Rui Shu

• 919-986-0975 • rshu@ncsu.edu • rshu.github.io

EDUCATION

North Carolina State University, Raleigh, NC Aug. 2014 - Nov. 2021
Ph.D. in Computer Science | Adviser: Dr. Tim Menzies (*IEEE Fellow*)
Research Interests: Hyperparameter Optimization | Search-Based Software Engineering | Security

Peking University, Beijing, China Sep. 2011 - Jun. 2014
M.S. in Software Engineering
Research Interests: Trusted Computing | Network Security | Cloud Computing | Chinese Wall Policy

Beijing Jiaotong University, Beijing, China Sep. 2006 - Jun. 2010
B.S. in Software Engineering
Coursework: Software Engineering | Data Structure | Operating System | Network | Algorithm

SKILLS AND INTERESTS

- **General Expertise:** Hyperparameter Optimization, Software Development, Machine Learning, and Security Analysis.
- **Programming:** Java, Python, C, shell script, SQL.
- **Data Analysis:** Scikit-learn, Tensorflow, Keras, Pandas.
- **Security:** Metasploit, Burp Suite, OWASP ZAP, Wireshark, Aircrack-ng, Nmap, Kali Linux.
- **DevOps:** Vagrant, Git, Jenkins, Docker, Ansible, Maven, MySQL, Mocha/Mockito Framework.
- **Work Interests:** Actively seeking software development internships as well as software engineering and machine learning research positions.

SELECTED RESEARCH PROJECTS AND INTERN

Build Ensemble System against Adversarial Evasion Attacks Jan, 2020 - Oct, 2020
NSF Funded Research Project, Software Engineering Lab, North Carolina State University

- Proposed a novel approach Omni that creates an ensemble of "unexpected models", i.e., models whose control hyperparameters have a large distance to the hyperparameters of an adversary's target model.
- Explored and selected ensemble base models with Bayesian optimization, and made an optimized weighed prediction via differential evolutionary optimization.
- The improvement rate of Omni's prediction accuracy over attack accuracy is about 53% (median value) across all datasets, with about 18% (median value) loss rate when comparing pre-attack accuracy and Omni's prediction accuracy.

Distinguish Security Bug Reports with Hyperparameter Optimization Aug, 2018 - Oct, 2019
NSF Funded Research Project, Software Engineering Lab, North Carolina State University

- Proposed a dual optimizer SWIFT that optimizes both machine learning learners and pre-processor options.
- Applied a novel technique called ϵ-dominance that learns how to avoid evaluation operations that do not significantly improve performance.
- Performed a thorough evaluation comparison with no optimization and individual optimization strategies of learners or pre-processors.

AWS Hadoop Cluster Anomaly Detection May, 2018 - Jul, 2018
Software Engineer Internship, Insightfinder Inc. Raleigh, NC

- Created an automatic tool that fetches runtime system logs of Hadoop clusters.
- Applied a log-based anomaly detection engine built on Self-Organizing Map (SOM) to monitor Hadoop clusters.

Discover Security Vulnerabilities of Docker Images on Docker Hub Jul, 2015 - Aug, 2016
NSF Funded Research Project, System Lab, North Carolina State University

- Built Docker Image Vulnerabilities Analysis (DIVA) system framework to automatically discover, download Docker images from Docker Hub, and analyzed image vulnerabilities with Quay Security Scanner (Clair).
- Analyzed Docker images dependency relationship and vulnerability propagation pattern on Docker Hub.

SELECTED COURSE PROJECTS

Detect Security Vulnerabilities in OpenMRS Jan, 2020 - May, 2020

Graduate Course Project, Software Security, North Carolina State University

- Created black-box test cases that map to ASVS standards, and performed static security analysis with Fotify and Coverity.
- Performed fuzzing testing with OWASP ZAP and Synopsys Defensics, and analyzed vulnerable dependencies with tools as OWASP-Dependency-Check, RedHat Victims, GitHub's checker, Sonatype DepShield and Snyk.
- Performed interactive application security testing with Synopsys Seeker and performed vulnerability discovery comparison between different detecting strategies.

Continuous Integration/Delivery Pipeline Jan, 2019 - May, 2019

Graduate Course Project, DevOps, North Carolina State University

- Integrated Ansible, Docker, Jenkins and Prometheus that atomically provision, configure, monitor and test iTrust and checkbox.io applications in AWS.
- Details at Deploy-Infra_Milestone, CM-Build_Milestone, Test-Analysis_Milestone.

Port Knocking Attack Aug, 2016 - Dec, 2016

Graduate Course Project, Network Security, North Carolina State University

- Implemented the Port Knocking attack in C language, i.e., when server receives right sequence of packets from client, it fetches remote malicious script and runs locally.

PUBLICATIONS

- **Rui Shu**, Tianpei Xia, Laurie Williams, Tim Menzies, ***Omni: Automated Ensemble with Unexpected Models against Adversarial Evasion Attack)***, Empirical Software Engineering (EMSE) (Under Review), 2020.
- **Rui Shu**, Tianpei Xia, Laurie Williams, Tim Menzies, ***How to Better Distinguish Security Bug Reports (using Dual Hyperparameter Optimization)***, Empirical Software Engineering (EMSE), 2020.
- Sarah Elder, Nusrat Zahan, **Rui Shu**, Monica Metro, Val Kozarev, Tim Menzies, Laurie Williams, ***No Sonic Screwdriver: An empirical study of vulnerability detection techniques on a Java application***, USENIX Security (Under Review), 2020.
- Sarah Elder, Nusrat Zahan, Val Kozarev, **Rui Shu**, Tim Menzies, Laurie Williams, ***Structuring a Comprehensive Software Security Course Around the OWASP Application Security Verification Standard***, 43rd International Conference on Software Engineering, Joint Track on Software Engineering Education and Training (ICSE-JSEET), 2021.
- Tianpei Xia, Wei Fu, **Rui Shu**, Tim Menzies, ***Predicting Project Health for Open Source Projects (using the DECART Hyperparameter Optimizer)***. Empirical Software Engineering (EMSE) (Under Review), 2020.
- Tianpei Xia, **Rui Shu**, Xipeng Shen, Tim Menzies, ***Sequential Model Optimization for Software Effort Estimation***. Transactions on Software Engineering (TSE), 2020.
- **Rui Shu**, Xiaohui Gu, William Enck, ***A Study of Security Vulnerabilities on Docker Hub***, Proceedings of the 7th ACM Conference on Data and Application Security and Privacy (CODASPY), Scottsdale, Arizona, March 2017.
- **Rui Shu**, Peipei Wang, Sigmund A. Gorski III, Benjamin Andow, Adwait Nadkarni, Luke Deshotels, Jason Gionta, William Enck and Xiaohui Gu, ***A Study of Security Isolation Techniques***, ACM Computing Surveys CSUR, 49.3 (October 2016): 50