





Prashant Rajput

CONTACT INFORMATION	 pr1365@nyu.edu  linkedin.com/in/prashanthrajput	 github.com/starlordphr  starlordphr.github.io
EDUCATION	<b>New York University</b> , Ph.D., Computer Science 2018-2023 <b>University of California Los Angeles</b> , M.S., Computer Science 2016-2017 <b>Savitribai Phule Pune University</b> , Bachelor of Engineering, Computer Engineering 2012-2016	
TECHNICAL SKILLS	Python, C++, Static/Dynamic Analysis, Malware Analysis, Anomaly Detection, Reverse Engineering, JTAG	
PROFESSIONAL EXPERIENCE	<b>Developer Support Engineer, InterSystems</b> , Worldwide Response Center May 2023 - Present <ul style="list-style-type: none"><li>Investigate, reproduce and perform root cause analysis for system performance issues and coredump files in complex technical environments.</li><li>Develop and build an ObjectScript fuzzer with support for structured data type inputs, standard mutators, and fuzzing feedback for testing proprietary code.</li></ul> <b>Software Engineer Intern, Meta</b> , Product Security Program Analysis May 2022 - Aug 2022 <i>In-Memory File System Sandbox for Auto-Generated Fuzzing Harnesses</i> <ul style="list-style-type: none"><li>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.</li><li>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.</li></ul> <b>Software Engineer Intern, Facebook</b> , Malware Analysis Infrastructure May 2021 - Aug 2021 <i>Improving Disassembly Database Support in ThreatData</i> <ul style="list-style-type: none"><li>Created EntDisassemblerDatabase, a graph schema to store disassembly databases using FB upload service.</li><li>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.</li></ul>	
RESEARCH EXPERIENCE	<b>Research Assistant, New York University</b> , Global Ph.D. Fellow Aug 2018 - May 2023 <i>Automated Vulnerability Localization and Hotpatching in Industrial Control Systems</i> <ul style="list-style-type: none"><li>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.</li><li>Successfully localized and hotpatched OOB write/read, OS command injection, and improper input validation, incurring latency of <math>\approx 222\text{ms}</math> and <math>\approx 332\text{ms}</math> for patch generation and deployment, respectively.</li></ul> <i>Remote Non-Intrusive Malware Detection based on Hardware Root-of-Trust</i> <ul style="list-style-type: none"><li>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 <math>\approx 99.75\%</math>.</li><li>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 <math>\approx 96.3\%</math>.</li></ul> <i>Platform Agnostic Remote Static Analysis Malware Detection for Industrial Control Systems</i> <ul style="list-style-type: none"><li>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.</li><li>Achieved <math>\approx 98\%</math>, <math>\approx 95\%</math> malware detection accuracy for ARM and x86_64 architecture, respectively, with an SVM model utilizing JTAG for data collection.</li></ul> <b>Research Assistant, NYUAD</b> , Center for Cyber Security Dec 2017 - July 2018 <i>Process-Aware Cyberattacks for Thermal Desalination Plants</i> <ul style="list-style-type: none"><li>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.</li></ul>	
PUBLICATIONS	<ul style="list-style-type: none"><li>Villa C., Doumanidis C., Lamri H., Rajput P., and Maniatakos M., "ICSQuartz: Scan Cycle-Aware and Vendor-Agnostic Fuzzing for Industrial Control Systems." <i>NDSS 2025</i>.</li><li>Rajput P., Doumanidis C., and Maniatakos M., "Automated Vulnerability Localization and Non-Intrusive Hotpatching in Industrial Control Systems using Data Dependence Graphs." <i>USENIX 2023</i>.</li><li>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." <i>RAID 2023</i>.</li><li>Doumanidis C., Rajput P., and Maniatakos M., "ICSML: Industrial Control Systems ML Framework for native inference using IEC 61131-3 code." <i>CPSS 2023</i>.</li><li>Rajput P., Sarkar E., Tychalas D., and Maniatakos M., "Remote Non-Intrusive Malware Detection for PLCs based on Chain of Trust Rooted in Hardware." <i>IEEE EuroS&amp;P 2021</i>.</li><li>Rajput P., and Maniatakos M., "Towards Non-intrusive Malware Detection for Industrial Control Systems." <i>IEEE DATE 2021</i>.</li><li>Rajput P., and Maniatakos M., "JTAG: A Multifaceted Tool for Cyber Security." <i>IEEE IOLTS 2019</i>.</li><li>Rajput P., Rajput P., Sazos M., and Maniatakos M., "Process-Aware Cyberattacks for Thermal Desalination Plants." <i>ACM Asia CCS 2019</i>.</li></ul>	