Prashant Rajput

Contact Information

pr1365@nyu.edu | github.com/starlordphr
linkedin.com/in/prashanthrajput | starlordphr.github.io

Education

New York University, Ph.D., Computer Science — 2018 - 05/17/2023
University of California Los Angeles, M.S., Computer Science — 2016 - 12/15/2017
Savitribai Phule Pune University, Bachelor of Engineering, Computer Engineering — 2012 - 06/30/2016

Technical Skills

Python, C++, DAST, Malware Analysis, Anomaly Detection, Reverse Engineering, JTAG

Professional Experience

Developer Support Engineer II, InterSystems — May 2023 - Present

- Investigated and resolved complex system performance issues and analyzed coredump files to identify root causes in high-scale technical environments.
- Designed and developed an ObjectScript fuzzer with support for structured data inputs, standard mutators, and feedback-based fuzzing to validate proprietary software robustness.
- Engineered and implemented raw stack annotation in Linux coredumps, enabling accurate and reliable backtrace generation similar to GDB for enhanced debugging capabilities.

Software Engineer Intern, Meta, Product Security Program Analysis — May 2022 - Aug 2022

In-Memory File System Sandbox for Auto-Generated Fuzzing Harnesses

- Designed and implemented an in-memory filesystem sandboxing library using Glibc hooks to redirect execution flow, enabling fuzzing in auto-generated harnesses and improving code coverage.
- Integrated the sandboxing library into the automated fuzzing pipeline and developed a crash triage dashboard to efficiently surface and analyze filesystem-related crashes.

Software Engineer Intern, Facebook, Malware Analysis Infrastructure — May 2021 - Aug 2021

Improving Disassembly Database Support in ThreatData

- Developed EntDisassemblerDatabase, a graph-based schema for storing disassembly data, leveraging Facebook's upload service to support scalable and structured analysis workflows.
- Designed and implemented TDSync, an IDA Pro plugin for real-time annotation syncing with the Disassembly UI, optimizing GraphQL mutations by transmitting diffs between annotation states to reduce data redundancy.

Research Experience

Research Assistant, New York University, Global Ph.D. Fellow — Aug 2018 - May 2023

Automated Vulnerability Localization and Hotpatching in Industrial Control Systems

- Developed ICSPatch, a tool for localizing and hotpatching control logic vulnerabilities using Data Dependence Graphs and a non-intrusive LKM patcher; tested on 24 synthetic vulnerable applications.
- Patched OOB read/write, OS command injection, and input validation flaws with ≈222ms patch generation and ≈332ms deployment latency.

Remote Non-Intrusive Malware Detection based on Hardware Root-of-Trust

- Proposed a non-intrusive, out-of-device malware detection approach leveraging semantic and microarchitectural features with an SVM model, achieving a detection accuracy of ≈99.75%.
- Implemented rootkit detection via integrity checks on static Linux kernel data structures and employed an OCSVM trained on static analysis of shared libraries to detect user-level rootkits, reaching ≈96.3% accuracy.

Platform Agnostic Remote Static Analysis Malware Detection for Industrial Control Systems

- Implemented static malware detection using entropy, string, and syscall histogram features from process .text sections, enabling platform-agnostic analysis.
- Achieved ≈98% (ARM) and ≈95% (x86_64) detection accuracy with an SVM model using JTAG-based data collection.

Publications

- Villa C., Doumanidis C., Lamri H., *Rajput P.*, and Maniatakos M., "ICSQuartz: Scan Cycle-Aware and Vendor-Agnostic Fuzzing for Industrial Control Systems." *NDSS 2025*.
- *Rajput P.*, Doumanidis C., and and Maniatakos M., "Automated Vulnerability Localization and Non-Intrusive Hotpatching in Industrial Control Systems using Data Dependence Graphs." *USENIX 2023*.
- Bytes A., *Rajput P.*, Doumanidis C., Maniatakos M., Zhou J., and Tippenhauer N., "FieldFuzz: In Situ Blackbox Fuzzing of Proprietary Industrial Automation Runtimes via the Network." *RAID 2023*.
- Doumanidis C., *Rajput P.*, and Maniatakos M., "ICSML: Industrial Control Systems ML Framework for native inference using IEC 61131-3 code." *CPSS 2023*.
- *Rajput P.*, Sarkar E., Tychalas D., and Maniatakos M., "Remote Non-Intrusive Malware Detection for PLCs based on Chain of Trust Rooted in Hardware." *IEEE EuroS&P 2021*.
- *Rajput P.*, and Maniatakos M., "Towards Non-intrusive Malware Detection for Industrial Control Systems." *IEEE DATE 2021*.
- *Rajput P.*, and Maniatakos M., "JTAG: A Multifaceted Tool for Cyber Security." *IEEE IOLTS 2019*.
- *Rajput P.*, Rajput P., Sazos M., and Maniatakos M., "Process-Aware Cyberattacks for Thermal Desalination Plants." *ACM Asia CCS 2019*.