Hardware Trust, Firmware Assurance: A Rust-based Root-of-Trust for Modern Secure Systems

PRESENTER: Xiling Sun / Principal Firmware Engineer / **Microsoft**

ABSTRACT:

This paper presents a robust RoT firmware architecture and development methodology using Rust and secure RTOS – Tock. It addresses memory safety and modularity challenges in legacy C-based designs, enabling resilient and scalable RoT solutions for modern hardware systems.