Prashant Rajput

Contact Information

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

Education

New York University, Ph.D., Computer Science 2018-2023
University of California Los Angeles, M.S., Computer Science 2016-2017
Savitribai Phule Pune University, Bachelor of Engineering, Computer Engineering 2012-2016

Technical Skills

Python, C++, Static/Dynamic Analysis, Malware Analysis, Anomaly Detection, Reverse Engineering, JTAG

Professional Experience

Developer Support Engineer, Worldwide Response Center, InterSystems May 2023 - Present

- Investigate, reproduce and perform root cause analysis for system performance issues and coredump files in complex technical environments.
- Develop and build an ObjectScript fuzzer with support for structured data type inputs, standard mutators, and fuzzing feedback for testing proprietary code.

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

Automated Vulnerability Localization and Hotpatching in Industrial Control Systems

- Developed ICSPatch to localize vulnerabilities in control logic using Data Dependence Graph, non-intrusively hotpatch it using an LKM patcher and tested on a synthetic dataset with 24 vulnerable control applications.
- Successfully localized and hotpatched OOB write/read, OS command injection, and improper input validation, incurring latency of ≈222ms and ≈332ms for patch generation and deployment, respectively.

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

- Proposed an out-of-the-device non-intrusive malware detection methodology utilizing semantic and microarchitectural information with an SVM model, demonstrating an accuracy increase to ≈99.75%.
- Utilized integrity verification of static Linux kernel data structures for rootkit detection and OCSVM trained on static analysis information of shared libraries for user-level rootkits, achieving an accuracy of ≈96.3%.

Platform Agnostic Remote Static Analysis Malware Detection for Industrial Control Systems

- Implemented static analysis malware detection technique for process text section by extracting entropy values for a 32-byte sliding window, string, and syscall histograms, to be utilized as platform-agnostic features.
- Achieved ≈98%, ≈95% malware detection accuracy for ARM and x86_64 architecture, respectively, with an SVM model utilizing JTAG for data collection.

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

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

- Designed and implemented in-memory file system sandboxing library employing Glibc hooks for redirecting execution flow to enable fuzzing in auto-generated harnesses while also improving coverage.
- Integrated file system sandboxing library into the auto-generated harness fuzzing pipeline and created a dashboard to list all library touching crashes for more accessible crash triaging.

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

Improving Disassembly Database Support in ThreatData

- Created EntDisassemblerDatabase, a graph schema to store disassembly databases using FB upload service.
- Designed and implemented TDSync, an IDA plugin for annotation syncing to Disassembly UI while reducing redundant data in the GraphQL mutation by utilizing diffs between consecutive annotation states.

Research Assistant, Center for Cyber Security, NYUAD Dec 2017 - July 2018

Process-Aware Cyberattacks for Thermal Desalination Plants

- Performed process-aware security assessment of desalination plants to identify attack entry points and quantified the detrimental effects of water hammering attacks, inducing a von Mises stress of 340 MPa.

Publications

- *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.*
- Anonimized, "ICS-QUARTZ: Scan Cycle-Aware and Vendor-Agnostic Fuzzing for Industrial Control Systems" *Under Review.*