# JIANLIANG WU

PH.D. CANDIDATE

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

## PUBLICATIONS

**Formal Model-Driven Discovery of Bluetooth Protocol Design Vulnerabilities.** *Jianliang Wu*, Ruoyu Wu, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2022

**ProFactory: Improving IoT Security via Formalized Protocol Customization.** Fei Wang, *Jianliang Wu*, Yuhong Nan, Yousra Aafer, Xiangyu Zhang, Dongyan Xu, and Mathias Payer. In Proceedings of the USENIX Security Symposium (Security), 2022

**LIGHTBLUE: Automatic Profile-Aware Debloating of Bluetooth Stacks.** *Jianliang Wu*, Ruoyu Wu, Daniele Antonioli, Mathias Payer, Nils Ole Tippenhauer, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. In Proceedings of the USENIX Security Symposium (Security), 2021

**BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy**. *Jianliang Wu*, Yuhong Nan, Vireshwar Kumar, Dave (Jing) Tian, Antonio Bianchi, Mathias Payer, and Dongyan Xu. In Proceedings of the USENIX Workshop on Offensive Technologies (WOOT), 2020.

**Best Paper Award** **CSAW'20 Applied Research Competition Finalist**

**BlueShield: Detecting Spoofing Attacks in Bluetooth Low Energy (BLE) Networks.** *Jianliang Wu*, Yuhong Nan, Vireshwar Kumar, Mathias Payer, and Dongyan Xu. In Proceedings of International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2020.

**All your sessions are belong to us: Investigating authenticator leakage through backup channels on Android.** Guangdong Bai, 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), 2015.

**Best Paper Award**

**PaddyFrog: systematically detecting confused deputy vulnerability in Android applications.** *Jianliang Wu*, Tingting Cui, Tao Ban, Shanqing Guo, and Lizhen Cui. Security and Communication Networks (SCN), vol. 8 no. 13 (2015).

**Automatically detecting ssl error-handling vulnerabilities in hybrid mobile web apps.** Chaoshun Zuo, *Jianliang Wu*, and Shanqing Guo. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (AsiaCCS), 2015.

**TrustFound: Towards a Formal Foundation for Model Checking Trusted Computing Platforms.** Guangdong Bai, Jianan Hao, *Jianliang Wu*, Yang Liu, Zhenkai Liang, and Andrew Martin. In International Symposium on Formal Methods (FM), 2014.

## Work Experience

**PurSec lab, Purdue University** *West Lafayette, IN*
Research Assistant *Aug. 2017 - PRESENT*
- IoT security research.

**People's Bank of China, Jinan Branch** *Jinan, China*
Senior Staff Member *Aug. 2015 - Jun. 2017*
- System maintenance.

**Software Engineering Lab, NUS** *Singapore*
Research Assistant *Oct. 2013 - Apr. 2014*
- Mobile security research combined with formal methods.

**Security Research Lab, Shandong University** *Jinan, China*
Research Assistant *Aug. 2012 - May. 2015*
- Mobile (Android) security research.

## Honors & Awards

**Best Paper Award** *2020*
BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy

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

**First Prize of Scientific and Technical Innovation** *2011*

**First Prize of Shandong Province in MCM** *2010*

## Talks & Presentations

**Formal Model-Driven Discovery of Bluetooth Protocol Design Vulnerabilities** *May. 2022*
43rd IEEE Symposium on Security and Privacy (S&P'22)

**LIGHTBLUE: Automatic Profile-Aware Debloating of Bluetooth Stacks** *Aug. 2021*
30th USENIX Security Symposium (Security'21)

**BlueShield: Detecting Spoofing Attacks in Bluetooth Low Energy Networks** *Oct. 2020*
23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID'20)

**BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy** *Sep. 2020*
21st CERIAS Annual Security Symposium

**BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy** *Aug. 2020*
14th USENIX Workshop on Offensive Technologies (WOOT'20)

## Professional Services

**PC member**
IEEE/ACIS International Conference on Software Engineering, Management and Applications (SERA) *2022*
CSAW Applied Research Competition *2021*

**Reviewer**
IEEE Network Magazine *2021*
Computer Networks *2021*

**Subreviewer**
IEEE Symposium on Security and Privacy (S&P) *2021, 2022*
USENIX Security Symposium (Security) *2022*
Network and Distributed System Security Symposium (NDSS) *2021, 2022, 2023*
ACM Asia Conference on Computer and Communications Security (AsiaCCS) *2022*
Conference on Dependable Systems and Networks (DSN) *2020*
EAI International Conference on Security and Privacy in Communication Networks (SecureComm) *2020*

## Media Coverage

**Security Boulevard: “Bluetooth Reconnection Flaw Could Lead to Spoofing Attacks”**
https://securityboulevard.com/2020/07/bluetooth-reconnection-flaw-could-lead-to-spoofing-attacks/

**Remark Board: “Billions of devices vulnerable to new ’BLESA’ Bluetooth security flaw”**
https://remarkboard.com/m/researchers-unveil-a-bluetooth-le-attack-impacting-billions/1eztwiylfko6v

