Maryam Rostamipoor

System Security Researcher
Port Jefferson, NY

Personal Website
GitHub
LinkedIn

Education

- **PhD in Computer Science** *2021-26*
  Stony Brook University, NY GPA: 3.91/4.0
- **MS in Computer Science** *2021-23*
  Stony Brook University, NY GPA: 3.91/4.0
- **ME in Information Security Engineering** *2011-13*
  Amirkabir University of Technology, Tehran, Iran GPA: 17.73/20
- **BE in Computer Engineering** *2007-11*
  Shiraz University of Technology, Fars, Iran GPA: 16.64/20

Technical Skills

- **Programming Languages**: Rust, Go, Python, Java, C.
- **Cloud & DevOps Tools**: Docker, Kubernetes, Helm, WebAssembly (Wasm), WASI, Amazon Web Services (AWS), Cloudflare Workers, Spin, Git.
- **Security Tools**: angr, Strace, SysDig, Burp Suite, Nessus, sqlmap, Metasploit, Web Inspect.
- **Security Concepts & Technologies**: Cryptography, Authentication, Authorization, VPN, DDoS/DoS Mitigation, Threat Detection, Malware Protection, PKI, SSL/TLS, IDS, Firewall, WAF, HSM.
- **Version Control & Collaboration**: Git, GitHub, GitLab.
- **Web Development**: Python (Django, Flask), REST APIs, HTML, CSS, JavaScript.
- **Operating Systems**: Linux, CentOS, Ubuntu.
- **Soft Skills**: Critical Thinking, Problem-Solving, Self-learning, Presentation, Adaptability.

Experience

- **Research Assistant at Hexlab** *Feb 2021 - now*
  Stony Brook University, Advisor: Dr. Michalis Polychronakis
  - *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 data. 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 of 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. Tool implemented in Python using the Angr platform.

- **Sadad Electronic Payment Company** *May 2018 - Feb 2021*
  Senior Web Application Security Engineer Tehran, Iran
  - Identified and remediated critical vulnerabilities in web and mobile applications through penetration testing, significantly reducing risk. Improved the security posture of web servers by implementing hardening measures and configuring HSM.
  - Provided security guidance to the development team, implemented secure coding practices, and enhanced overall application security. Conducted a comprehensive audit of the WAF configuration, identified misconfigurations, and mitigated them effectively.

- **APA Research Center of Amirkabir University of Technology** *Feb 2017 - May 2018*
  Researcher and Senior Web Application Security Engineer Tehran, Iran
  - Performed black/gray box penetration testing on customers' web and mobile applications, APIs, following OWASP guidelines and industry-standard methodologies, identifying and reporting 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.

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, 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.
  - 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 datasets (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**, Aliakbar Sadeghi, and Michalis Polychronakis, *KubeKeeper: Protecting Kubernetes Secrets Against Excessive Permissions*, Under submission to USENIX 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*, 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 Mentoring Experiences

- **Teaching Assistant, Operating Systems** *Instructor: Erez Zadok*
  Stony Brook University Spring 2022
- **Mentorship** *Student: Daniel Kogan*
  Stony Brook University Spring 2023
  - Actively mentored Daniel in applying LeakLess to enhance security on Cloudflare Workerd (open-sourced Cloudflare Workers).

Presentations and Posters

- **LeakLess: Selective Data Protection against Memory Leakage Attacks for Serverless Environments**
  Graduate Research Day (GRD), Stony Brook University Spring 2024
  - Presented the LeakLess project, highlighting selective in-memory encryption to mitigate memory leakage attacks in serverless environments.