxy.
- **Operating Systems (Spring 2021):** Toy filesystem, CPU profiler, distributed shared memory; custom cryptographic syscall for Linux.
- **Visualization (Spring 2022):** Interactive dashboard comparing democracy levels [code, video].

Mentorship & Teaching

- **PhD Mentor (2023–2025):** Mentored 2 master's and 3 undergraduate students on projects in Kubernetes security, serverless memory protection, and binary analysis; guided them through research design, tool implementation, and paper preparation.
- **Teaching Assistant, Operating Systems (Spring 2022):** Assisted in assignment delivery, grading, and student guidance for 80 graduate students at Stony Brook University.