Prashant Rajput

Contact Information

prashanthrajput@nyu.edu | github.com/starlordphr
linkedin.com/in/prashanthrajput | prashanthrajput.com

Education

New York University, Brooklyn, NY
Ph.D., Computer Science & Engineering — Expected 2022

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 using Semantic and Microarchitectural-based Features

- Proposed an out-of-the-device non-intrusive malware detection methodology utilizing high and low-level information collected by JTAG using Lauterbach PowerDebug PRO.
- Built an SVM model for identifying the operation of malware in a Linux-based embedded device and studied the impact of concept drift and spatial experimental bias.
- Demonstrated an accuracy increase to ≈99.75% in cases where malware is detected by utilizing semantic and microarchitectural information, culminating in a comprehensive system overview.

Rootkit Protection for Linux-based Embedded Devices based on Hardware Root-of-Trust

- Implemented an out-of-the-device rootkit injection prevention technique with an intrusive mode of operation employing hardware breakpoints for monitoring unauthorized modifications.
- Proposed a non-intrusive rootkit detection approach with preliminary disassembly support using integrity verification of critical static Linux kernel data structures such as Syscall table.
- Achieved ≈96.3% accuracy with One-Class SVM in averting the injection of user-level rootkits by applying static analysis information collected from the binaries of shared libraries.

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. and Maniatakos M., "JTAG: A Multifaceted Tool for Cyber Security," *2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, 155-158.
- Rajput P., Rajput P., Sazos M., and Maniatakos M., "Process-Aware Cyberattacks for Thermal Desalination Plants," *2019 ACM Asia Conference on Computer and Communications Security (Asia CCS '19)*, 441–452.
- Rajput P., "Phish Muzzle: This Fish Won't Bite," *2017, Department of Computer Science, University of California Los Angeles, USA*.