ОРГАНІЗАЦІЯ ДОВІРЕННОГО СЕРЕДОВИЩА ВИКОНАННЯ З ВИКОРИСТАННЯМ QEMU ТА TRUST DOMAIN EXTENSIONS ВІД INTEL

Шулік П.В., Федюшин О.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Для ефективного захисту і обробки інформації у сучасних комп'ютерних системах використовується архітектура з розподілом на два світа: звичайний (non secure world) – де працює звичайне програмне забезпечення та захищений світ (secure world), в якому ведеться робота з конфіденційною інформацією. Для організації такого розподілу необхідна підтримка як з боку програмного так і з боку апаратного забезпечення. Як приклад програмної підтримки такого підходу можна привести опен соурс фреймфорк OP-TEE [1].

OP-TEE фреймфорк орієнтований на платформу ARM та технологію ARM TrustZone де периферія теж поділяється для роботи з захищеною та звичайною інформацією. Підтримка OP-TEE з боку Intel-x86 платформ є проблематичною, тому що Intel не має подібних рішень. Але Intel-x86 має розвинену апаратну підтримку віртуалізацій, де для secure world може використовуватися емулятор QEMU/KVM, на якому і виконується secure world.

Метою даного дослідження є розгляд одного із підходів інтеграції OP-TEE фреймворка з Intel-X86 платформами із використанням технологій віртуалізації. **Предметом дослідження** є програмні засоби інтеграції OP-TEE фреймворка с Intel-X86 з використанням QEMU/KVM [2].

Суть інтеграції OP-TEE складається в заміщенні технології TrustZone віртуальними машинами QEMU/KVM та технологією Intel Trust Domain Extensions (Intel TDX). Intel TDX вводить нові архітектурні елементи, які допоможуть розгорнути апаратно ізольовані віртуальні машини під назвою Trust Domains (TDs) на основі Intel® Total Memory Encryption - Multi-Key (Intel TME) і режим виконання процесора під назвою Secure-Arbitration Mode (SEAM). У цьому випадку основна операційна система і гіпервізор KVM (а також емулятор QEMU, де виконується робота з конфіденційною інформацією) ізолюються одна від одного.

Таким чином, практично технологія Intel TDX виконує дуже схожу функціональність з ARM TrustZone, може використовуватися сумісно з OP-TEE фрейворком.

Список літератури

1. GlobalPlatform, Inc.: TEE System Architecture Version 1.2 (Nov 2018), GPD SPE 009

2. Arshad Nehal, Priyanka Ahlawat Securing IoT applications with OP-TEE from hardware level OS: 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA) 10.1109/ICECA.2019.8822040