

JINWEN WANG

<https://jinwenwang.github.io>

EDUCATION

Washington University in St. Louis
Ph.D. in Computer Science (GPA 3.88/4.0)

Sep 2019 - Present

Tsinghua University
M.S. in Computer Science (Rank 2/29)

Sep 2016 - Jun 2019

Sichuan University
B.E. in Computer Science (Rank Top 10%)

Sep 2012 - Jun 2016

RESEARCH INTERESTS

System Security, Software Security, Cyber-Physical System

PUBLICATIONS

Main Conference Papers

[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*, 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.

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.

SKILLS

Programming languages: C, C++, and Python.

Kernel Programming: Linux kernel modification, device driver modification.

Compiler Customization: Software Instrumentation using LLVM, GCC.

Reverse Engineering: Ghidra

AWARDS

| | |
|------------------------------------|-------------|
| Qualcomm Best Demo Award Runner Up | <i>2023</i> |
| Travel Grant in RTSS | <i>2022</i> |
| Dean's International Fellowship | <i>2019</i> |
| National Scholarship in China | <i>2013</i> |

SERVICES

Subreviewers:

IEEE/ACM Transactions on Networking

External Reviewer:

2023: IEEE EuroS&P, ACM Asia CCS

2022: ACM CCS, ACM Asia CCS, IEEE INFOCOM

2021: ISOC NDSS, IEEE INFOCOM

2020: ISOC NDSS, IEEE INFOCOM

2019: IEEE INFOCOM