





Prashant Rajput

CONTACT INFORMATION	 pr1365@nyu.edu  linkedin.com/in/prashanthrajput	 github.com/starlordphr  prashanthrajput.com
EDUCATION	New York University , Brooklyn, NY Ph.D., Computer Science Expected 2023 University of California Los Angeles , Los Angeles, CA M.S., Computer Science 2016-2017 Savitribai Phule Pune University , Pune, India Bachelor of Engineering, Computer Engineering 2012-2016	
TECHNICAL SKILLS	• Python, Hack, React, C++, Java, PHP, and JavaScript.	
PROFESSIONAL EXPERIENCE	Research Assistant Aug 2018 - Present Global Ph.D. Fellow, New York University, Brooklyn, NY <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 high and low-level information collected by JTAG using Lauterbach PowerDebug PRO.Demonstrated an accuracy increase to $\approx 99.75\%$ by utilizing semantic and microarchitectural information with an SVM model for malware detection.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 external non-intrusive static analysis malware detection leveraging out-of-the-device virtual to physical address translation with JTAG.Performed static analysis of process text section for extracting entropy values for a 32-byte sliding window, string, and syscall histograms, to be utilized as platform-agnostic features.Achieved 98%, $\approx 95\%$ malware detection accuracy for ARM and x86_64 architecture, respectively, with an SVM model. Software Engineer Intern May 2021 - Aug 2021 Facebook, Malware Analysis Infrastructure, CA <i>Improving Disassembly Database Support in ThreatData</i> <ul style="list-style-type: none">Created EntDisassemblerDatabase, a schema to represent disassembly databases and associated it with existing ThreatData graph.Modified ThreatData UI to upload disassembly databases using FB upload service and preview related intel source reports.Designed and implemented TDSync, an IDA plugin to enable annotation sync between local instances and Disassembly UI.Reduced redundant data in a GraphQL mutation by utilizing diffs between consecutive annotation states. Research Assistant Dec 2017 - July 2018 Center for Cyber Security, NYUAD, Abu Dhabi, UAE <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, estimate the corresponding financial loss, and mechanical damage.Computed the resultant thermal shocks and pressure surges during water hammer in the piping system on sudden valve closure in MATLAB.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.	
PUBLICATIONS	<ul style="list-style-type: none">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>.	