

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 problems in emerging mobile and smart manufacturing platforms. I have built systems and tools to facilitate security audits of Android frameworks and applications, and used them to discover 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 08/2014-04/2019 (expected)
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

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, Dec. 2017.

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

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

- Abstract low-level functionality of control devices in a middleware architecture that has a centralized view of the manufacturing system
- Design a central controller that provides flexible APIs to developers, who are able to implement apps to improve productivity, quality, and security

Google summer of code 2017: Conpot 05/2017-08/2017

- Conpot is an Industrial Control System (ICS) honeypot under The HoneyNet Project that collects intelligence about the motives and methods of adversaries targeting ICS
- Improved Conpot's Modbus protocol and fixed bugs including those coming from dependent libraries
- Added Ethernet/IP support to Conpot, providing both TCP and UDP Ethernet/IP honeypots

Security study of native IPC channels on Android 08/2015-05/2016

- Studied Android inter-process communication (IPC) mechanisms inherited from Linux
- Investigated app attack vectors exposed through Linux IPC channels, which are not protected by SEAndroid
- Developed a toolset that uses static analysis and dynamic profiling to detect vulnerable apps and system daemons

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 policies
- 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

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

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

SKILLS

Programming: Java, Python, C/C++, Scala, Shell
Tools: Vim, Git, IDA Pro, Matlab, Hadoop, Neo4j

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
National Scholarship, Ministry of Education, China

2012
2010