JINWEN WANG

https://j1nwenwang.github.io

EDUCATION

Washington University in St. Louis *Sep 2019 - Present*
Ph.D. in Computer Science

Tsinghua University *Sep 2016 - Jun 2019*
M.S. in Computer Science

Sichuan University *Sep 2012 - Jun 2016*
B.E. in Computer Science

RESEARCH INTERESTS

System Security, Software Security, Cyber-Physical System

PUBLICATIONS

Main Conference Papers (first author publications highlighted)

[**Security 24**]**Opportunistic Data Flow Integrity for Real-time Cyber-physical Systems Using Worst Case Execution Time Reservation.** Yujie Wang, Ao Li, **Jinwen Wang**, Sanjoy Baruah, and Ning Zhang, *International Conference on Real-Time Networks and Systems*, 2024.

[**Security 24**]**Your Firmware Has Arrived: A Study of Firmware Update Vulnerabilities.** Yuhao Wu, **Jinwen Wang**, Yujie Wang, Shixuan Zhai, Zihan Li, Yi He, Kun Sun, Qi Li, and Ning Zhang, *International Conference on Real-Time Networks and Systems*, 2024.

[**CCS 23**] **Secure and Timely GPU Execution in Cyber-physical Systems.** **Jinwen Wang**, Yujie Wang, and Ning Zhang, *ACM Conference on Computer and Communications Security*, 2023.

[**Security 23**] **ARI: Attestation of Real-time Mission Execution Integrity.** **Jinwen Wang**, Yujie Wang, Ao Li, Yang Xiao, Ruide Zhang, Wenjing Lou, Y. Thomas Hou, and Ning Zhang, *USENIX Security Symposium*, 2023.

[**DAC 23**] **IP Protection in TinyML.** **Jinwen Wang**, Yuhao Wu, Han Liu, Bo Yuan, Roger Chamberlain, and Ning Zhang, *ACM/IEEE Design Automation Conference*, 2023, (Acceptance Rate: 23%).

[**RTNS 23**]**A Procrastinating Control-Flow Integrity Framework for Periodic Real-Time Systems.** Tanmaya Mishra, **Jinwen Wang**, Thidapat Chantem, Ryan Gerdes and Ning Zhang, *International Conference on Real-Time Networks and Systems*, 2023.

[**Oakland 22**] **RT-TEE: Real-time System Availability for Cyber-physical Systems using ARM TrustZone.** **Jinwen Wang**, Ao Li, Haoran Li, Chenyang Lu, and Ning Zhang, *IEEE Symposium on Security and Privacy*, 2022, (Acceptance Rate: 147/1012=14.5%).

[**IROS 22**] **From Timing Variations to Performance Degradation: Understanding and Mitigating the Impact of Software Execution Timing in SLAM.** Ao Li, Han Liu, **Jinwen Wang**, and Ning Zhang, *IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2022.

Journal Papers

[**TON 23**] **Interface-Based Side Channel in TEE-Assisted Networked Services** Xiaohan Zhang, **Jinwen Wang**, Yueqiang Cheng, Qi Li, Kun Sun, Yao Zheng, Ning Zhang, and Xinghua Li, *IEEE/ACM Transactions on Networking*, 2023.

Workshop Papers

[**VehicleSec 23**] **Demo: Real-time System Availability for Cyber-physical Systems using ARM TrustZone.** **Jinwen Wang**, Ao Li, Haoran Li, Chenyang Lu, and Ning Zhang, *Inaugural Symposium on Vehicle Security and Privacy*, 2023.

[**RTSS 22**] **Work-in-Progress: Measuring Security Protection in Real-time Embedded Firmware.** Yuhao Wu, Yujie Wang, Shixuan Zhai, Zihan Li, Ao Li, **Jinwen Wang**, and Ning Zhang, *IEEE Real-Time Systems Symposium*, 2022.

[**CCS 21**] **Chronos: Timing Interference as a New Attack Vector on Autonomous Cyber-physical Systems.** Ao Li, **Jinwen Wang**, and Ning Zhang, *ACM SIGSAC Conference on Computer and Communications Security*, 2021.

AWARDS

Qualcomm Best Demo Award Runner Up	*2023*
Travel Grant in RTSS	*2022*
Dean's International Fellowship	*2019*
National Scholarship in China	*2013*

SERVICES

Subreviewers:

IEEE/ACM Transactions on Networking

External Reviewer:

IEEE S&P, Usenix Security, IEEE ACSAC	*2024*
IEEE EuroS&P, ACM Asia CCS	*2023*
ACM CCS, ACM Asia CCS, IEEE INFOCOM	*2022*
ISOC NDSS, IEEE INFOCOM	*2021*
ISOC NDSS, IEEE INFOCOM	*2020*
IEEE INFOCOM	*2019*