УДК 004.056.5 **DOI:10.30837/rt.2025.2.221.08**

П.В. ШУЛІК, канд. техн. наук, О.І. ФЕДЮШИН, канд. техн. наук,
Д.О. В'ЮХІН, О.Ю. МОРОЗОВ

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

Вступ

В сучасних 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 конфіденційною інформацією. Звичайний світ не має доступу до захищеного світу тоді як останній може з'єднуватись при бажанні з різними пристроями. Цей підхід стосується не тільки процесора, але і пам'яті, транзакції на шинах, переривань, периферійних пристроїв в рамках системи, в тому числі, програмного забезпечення.

Як приклад програмної підтримки такого підходу можна навести опен соурс фреймфорк OP-TEE (Open Portable Trusted Execution Environment) [1]. Типова архітектура програмного забезпечення OP-TEE показана на рис. 1.

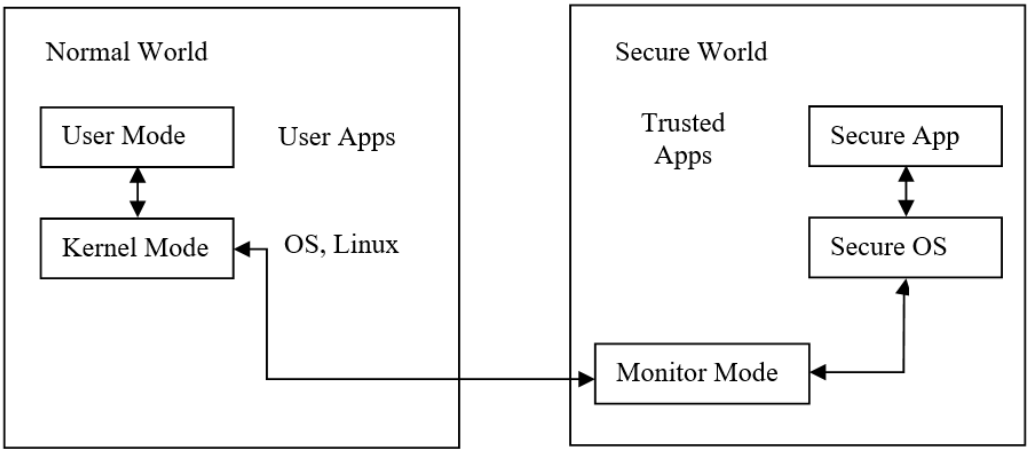

Рис. 1. Типова архітектура поділу світів OP-TEE

У звичайному світі працює основна операційна система, наприклад Linux або Android та звичайні додатки. Коли потрібно запустити якусь задачу, яка працює з конфіденційними даними, наприклад, аутентифікація, шифрування даних, банківські операції та інше, то йде запит від звичайного до сек'юрного світу. Для цього використовується API, який надається сек'юрним світом. Звернення до API виконується через Kernel module (або драйвер) та Monitor. Monitor розташований в сек'юрному світі та виступає арбітром, який обробляє запити від звичайного світу та повертає відповіді. В сек'юрному світі на рівні User space працюють додатки, які запускаються у відповідь на API запити.

Для підтримки різних світів необхідна апаратна підтримка, де периферія також поділяється на елементи для роботи з захищеною та звичайною інформацією – наприклад, розподіл оперативної пам'яті та флеш пам'яті. Така підтримка існує з боку ARM систем [2] і називається ARM TrustZone. В ARM TrustZone вводиться захищений режим роботи ARM ядра, в ньому виконується робота з секретною інформацією, яка не повинна бути доступною для основної операційної системи та її додатків. Спочатку OP-TEE була створена безпосередньо для підтримки ARM TrustZone для процесорів ARM Cortex A, де використовуються Unix-подібні операційні системи. Але OP-TEE поширюється дуже активно останні декілька років для роботи вбудованих та мобільних пристроїв і набрала популярності. Такий стан справ

викликає інтерес до використання OP-TEE з боку виробників серверних рішень, де системи в основному базуються на процесорах Intel-x86. Підтримка такого підходу з боку Intel-x86 платформ є проблематичною, тому що Intel не має подібних ARM TrustZone рішень. Але Intel-x86 має розвинену апаратну підтримку віртуалізацій, де для організації secure world може використовуватися окрема віртуальна машина.

Апаратна віртуалізація Intel-x86 – це технологія, що дозволяє запуск віртуальних машин в ізольованому режимі, де пам'ять, дисковий простір, периферія можуть бути розподілені та ізольовані між віртуальними машинами, тобто одна віртуальна машина не буде мати доступу до ресурсів іншої віртуальної машини.

