Prashant Rajput

Contact Information

✉ pr1365@nyu.edu
in 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, C++, Java, PHP, JavaScript, and MATLAB.

Professional Experience

Research Assistant — Aug 2018 - Present
Global Ph.D. Fellow, New York University, Brooklyn, NY

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

- 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 ≈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 ≈96.3%.

Platform Agnostic Remote Static Analysis Malware Detection for Industrial Control Systems

- 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%, ≈95% malware detection accuracy for ARM and x86_64 architecture, respectively, with an SVM model.

Research Assistant — Dec 2017 - July 2018
Center for Cyber Security, NYUAD, Abu Dhabi, UAE

Process-Aware Cyberattacks for Thermal Desalination Plants

- 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.

Graduate Student Researcher — Sept 2016 - Nov 2017
UCLA, Los Angeles, CA

Detecting Targeted Spear Email Phishing Attacks in Outlook

- Developed a metadata-based approach for defending against email spear-phishing attacks.
- Extended Levenshtein Distance with MySQL backend for identifying suspicious emails.
- Optimized the solution by reducing search space using additional MySQL queries.

Cyber Security Intern — April 2017 - Nov 2017
Ariento, Los Angeles, CA

- Customized and maintained network security monitoring infrastructure with AWS.
- Implemented security rules in OSSEC and Snort to detect suspicious behavior over networks.
- Conducted security assessments and penetration tests for clients using Kali Linux.

Publications

- 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.*