World Academy of Science, Engineering and Technology
International Journal of Cognitive and Language Sciences
Vol:17, No:07, 2023

Security Design of Root of Trust Based on RISC-V

Authors : Kang Huang, Wanting Zhou, Shiwei Yuan, Lei Li

Abstract : Since information technology develops rapidly, the security issue has become an increasingly critical for computer system. In particular, as cloud computing and the Internet of Things (IoT) continue to gain widespread adoption, computer systems need to new security threats and attacks. The Root of Trust (RoT) is the foundation for providing basic trusted computing, which is used to verify the security and trustworthiness of other components. Design a reliable Root of Trust and guarantee its own security are essential for improving the overall security and credibility of computer systems. In this paper, we discuss the implementation of self-security technology based on the RISC-V Root of Trust at the hardware level. To effectively safeguard the security of the Root of Trust, researches on security safeguard technology on the Root of Trust have been studied. At first, a lightweight and secure boot framework is proposed as a secure mechanism. Secondly, two kinds of memory protection mechanism are built to against memory attacks. Moreover, hardware implementation of proposed method has been also investigated. A series of experiments and tests have been carried on to verify to effectiveness of the proposed method. The experimental results demonstrated that the proposed approach is effective in verifying the integrity of the Root of Trust's own boot rom, user instructions, and data, ensuring authenticity and enabling the secure boot of the Root of Trust's own system. Additionally, our approach provides memory protection against certain types of memory attacks, such as cache leaks and tampering, and ensures the security of root-of-trust sensitive information, including keys.

Keywords : root of trust, secure boot, memory protection, hardware security
Conference Title : ICSLP 2023 : International Conference on Speech and Language Processing
Conference Location : Stockholm, Sweden
Conference Dates : July 06-07, 2023