Метою даного дослідження є створення системи захисту інформації на основі інтеграції OP-TEE фреймворка з Intel-X86 платформами з використанням технологій віртуалізації.

Предметом дослідження є програмні засоби інтеграції OP-TEE фреймворка з 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 [3, 4].

Інтеграції OP-TEE фреймворка з Intel-x86 платформами

У 2006 р. Intel представила VT-x – розширення для ефективної віртуалізації архітектури IA-32. Воно включає в себе набір інструкцій VMX і два нових режими роботи. Нові режими були названі root і non-root. Перший з них – для монітора віртуальних машин, другий – для гостьових оточень. За замовчуванням після включення живлення віртуалізація недоступна. Вхід в режим root відбувається після виконання нової інструкції VMXON, а наступні входи в non-root – за допомогою VMLAUNCH/VMRESUME.

Ключовий процес в будь-якій системі апаратної віртуалізації – це збереження поточного стану процесора гостя і завантаження стану монітора. Для зберігання станів як гостя, так і господаря використовується сутність під назвою VMCS (англ. Virtual Machine Control Structure). Ця структура повинна бути своя для кожного активного гостя. На рис. 2, що ілюструє переходи між режимами root і non-root, всередині VMCS використовуються дві області: стан гостя (guest-state) і стан господаря (host-state).

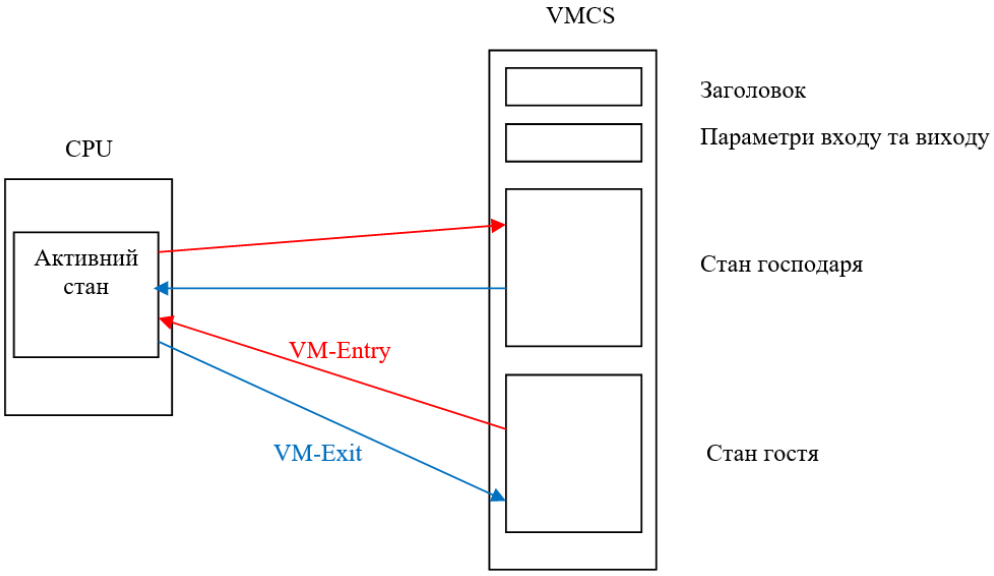

Рис. 2. VMCS та її стани

На рис. 2 подія VM-Entry – це одна з двох інструкцій: VMLAUNCH або VMRESUME, – а VM-Exit – одна з безлічі синхронних і асинхронних подій, оголошених привілейованими

в контексті VT-x non-root і тому вимагають перехоплення монітором. Деталі того, що і як завантажувати при переході з root в non-root і назад, також зберігаються в VMCS в елементах VM-entry і VM-exit controls(параметри входу і виходу). Області збереження розбиті на поля, кожне з яких зберігає в собі регістр або іншу архітектурну інформацію процесора.

У якості господаря (або арбітра), який керує перемиканням роботи процесора та доступу до ресурсів, може виступати гіпервізор першого типу або основна (хост) операційна система.

Таким чином архітектура Intel VT-x – це апаратно-програмне середовище, яке дуже схоже на ARM TrustZone з точки зору ізоляції програмного коду та ресурсів. Необхідно тільки вибрати архітектуру програмного забезпечення, тобто вирішити де буде розташований normal world та secure world.

Існує варіант інтеграції фреймворка OP-TEE на базі Intel VT-x та гіпервізора компанії Intel Kernel Guard Technology (iKGT).

iKGT – це легкий гіпервізор типу 1, з відкритим кодом Intel (https://github.com/intel/ikgt-core). Основний підхід закладений в iKGT [5] називається Intel Supervisor Mode Execution Prevention (SMEP) – запобігання виконання коду в режимі супервізора [6]. 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). Тобто до можливостей ізоляції Intel VT-x додається ще SMEP.

