Yuru Shao

4917 BBB, 2260 Hayward St,
University of Michigan,
Ann Arbor, MI 48109

Email: yurushao@umich.edu
Homepage: yurushao.info
Tel: (+1) 734-545-9557

RESEARCH INTERESTS

My research focuses on the study of security threats in software and cyber-physical systems through systematic problem analysis. I have built systems and tools to facilitate security audits of Android frameworks and applications, and used them to identify and correct bad practices and vulnerabilities. I have been working on bringing software-defined approaches to the control and security of smart manufacturing systems.

EDUCATION

University of Michigan, Ann Arbor — 08/2014-present
PhD student in Computer Science and Engineering
- Advisor: Professor Z. Morley Mao

University of Michigan, Ann Arbor — 08/2014-05/2016
Master of Science in Computer Science and Engineering

Wuhan University, Wuhan, China — 09/2009-06/2013
Bachelor of Engineering in Computer Science

PUBLICATIONS

Lei Xue, Chenxiong Qian, Hao Zhou, Xiapu Luo, Yajin Zhou, Yuru Shao, Alvin T.S. Chan. NDroid: Towards Tracking Information Flows Across Multiple Android Contexts, *IEEE Transactions on Information Forensics & Security (TIFS), March 2019*.

Felipe Lopez, Yuru Shao, Z. Morley Mao, James Moyne, Kira Barton, Dawn Tilbury. A software-defined framework for the integrated management of smart manufacturing systems, *Manufacturing Letters, Vol. 15, Jan. 2018*.

Felipe Lopez, Miguel Saez, Yuru Shao, Efe Balta, James Moyne, Morley Mao, Kira Barton, and Dawn Tilbury, Categorization of Anomalies in Smart Manufacturing Systems to Support the Selection of Detection Mechanisms, *13th IEEE Conference on Automation Science and Engineering (CASE), 2017*.

Yuru Shao, Jason Ott, Yunhan Jack Jia, Zhiyun Qian, and Z. Morley Mao, The Misuse of Android Unix Domain Sockets and Security Implications, *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS), 2016*.

Yuru Shao, Jason Ott, Qi Alfred Chen, Zhiyun Qian, and Z. Morley Mao, Kratos: Discovering Inconsistent Security Policy Enforcement in the Android Framework, *Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS), 2016*.

Qi Alfred Chen, Zhiyun Qian, Yunhan Jia, Yuru Shao, and Z. Morley Mao, Static Detection of Packet Injection Vulnerabilities — A Case for Identifying Attacker-controlled Implicit Information Leaks, *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS), 2015*.

Yuru Shao, Xiapu Luo, and Chenxiong Qian, Towards a Salable Resource-driven Approach for Detecting Repackaged Android Applications, *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC), 2014*.

Yuru Shao, Xiapu Luo, and Chenxiong Qian, RootGuard: Protecting Rooted Android Phones, *IEEE Computer 47(6): 32-40, 2014*.

Chenxiong Qian, Xiapu Luo, and Yuru Shao, NDroid: Tracking Information Leaks through Java Native Interface in Android Apps, *Proceedings of the 44th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2014*.

RECENT PROJECTS

An automated approach to generating device-level security configurations for smart manufacturing systems 04/2018-present

- Smart manufacturing systems expose communication interfaces in order to support connectivity and interoperability, which inevitably expand the attack surfaces.
- We analyze manufacturing network traffic collected from a Rockwell full-fledged testbed to identify underutilized security features, and study over 800 real-world programmable controller (PLC) programs to identify bad practices that cause unnecessary exposure of PLC internal states.
- We develop tools that automate the analyses and suggest secure device-level configurations.

A software-defined control framework for the agile reconfiguration of smart manufacturing systems 06/2017-present

- We abstract low-level functionality of distributed control devices in a middleware architecture that has a centralized view of the manufacturing system.
- We design a central controller that provides flexible APIs to developers and empowers them to implement apps to improve productivity, quality, and security.

Security study of native inter-process communication (IPC) channels on Android 08/2015-05/2016

- Investigated app attack vectors exposed through Linux IPC channels that are not protected by SEAndroid
- Developed a toolset that uses static and runtime analyses to detect vulnerable apps and high-privileged system daemons
- Designed SEAndroid improvements and a secure native IPC framework

Detecting inconsistent security policy enforcement in the Android framework 08/2014-08/2015

- Analyzed and categorized security checks implemented in the Android framework
- Developed static analysis tool that can systematically detect inconsistent security policy enforcement without relying on exact knowledge of security polices
- Applied tool to various versions of Android, discovered more than 10 zero-day vulnerabilities

WORK EXPERIENCE

Graduate Research Assistant 08/2014-present
Department of EECS, University of Michigan

Intern 06/2018-08/2018
Secure Application Frameworks (SAF), Facebook

Research Intern 06/2016-08/2016, 05/2017-08/2017
Security and Services Lab (SSL), Samsung Research America

	Research Assistant Department of Computing, The Hong Kong Polytechnic University	11/2013-07/2014

HONORS & AWARDS

Google Summer of Code, the Honeynet Project	2017
CCS Student Travel Grant, ACM	2016
Rackham Travel Grant, University of Michigan	2015, 2016
USENIX Security Student Travel Grant, USENIX Association	2015
Outstanding Undergraduate Award, China Computer Federation	2012
Google Excellence Scholarship, Google	2012
National Scholarship, Ministry of Education, China	2010