Jianliang Wu

Ph.D Student

wu1220@purdue.edu

Education

Purdue University *West Lafayette, IN, USA*

Ph.D in Computer Science *Aug. 2017 - Present*

- Co-advised by Dongyan Xu and Antonio Bianchi

Shandong University *Jinan, Shandong, China*

M.E in Computer Science *Aug. 2012 - May. 2015*

- Advised by Shanqing Guo

Shandong University *Jinan, Shandong, China*

B.S in Computer Science *Aug. 2008 - May. 2012*

- Overall GPA: 85%

Research Interests

IoT Security, System Security, Mobile Security, Program Analysis, Binary Analysis

Skills

Program Languages Python, Java, C, Assembly (X86, ARM)

Research Tools LLVM, IDA pro, Ghidra, Angr

Work Experience

FRIENDS lab, Purdue University *West Lafayette, IN*

Research Assistant *Aug. 2017 - PRESENT*

- IoT security research.
- Currently focusing on Bluetooth stack security starting from the firmware up to the application security. Binary analysis is used for firmware analysis when source code is not available. While compiler-based (LLVM) program analysis is used at the higher level when source code is available.
- Bluetooth Low Energy spoofing attack against mobile phones and device agnostic defense.

People's Bank of China, Jinan Branch *Jinan, China*

Senior Staff Member *Aug. 2015 - Jun. 2017*

- System maintenance.
- I was responsible for the maintenance of the systems running on the branch's servers.

Software Engineering Lab, NUS *Singapore*

Research Assistant *Oct. 2013 - Apr. 2014*

- Mobile security research combined with formal methods.
- Investigating authentication information leakage via backup channel in Android.

Security Research Lab, Shandong University *Jinan, China*

Research Assistant *Aug. 2012 - May. 2015*

- Mobile security research.
- Detecting Android application permission misuse (potential confused deputy applications) based on program analysis.

Recent Projects

Bluetooth stack multi-layer debloating *In progress*

Debloating Bluetooth stack on multi-layers from the firmware up to the application layers. We use binary analysis techniques for firmware debloating when no source code is available. At the higher level where source code is available, we use the compiler (LLVM) based program analysis techniques to do analysis and debloating.

BlueShield: Detecting Spoofing Attacks in Bluetooth Low Energy Networks *In submission*

We discovered a new vulnerability in Android and iOS Bluetooth Low Energy (BLE) stack so that an attacker can lunch spoofing attacks against the user even if the user's phone is paired with the BLE devices. To detect all spoofing attacks no matter if the attacker utilizes the vulnerability or not, we design and implement a device-agnostic detecting framework that uses physical BLE device features and BLE protocol features.

Publications

Automatically detecting ssl error-handling vulnerabilities in hybrid mobile web apps *2015*

Zuo, Chaoshun, **Jianliang Wu**, and Shanqing Guo.
In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS).

All your sessions are belong to us: Investigating authenticator leakage through backup channels on Android *2015*

Bai, Guangdong, Jun Sun, **Jianliang Wu**, Quanqi Ye, Li Li, Jin Song Dong, and Shanqing Guo.
In 2015 20th International Conference on Engineering of Complex Computer Systems (ICECCS)
Best Paper Award

PaddyFrog: systematically detecting confused deputy vulnerability in Android applications *2015*

Wu, Jianliang, Tingting Cui, Tao Ban, Shanqing Guo, and Lizhen Cui.
Security and Communication Networks 8 (SCN).

TrustFound: Towards a Formal Foundation for Model Checking Trusted Computing Platforms *2014*

Bai, Guangdong, Jianan Hao, **Jianliang Wu**, Yang Liu, Zhenkai Liang, and Andrew Martin.
In International Symposium on Formal Methods (FM).

Honors & Awards

Best Paper Award *2015*

All your sessions are belong to us: Investigating authenticator leakage through backup channels on Android

Talks & Presentations

BlueShield: Detecting Spoofing Attacks in Bluetooth Low Energy Networks *Oct. 2019*

Navy Crane visitors meeting