Secure IoT Platform with Advanced Key Generation and Robust Cybersecurity

Lih-Yih Chiou, Zhi-Fang Chen, Jia Qi Choy,
Han-Yu Chen, Che-Yu Chang and Yin-Yin Shen
Academy of Innovative Semiconductor and Sustainable Manufacturing and Dept. Electrical Engineering,
National Cheng Kung University, Taiwan
Email: lihyih@mail.ncku.edu.tw

Radek Holý, Miroslav Vaniš, Martin Šrotýř
Deptment of Transport Telematics
Czech Technical University, Czech Republic
Email: vanismir@fd.cvut.cz

I. Introduction

The rapid growth of Internet of Things (IoT) devices in industrial environments has expanded the attack surface of critical infrastructure. Conventional embedded systems rely on software-based cryptography, which is vulnerable to side-channel attacks, firmware tampering, and physical probing, while compliance with standards such as IEC 62443 and ISO/IEC 15408 remains a significant challenge.

To address these vulnerabilities, this work presents a hardware-secure System-on-Chip (SoC) platform co-developed by National Cheng Kung University (NCKU) and Czech Technical University (CTU), integrating hardware-rooted security with a dual-core RISC-V architecture for enhanced security and high-performance cryptographic processing.

II. System Architecture

The proposed SoC adopts a dual-core RISC-V architecture consisting of an RV32 privileged core and an RV64 user core interconnected via a system bus. The RV32 core executes the two-stage secure boot process and manages cryptographic operations, while the RV64 core is activated after system initialization to run user applications. The overall system architecture is illustrated in Fig. 1.

A hardware-rooted chain of trust is established through a staged secure boot mechanism. The First Stage Boot Loader (FSBL), stored in immutable ROM, loads and decrypts the encrypted Second Stage Boot Loader (SSBL) using a PUF-derived key, after which the SSBL loads, decrypts, and verifies the user application before execution.

The security architecture further incorporates a Physical Unclonable Function (PUF)-based key generation module, AES-GCM authenticated encryption, SHA-256 hardware acceleration, and Physical Memory Protection (PMP) for hardware-enforced memory isolation.

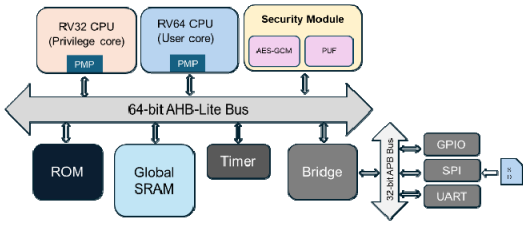

Fig. 1. System architecture

III. Security Mechanisms

To secure both device communication and system integrity, the proposed platform integrates a mutual authentication protocol and a two-stage secure boot mechanism. The mutual authentication protocol, based on asymmetric cryptography and PUF-derived device identity, provides strong resistance against replay attacks, man-in-the-middle attacks, and device spoofing by enforcing bidirectional authentication and secure session key establishment.

In addition, a hardware-rooted two-stage secure boot process ensures that only authenticated firmware is executed, establishing a continuous chain of trust across all boot stages.

IV. Experimental Results

The implemented PUF demonstrates high reliability (0.9779) and near-ideal inter-chip uniqueness, while successfully passing all NIST SP 800-22 randomness tests, validating its suitability for secure key generation.

V. Standards Compliance

The proposed platform is evaluated against the Purdue Model for Industrial Control Systems (ICS) and mapped to IEC 62443 and ISO/IEC 15408 requirements. Results indicate that the system satisfies key Security Level 1 device-layer security requirements, providing a standards-compliant solution for industrial IoT deployment.

VI. Conclusion

This work demonstrates that integrating hardware-rooted security primitives with a structured SoC architecture enables robust protection against both physical and network-based attacks while maintaining high performance. The proposed platform provides a practical foundation for secure and standards-compliant industrial IoT systems.

References

[1] M. H. Asghar, N. Mohammadzadeh, A. Negi, and T. Kazerouni, “Principal ingredients and framework of Internet of Things (IoT),” in Proc. 2015 Twelfth International Conference on Wireless and Optical Communications Networks (WOCN), 2015, pp. 1–6.

[2] M. A. Prada-Delgado, A. Vázquez-Reyes, and I. Baturone, “Trustworthy firmware update for Internet-of-Thing Devices using physical unclonable functions,” in Proc. 2017 Global Internet of Things Summit (GIoTS), 2017, pp. 0–4.