Yang Longlong

Shanghai | LinkedIn | +8619821217077 | Email | GitHub

EDUCATION

Sichuan University **Chengdu**
B.Eng. in Software Engineering *2014.09 – 2018.06*

- Second Prize of LanQiao Cup, Cert. Num. 010602054.
- Software copyright registered under the number 2017SR355413.

Sichuan University **Chengdu**
M.S. in Cybersecurity *2018.09 – 2021.06*

- Exam free with First-Class scholarships.
- Chinese patent registered under the number 202011539052.8.

WORK EXPERIENCE

Intel Corporation **Shanghai**
Software Engineer *2021.07-2024.10*

- Created a new DXE module to extend measurement of CPU microcode patches to TPM. This is his first commit for an open-source project. This DXE module enhanced the trusted computing security for BIOS. And he created this module after just 5 months of his joining Intel. Which shows that he have a strong ability to quickly adapt to new environments and technologies and can make significant contributions in a short period of time. This achievement demonstrates his proficiency in BIOS development, understanding of trusted computing principles, and capability to contribute to open-source projects. It also highlights his initiative in enhancing system security and his rapid integration into Intel's development ecosystem.
- Developed SPDM protocol v1.1 and v1.2 with Rust Programming Language. And the latest version can be found here. This work demonstrates his expertise in modern secure communication protocols and proficiency in Rust programming language. It highlights his skills in protocol development, cryptography, and secure system design. This project also underlines his versatility in programming languages, as he successfully applied Rust to a complex, security-critical task after 2 months of learning.
- Created an Intel TDX Connect TEE-IO provisioning agent (TPA) Module to offload SPDM session establishment and device evidence collection from TDX Module. Which is not yet open-sourced. TPA Module acts as an extension of TDX Module, will be released and signed by Intel Corporation. This project showcases his advanced expertise in secure computing technologies, particularly in Trusted Execution Environments (TEE) and Intel's Trust Domain Extensions (TDX). By developing the TPA Module, he has contributed to enhancing the efficiency and security of Intel's confidential computing infrastructure. The work involved complex architectural design to optimize system performance and security. Creating a module that meets Intel's stringent quality and security standards demonstrates his ability to work on cutting-edge, proprietary technologies while managing sensitive intellectual property. The fact that this module will be officially released and signed by Intel Corporation speaks to the quality and significance of his work.
- Led a TDX Connect TEE-IO device firmware development, which is based on Intel Agilex FPGA series. The project involved integrating complex security protocols with high-performance FPGA architecture to create a robust and efficient TEE-IO solution. His responsibilities included overseeing the entire development lifecycle, from initial design and architecture planning to implementation, testing, and optimization. By utilizing the Agilex FPGA's advanced features, we were able to create a firmware solution that balanced high-speed data processing with stringent security requirements essential for TEE applications. This project not only demonstrated his technical expertise in FPGA firmware development but also highlighted his project management skills in coordinating cross-functional teams, managing timelines, and ensuring deliverables met Intel's exacting standards.

SKILLS

Software development, Rust/C programming language, Cryptography, Confidential Computing, Good verbal and written communication, Adaptability and quick learning, Creative thinking and innovation, Strong problem-solving and analytical skills, Git version control and Team Collaboration, Mandarin/Cantonese/English speaking.