XÂY DỰNG HỆ THỐNG MÔI TRƯỜNG THỰC THI BẢO MẬT TRÊN PHẦN CỨNG

Hứa Nguyên Khang, Thái Hồng Hải, Mã Khải Minh, Lê Thành Nghị, Nguyễn Thanh Lộc, Cao Trần Bảo Thương, Lê Đức Hùng
Khoa Điện tử - Viễn thông,
Trường Đại học Khoa học Tự Nhiên, ĐHQG-HCM
ldhung@hcmus.edu.vn

Tóm tắt

Bài báo trình bày kết quả xây dựng và thiết kế hệ thống bảo mật dựa trên Root-of-Trust và Keystone Enclave. Hệ thống tận dụng ưu điểm của kiến trúc RISC-V, trong đó có kiến trúc bộ nhớ PMP (Physical Memory Protection), cho phép phân quyền người dùng ở Supervisor Mode (S-mode), Machine Mode (M-mode), User Mode (U-mode) sẽ được truy cập ở các không gian bộ nhớ, đảm bảo tính bảo mật cho các phân quyền cụ thể. Ngoài ra, bài báo trình bày quá trình xác thực Root-of-Trust ở mức thấp trong quá trình khởi động dùng thuật toán SHA3 để băm dữ liệu và ED25519 để mã hóa và chứng thực. Sau khi chuyển quyền qua hệ điều hành, các gói tin được xác thực và giám sát bởi Security Monitor trên RISC-V. Kết quả là hệ thống được viết bằng ngôn ngữ C/C++, được thực thi trên bo mạch Si-Five chứa chip RISC-V và máy tính để demo quá trình bảo mật dữ liệu. Hệ thống có thể ứng dụng trong bảo mật hệ thống Internet-of-Things (IoTs), bảo mật quá trình truyền nhận dữ liệu trong mạng từ các node, máy con đến máy chủ.

Từ khóa: Root-of-trust, security, hardware, RISC-V, Keystone, Internet-of-Things (IoTs).

IMLEMENTATION OF A TRUSTED EXECUTION ENVIRONMENT ON HARDWARE SYSTEM

Hua Nguyen Khang, Thai Hong Hai, Ma Khai Minh, Le Thanh Nghi, Nguyen Thanh Loc, Cao Tran Bao Thuong, Le Duc Hung
Faculty of Electronics and Telecommunications,
University of Science, VNU-HCM
ldhung@hcmus.edu.vn

Abstract

This paper showed the results of building and designing a trusted execution system based on Root-of-Trust and Keystone Enclave. The system prioritizes RISC-V's architecture including the advanced memory structure PMP (Protect Physical Memory), allowing users in Supervision Mode (S- mode), Machine mode (M-mode), User mode (U-mode) can access to the assigned specific memory pages, ensuring the security of each privilege. In addition,

the Root-of-Trust authentication was implemented at a lower level during the boot process using the SHA3 algorithm to hash data and ED25519 for encryption and authentication. After passing permissions to access the operating system, the packets are authenticated and monitored by Security Monitor on RISC-V. The system was successfully designed on the Si-Five development board which contains the RISC-V chip and a computer to demonstrate the operation of the trusted execution system. The system can be applied in secured Internet-of-Things (IoTs) systems, secured data transmission in the network from nodes, or clients to servers.

Keyword: Root-of-trust, security, hardware, RISC-V, Keystone, Internet-of-Things (IoTs).