ВИКОРИСТАННЯ ВІРТУАЛЬНИХ МАШИН ДЛЯ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ НА ПЛАТФОРМАХ INTEL

Шулік П.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Вже понад більш ніж 10 років в операційних системах для захисту інформації існує підхід з використанням двох операційних систем, де система поділяється на два світи: звичайний (non secure world) – де працює звичайне програмне забезпечення, та захищений світ (secure world), в якому ведеться робота з секретною інформацією. Як приклад програмної підтримки такого підходу можна привести опен соурс фреймфорк OP-TEE [1]. Також для такого розподілу необхідна і апаратна підтримка, де периферія теж поділяється для роботи з захищеною та звичайною інформацією. Така підтримка існує з боку ARM систем і називається ARM TrustZone. В ARM TrustZone вводиться захищений режим роботи ARM ядра –у якому виконується робота з секретною інформацією, яка не повинна бути доступною для основної операційної системи та її додатків. Підтримка такого підходу з боку Intel-x86 платформ є проблематичною, тому що Intel не має подібних рішень. Але Intel-x86 має розвинену апаратну підтримку віртуалізацій, де для організації secure world може використовуватися окрема віртуальна машина.

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.

Суть інтеграції OP-TEE складається в заміщенні технології TrustZone віртуальними машинами та технологіями процесорів Intel-x86 VT-d/VT-x, де апаратні ресурси розподіляються між віртуальними операційними системами, і забезпечують ізоляцію ресурсів та інформації між операційними системами. У якості арбітра, який керує переключенням роботи процесора та доступу до ресурсів може виступати гіпервізор першого типу. У якості такого гіпервізора в запропонованому рішенні виступає гіпервізор компанії Intel Kernel Guard Technology (iKGT). Основний підхід закладений в iKGT називається Intel Supervisor Mode Execution Prevention (SMEP) - запобігання виконання коду в режимі супервізора. Технологія полягає в запобіганні виконання коду, розташованого на сторінці користувача (тобто звичайний світ, який не повинен мати доступу до захищеної інформації), при поточному рівні привілеїв рівному 0 (рівень доступу до захищеної інформації).

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

Список літератури

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