**Sec News: “BLESA: billions of devices vulnerable to Bluetooth security flaw”**
https://en.secnews.gr/267536/bluetooth-flash/

**Editorials 360: “Billions of Units Susceptible To New ’BLESA’ Bluetooth Spoofing Assault”**
https://www.editorials360.com/2020/09/17/billions-of-units-susceptible-to-new-blesa-bluetooth-spoofing-assault/

**Threats Hub: “Billions of devices vulnerable to new ‘BLESA’ Bluetooth security flaw”**
https://www.threatshub.org/blog/billions-of-devices-vulnerable-to-new-blesa-bluetooth-security-flaw/

**Cyware: “Cyware Daily Threat Intelligence, September 16, 2020”**
https://cyware.com/daily-threat-briefing/cyware-daily-threat-intelligence-september-16-2020-bc5d

**Google News Post: “Critical Bluetooth safety vulnerability may just have an effect on billions of gadgets international”**
http://googlenewspost.com/2020/09/16/critical-bluetooth-security-vulnerability-could-affect-billions-of-devices-worldwide/

**How To Fix: “Experts discovered BLESA attack, to which are vulnerable billions of Bluetooth devices”**
https://howtofix.guide/experts-discovered-blesa-attack-to-which-are-vulnerable-bluetooth-devices/

**Sensors Tech Forum: “Bluetooth Low Energy Spoofing Attack Endangers Billions of Devices”**
https://sensorstechforum.com/blesa-attack-endangers-billions-devices/

**Silicon Angle: “Vulnerability in the Bluetooth software stack opens the door to hackers”**
https://siliconangle.com/2020/09/16/vulnerability-bluetooth-software-stack-opens-door-hackers/

**International Business Times: “What Is BLESA? Hackers Can Potentially Target Billions of Devices with Bluetooth Security Flaw”**
https://www.ibtimes.sg/what-blesa-hackers-can-potentially-target-billions-devices-bluetooth-security-flaw-51582

**TechRadar: “Critical Bluetooth security vulnerability could affect billions of devices worldwide”**
https://www.techradar.com/news/critical-bluetooth-security-vulnerability-could-affect-billions-of-devices-worldwide

**SysDVD: “Billions of Bluetooth Devices Vulnerable to BLESA Attack – Hacker”**
http://sysdvd.com/billions-of-bluetooth-devices-vulnerable-to-blesa-attack-hacker/

**Tom’s Guide: “Billions of Android phones and smart devices open to attack – what to do now”**
https://www.tomsguide.com/news/blesa-bluetooth-attack

**ThreatPost: “Bluetooth Spoofing Bug Affects Billions of IoT Devices”**
https://threatpost.com/bluetooth-spoofing-bug-iot-devices/159291/

**NetSec.news: “Billions of Devices Vulnerable to ‘BLESA’ Bluetooth Spoofing Vulnerability”**
https://www.netsec.news/billions-of-devices-vulnerable-to-blesa-bluetooth-spoofing-vulnerability/

**ZDNet: “Billions of devices vulnerable to new ’BLESA’ Bluetooth security flaw”**
https://www.zdnet.com/article/billions-of-devices-vulnerable-to-new-blesa-bluetooth-security-flaw/

**Slashdot: “Billions of Devices Vulnerable To New ’BLESA’ Bluetooth Spoofing Attack”**
https://it.slashdot.org/story/20/09/16/220211/billions-of-devices-vulnerable-to-new-blesa-bluetooth-spoofing-attack

**AppleInsider: “’BLESA’ Bluetooth vulnerability impacts billions of devices, but iOS users are safe”**
https://appleinsider.com/articles/20/09/17/blesa-bluetooth-vulnerability-impacts-billions-of-devices-but-ios-users-are-safe

**ITSecurity Wire: “‘BLESA’ Bluetooth Security Flaw Could Affect Billions of Devices”**
https://itsecuritywire.com/quick-bytes/blesa-bluetooth-security-flaw-could-affect-billions-of-devices/

**Digital Information World: “The new BLESA Bluetooth security flaw can keep billions of devices vulnerable”**
https://www.digitalinformationworld.com/2020/09/the-new-blesa-bluetooth-security-flaw-can-keep-billions-of-devices-vulnerable.html

**Bitdefender BOX: “New ‘BLESA’ Bluetooth Vulnerability Could Affect Billions of IoT Devices, Researchers Warn”**
https://www.bitdefender.com/box/blog/iot-news/new-blesa-bluetooth-vulnerability-affect-billions-iot-devices-researchers-warn

**DAZEINFO: “BLESA: The New Bluetooth Vulnerability Putting Billions of Devices At Risk”**
https://dazeinfo.com/2020/09/17/bluetooth-vulnerability-blesa-devices-rick/

**myce: “BLESA Bluetooth Flaw Affects IoT Devices”**
https://www.myce.com/news/blesa-bluetooth-flaw-affects-iot-devices-94440/