JIANLIANG WU

ASSISTANT PROFESSOR

8888 University Drive, Burnaby, British Columbia, V5A 1S6, Canada

wujl@sfu.ca | https://allenjlw.github.io/

Work Experience

Simon Fraser University — *Burnaby, BC, CA*
Assistant Professor — *Jan. 2024 - Present*

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

Education

Purdue University — *West Lafayette, IN, USA*
Ph.D. in Computer Science — *Aug. 2017 - Jun. 2023*

Shandong University — *Jinan, Shandong, China*
M.E. in Computer Science — *Aug. 2012 - May. 2015*

Shandong University — *Jinan, Shandong, China*
B.S. in Computer Science — *Aug. 2008 - May. 2012*

Research Interests

My research investigates Systems Security at both the design and implementation levels to secure diverse computing platforms, especially devices directly interacting with users and surrounding environments, aiming to improve the security of real-world computing devices by leveraging and combining formal analysis, program analysis, machine learning, etc.

Research Funding

Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Launch Supplement — *Apr. 2024*
CAD 12,500

Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery — *Apr. 2024 - Apr. 2029*
CAD 205,000

SFU Start-up Grant — *Jan. 2024 - Dec. 2028*
CAD 150,000

Student Supervision

Zidong Zhang — *Aug. 2024 - Present*
Simon Fraser University — *MSc*

Ashkan Jangodaz — *Start from Aug. 2025*
Simon Fraser University — *PhD*

Hao Wen — *Start from Aug. 2025*
Simon Fraser University — *PhD*

Yuan Ye — *Start from Aug. 2025*
Simon Fraser University — *PhD*

Munim Hasan Wasi — *Start from Aug. 2025*
Simon Fraser University — *MSc*

Xiaofeng Liu — *Aug. 2023 - Jun. 2025*
Shandong University — *PhD, Co-advised with Shanqing Guo*

Publications

Formalization, Implementation, and Verification of the Bluetooth L2CAP State Machine. Tan Khang Le, Mohammad Omidvar Tehrani, Yuepeng Wang, *Jianliang Wu*, Steven Y. Ko. In Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom), 2025.

MBFuzzer: A Multi-Party Protocol Fuzzer for MQTT Brokers. Xiangpu Song, *Jianliang Wu*, Yingpei Zeng, Hao Pan, Chaoshun Zuo, Qingchuan Zhao, Shanqing Guo. In Proceedings of the USENIX Security Symposium (Security), 2025.

Why Am I Seeing Double? An Investigation of Device Management Flaws in Voice Assistant Platforms. M. Ozgur Ozmen, M. Oguz Sakaoglu, Jackson Bizjak, *Jianliang Wu*, Antonio Bianchi, Dave (Jing) Tian, and Z. Berkay Celik. In Proceedings of the Privacy Enhancing Technologies (PoPETS), 2025.

A Thorough Security Analysis of BLE Proximity Tracking Protocols. Xiaofeng Liu, Chaoshun Zuo, Qinsheng Hou, Pengcheng Ren, *Jianliang Wu*, Qingchuan Zhao, Shanqing Guo. In Proceedings of the USENIX Security Symposium (Security), 2025.

VeriBin: Adaptive Verification of Patches at the Binary Level. Hongwei Wu, *Jianliang Wu*, Ruoyu Wu, Ayushi Sharma, Aravind Machiry, and Antonio Bianchi. In Proceedings of the Network and Distributed System Security Symposium (NDSS), 2025.

CSFuzzer: A grey-box fuzzer for network protocol using context-aware state feedback. Xiangpu Song, Yingpei Zeng, *Jianliang Wu*, Hao Li, Chaoshun Zuo, Qingchuan Zhao, Shanqing Guo. Computers & Security, Volume 157, (2025), 104581.

Securing Bluetooth Across Layers: A Systematic Review of Protection Strategies. *Jianliang Wu*, Ruoyu Wu, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. 2025. GetMobile: Mobile Comp. and Comm. 29, 1 (2025), 5–8.

Finding Traceability Attacks in the Bluetooth Low Energy Specification and Its Implementations. *Jianliang Wu*, Patrick Traynor, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. In Proceedings of the USENIX Security Symposium (Security), 2024.

SoK: The Long Journey of Exploiting and Defending the Legacy of King Harald Bluetooth. *Jianliang Wu*, Ruoyu Wu, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2024.

Are You Spying on Me? Large-Scale Analysis on IoT Data Exposure through Companion Apps. Yuhong Nan, Xueqiang Wang, Luyi Xing, Xiaojing Liao, Ruoyu Wu, *Jianliang Wu*, Yifan Zhang, and XiaoFeng Wang. In Proceedings of the USENIX Security Symposium (Security), 2023.

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 Proceedings of the 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 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.

Honors & Awards

Dean's Excellence Fellowship, SFU *Jan. 2024 - Dec. 2026*
Best Paper Award, WOOT *2020*
Best Paper Award, ICECCS *2015*
First Prize of Scientific and Technical Innovation *2011*

Talks & Presentations

Securing Bluetooth Protocols from Their Designs to Implementations *Aug. 2024*
Zhejiang University

Finding Traceability Attacks in the Bluetooth Low Energy Specification and Its Implementations *Aug. 2024*
33rd USENIX Security Symposium (Security'24)

SoK: The Long Journey of Exploiting and Defending the Legacy of King Harald Bluetooth *May. 2024*
43rd IEEE Symposium on Security and Privacy (S&P'24)

Securing IoT Systems via Protocol Formal Analysis and Debloating *Jul. 2023*
Shandong University

Attack and Defense Practices against Bluetooth Protocols *Jul. 2023*
Shanghai Jiao Tong University

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)

Teaching

CMPT 403 System Security and Privacy
Instructor, SFU *Fall, 2025*
CMPT 479/982 Systems Security Research Seminar
Instructor, SFU *Fall, 2025*
CMPT 479/982 Mobile Security
Instructor, SFU *Spring, 2025*
CMPT 789 Applied Crypto
Instructor, SFU *Fall, 2024*
CMPT 471 Networking II
Instructor, SFU *Spring, 2024*
Software Security
Guest lecture, invited by Dr. Antonio Bianchi at Purdue *2022*
IoT/CPS Security
Guest lecture, invited by Dr. Z. Berkay Celik at Purdue *2022*

Professional Services

Conference Organizing Committee
ASAP, Local arrangement chair *2025*
IWQoS, Publicity chair *2025*
Conference TPC member

IEEE S&P	*2026*
ICDCS	*2025*
AsiaCCS	*2025*
USENIX Security	*2025*
RAID	*2024*
IEEE/ACIS International Conference on Software Engineering, Management and Applications (SERA)	*2022*
CSAW Applied Research Competition	*2021, 2023, 2024*

Journal Reviewer

IEEE Internet of Things Journal	*2024*
IEEE Transactions on Dependable and Secure Computing	*2022, 2023, 2024*
Journal of Information Security and Applications	*2022*
IEEE Network Magazine	*2021, 2024*
Computer Networks	*2021*

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/