Maryam Rostamipoor

Security Engineer | Security Researcher
PhD '26 | San Jose, CA
Green Card Holder

GitHub: @mrostamipoor
mrostamipoor@cs.stonybrook.edu
LinkedIn: @maryam-rostamipoor
Website: mrostamipoor.github.io

Summary

Security Engineer with **8+ years** of combined industry and research experience, completing a **PhD in Computer Science** (May 2026). Specializes in **cloud and platform security**, **Kubernetes and container hardening**, **secrets management**, **static analysis**, and **penetration testing**. Built production-grade security systems deployed across hundreds of real-world applications, with publications at **NDSS** and **IEEE EuroS&P**. Led security engineering and penetration testing teams in financial infrastructure. Experienced in **threat modeling**, **security architecture reviews**, **CI/CD security**, and **security automation at scale**.

Core Areas: Cloud and platform security, threat modeling, security architecture reviews, manual vulnerability discovery and exploitation (XSS, SQL injection, SSRF, IDOR, RCE), Kubernetes and container security, AWS/cloud security, CI/CD and IaC security, secrets management, static and data-flow analysis, security automation.

Experience

- **Security & Privacy Researcher — HexLab, Stony Brook University** *Feb 2021 – May 2026*
  Cloud and Platform Security Research Stony Brook, NY
  - Built **LeakLess**: in-memory encryption architecture protecting sensitive data against **memory-disclosure and transient-execution attacks** (Spectre/Meltdown class) in 91% of serverless applications with only **2.8–8.5%** overhead. Published at **NDSS 2025**.
  - Built **KubeKeeper**: cryptographic Secrets protection for Kubernetes using RBAC and Admission Webhooks, eliminating excessive-permission exposures across **498** real-world applications with **zero runtime overhead**. Published at **EuroS&P 2025**.
  - Developed **LeakGauge**: IaC-aware static analysis framework (CodeQL) that traces sensitive data flows across serverless deployments, identifying **1,400+** secret-exposure paths across **500+** applications — designed as a CI/CD security guardrail.
  - Created **Confine**: automated seccomp policy generation for containers via static binary analysis, filtering **144+** system calls on average and mitigating **28** Linux kernel CVEs. Published in *Computers & Security*, 2023.

- **Sadad Electronic Payment Company** *May 2018 – Feb 2021*
  Head of Software Security Team Tehran, Iran
  - Led product and platform security for a **national-scale banking ecosystem**, performing threat modeling, security architecture reviews, and risk assessments across web, mobile, and API-driven systems.
  - Manually exploited real-world vulnerabilities including **XSS, SQL injection, SSRF, IDOR, authentication bypass, and RCE**, uncovering critical attack chains in production financial applications.
  - Conducted penetration testing of **20+ web/mobile services and APIs**, eliminating high-severity vulnerabilities and integrating secure development practices into the SDLC.
  - Automated vulnerability triage and remediation tracking workflows, reducing remediation time by **40%**.

- **APA Research Center, Amirkabir University of Technology** *Feb 2017 – May 2018*
  Researcher & Senior Software Security Engineer Tehran, Iran
  - Performed penetration testing across **90+** web, mobile, and API systems, discovering **CVSS $\geq$ 9** vulnerabilities in national stock exchange infrastructure processing millions of daily transactions.
  - Evaluated configurations against **CIS benchmarks**; designed secure baselines and automated auditing scripts for **54** production servers, reducing review time by **70%**. Guidance adopted by **100+** organizations.

- **Stock Exchange Organization** *Dec 2015 – Feb 2017*
  Senior Web Application Security Engineer Tehran, Iran
  - Led offensive security assessments across **50+** production web applications and APIs supporting national financial trading platforms, mitigating high-risk attack paths.

– Hardened **54** production servers by designing secure baselines and automated auditing scripts, reducing configuration review time by **70%**.

Skills

- **Security & Privacy:** Applied cryptography, in-memory encryption, secrets management, data-flow and taint analysis, memory safety, trusted execution, container isolation (seccomp, AppArmor), threat modeling (STRIDE), detection engineering, DevSecOps.
- **Systems & Infrastructure:** Linux kernel internals, system-call filtering, AWS (IAM, VPC, Security Groups, S3, RDS, Lambda, Security Hub, Config, CloudTrail, IAM Access Analyzer), Kubernetes (RBAC, Secrets, Admission Webhooks), Docker, IaC security validation, CI/CD security integration (GitHub Actions), secure-by-default architecture.
- **Program & Binary Analysis:** Static and dynamic analysis of ELF and script-based payloads; CodeQL, angr, Ghidra; data- and taint-flow tracking; automated vulnerability discovery.
- **Programming:** Python, C, Go, Rust, JavaScript.
- **AI/ML for Security:** scikit-learn, Pandas, NumPy; LLM-assisted source/sink modeling, rule synthesis, and anomaly detection for security analytics.
- **Web Vulnerability Exploitation:** XSS, SQL injection, SSRF, IDOR, CSRF, deserialization, authentication bypass, and remote code execution across web and API architectures.
- **Vulnerability Assessment:** Burp Suite, Acunetix, Nessus, Metasploit, WebInspect, SQLmap.

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

Awards and Honors

- **Catacosinos Fellowship** for academic excellence and research potential *2025*
- **Internet Society NDSS Fellowship** *2025*
- Selected for the **CRA-WP Grad Cohort for Women & IDEALS** *2025*
- **GAANN Fellowship** (U.S. Dept. of Education) *2023*

Teaching & Mentorship

- Mentored graduate and undergraduate researchers on Kubernetes security, serverless security, and binary analysis.
- Delivered penetration testing and secure coding training to **200+** students and professionals.

Publications

- **Maryam Rostamipoor**, Seyedhamed Ghavamnia, and Michalis Polychronakis. *"LeakLess: Selective Data Protection against Memory Leakage Attacks for Serverless Environments"*. Network and Distributed System Security Symposium (NDSS), 2025.
- **Maryam Rostamipoor**, Aliakbar Sadeghi, and Michalis Polychronakis. *"KubeKeeper: Protecting Kubernetes Secrets Against Excessive Permissions"*. IEEE European Symposium on Security & Privacy (EuroS&P), 2025.
- **Maryam Rostamipoor**, Seyedhamed Ghavamnia, and Michalis Polychronakis. *"Confine: Fine-grained System Call Filtering for Container Attack Surface Reduction". Computers & Security*, 2023.

Under Submission / Preparation

- Aliakbar Sadeghi, **Maryam Rostamipoor**, Nick Nikiforakis, and Omar Chowdhury. *"Fake APIs, Real Threats: Studying Activities Targeting APIs in the Wild"*. Under submission.
- **Maryam Rostamipoor**, and Michalis Polychronakis. *"LeakGauge: Infrastructure-as-Code–Aware Sensitive Data Flow Analysis in Event-Driven Serverless Applications"*. In preparation.