ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ INTEL ДЛЯ СТВОРЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ OPEN PORTABLE TRUSTED EXECUTION ENVIRONMENT (OP-TEE)

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

OP-TEE фреймворк являється поширеним в системах захисту інформації на базі ARM SoC та використовується в сучасних смартфонах, системах інтернету речей та інших хмарних системах [1]. OP-TEE базується на технології захисту інформації ARM TrustZone. Суть даної технології складається в тому, що вводиться додатковий режим роботи ARM ядра – захищений режим у якому виконується робота з секретною інформацією, яка не повинна бути доступною для основної операційної системи та її додатків. Таким чином система поділяється на два світа: звичайний (non secure world) – де працює звичайне програмне забезпечення та захищений світ (secure world), в якому ведеться робота з секретною інформацією.

Метою даного дослідження є розгляд одного із підходів інтеграції OP-TEE фреймворка с Intel-X86 платформами, які не підтримують технологію ARM Trust Zone. **Предметом дослідження** є програмні засоби інтеграції OP-TEE фреймворка с Intel-X86.

Суть інтеграції OP-TEE складається в заміщенні технології TrustZone віртуальними 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 орбітра, який керує переключенням роботи процесора та доступу до ресурсів може виступати гіпервайзор першого типу. У якості такого гіпервайзора в запропонованому рішенні виступає гіпервайзор 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 фрейворком.

Список літератури

1. 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