





Prashant Rajput

CONTACT INFORMATION	 pr1365@nyu.edu  linkedin.com/in/prashanthrajput  github.com/starlordphr  prashanthrajput.com	
EDUCATION	New York University, Ph.D., Computer Science University of California Los Angeles, M.S., Computer Science Savitribai Phule Pune University, Bachelor of Engineering, Computer Engineering	Expected May 2023 2016-2017 2012-2016
TECHNICAL SKILLS	Python, C++, Hack, React, Java, PHP, and JavaScript.	
PROFESSIONAL EXPERIENCE	Research Assistant , Global Ph.D. Fellow, New York University <i>Automated Vulnerability Localization and Hotpatching in Industrial Control Systems</i> <ul style="list-style-type: none">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 $\approx 222\text{ms}$ and $\approx 332\text{ms}$ for patch generation and deployment, respectively. <i>Remote Non-Intrusive Malware Detection based on Hardware Root-of-Trust</i> <ul style="list-style-type: none">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 $\approx 99.75\%$.Utilized integrity verification of critical 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 $\approx 96.3\%$. <i>Platform Agnostic Remote Static Analysis Malware Detection for Industrial Control Systems</i> <ul style="list-style-type: none">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 $\approx 98\%$, $\approx 95\%$ 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 <i>In-Memory File System Sandbox for Auto-Generated Fuzzing Harnesses</i> <ul style="list-style-type: none">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 <i>Improving Disassembly Database Support in ThreatData</i> <ul style="list-style-type: none">Created EntDisassemblerDatabase, a schema to represent disassembly databases, associated it with the existing ThreatData graph, and modified ThreatData UI to upload 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 <i>Process-Aware Cyberattacks for Thermal Desalination Plants</i> <ul style="list-style-type: none">Performed process-aware security assessment of desalination plants to identify attack entry points, categorize the attacks, and estimate the corresponding financial loss and mechanical damage.Quantified the detrimental effects of water hammering during such attacks in terms of Maximum induced von Mises stresses (340 MPa) and maximum displacement (19.94mm) with ANSYS.	Aug 2018 - Present
PUBLICATIONS	<ul style="list-style-type: none">Bytes A., Rajput P., Doumanidis C., Maniatakos M., Zhou J., and Tippenhauer N., "FieldFuzz: Enabling vulnerability discovery in Industrial Control Systems supply chain using stateful system-level fuzzing." <i>Under Review</i>.Doumanidis C., Rajput P., and Maniatakos M., "ICSML: Industrial Control Systems Machine Learning Inference Framework natively executing on IEC 61131-3 compliant devices." <i>Under Review</i>.Rajput P., Doumanidis D., and Maniatakos M., "Automated Vulnerability Localization and Non-Intrusive Hotpatching in Industrial Control Systems using Data Dependence Graphs." <i>USENIX 2023</i>.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&P 2021</i>.Rajput P., and Maniatakos M., "Towards Non-intrusive Malware Detection for Industrial Control Systems." <i>IEEE DATE 2021</i>.Rajput P. and Maniatakos M., "JTAG: A Multifaceted Tool for Cyber Security." <i>IEEE IOLTS 2019</i>.Rajput P., Rajput P., Sazos M., and Maniatakos M., "Process-Aware Cyberattacks for Thermal Desalination Plants." <i>ACM Asia CCS 2019</i>.	