Використання гіпервізора потребує використання гостьової операційної системи – тобто віртуальної машини. Таким чином увесь код як звичайного, так і захищеного світу виконується всередині віртуальної машини (на рис. 3).

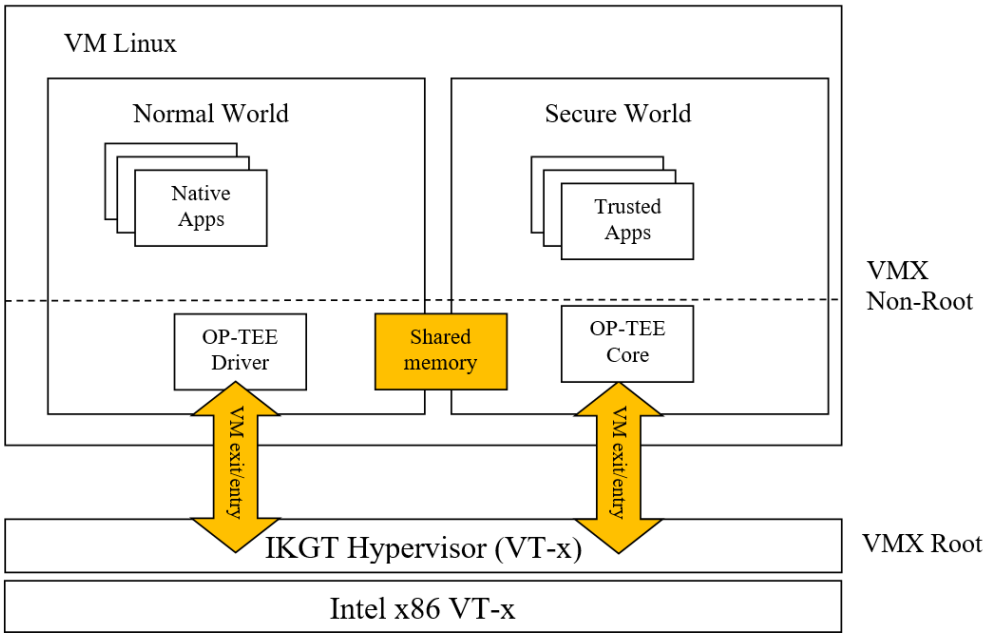

Рис. 3. Архітектура OP-TEE & IKGT

Ізоляція пам'яті досягається шляхом відповідного налаштування розширених таблиць сторінок, тому Linux не може отримати доступ до пам'яті OP-TEE. Тим не менш, є один блок спільної пам'яті, до якого може отримати доступ як Linux, так і OP-TEE для обміну параметрами та даними.

Перемикання між світами здійснюється командою «VMCALL», яка може бути викликана з Linux або з OP-TEE. Наступним кроком є виклик «VM exit» до гіпервізора iKGT, відповідального за детальне перемикання світу, таких як збереження або відновлення контексту VM, виконання «VM entry» в інший світ та інше.

В підході з використанням iKGT normal та secure world підтримують сумісність рівня API з архітектурою ARM TrustZone. Тільки драйвер Linux ядра ОС OP-TEE і OP-TEE залежать від архітектури.

Існуючий підхід має певну кількість недоліків: по-перше, normal world та secure world працюють в рамках однієї віртуальної машини, тобто в рамках однієї операційної системи. Використовуються тільки механізми перемикання між віртуальними машинами, але перемикання виконується тільки між сторінками пам’яті та використовується SMEP для обмеження доступу. Тобто, з точки зору безпеки, такий підхід дає більше можливостей для майбутніх хакерських атак. По-друге, цей підхід недостатньо модульний і потребує значних модифікацій при переході на інші платформи.

Архітектура з двома VM та використанням ACRN Hypervisor

Запропоноване в роботі рішення (див. рис. 4) базується на ізоляції secure world в окрему віртуальну машину. Апаратна підтримка теж базується на Intel x86 VT-x, але secure world існує повністю в окремій віртуальний машині. Таким чином ми маємо дві віртуальні машини – одна для normal world, де виконується основна операційна система, а друга віртуальна машина для OP-TEE. У якості гіпервізора використовуються гіпервізор ACRN [7]. ACRN – це гіпервізор першого типу з відкритим кодом, який був розроблений компанією Intel. ACRN гнучкий та легковісний, також використовується в різноманітних embedded системах, де важливі маленькі розміри гіпервізора та його гнучкість в адаптації до різноманітних систем та платформ.

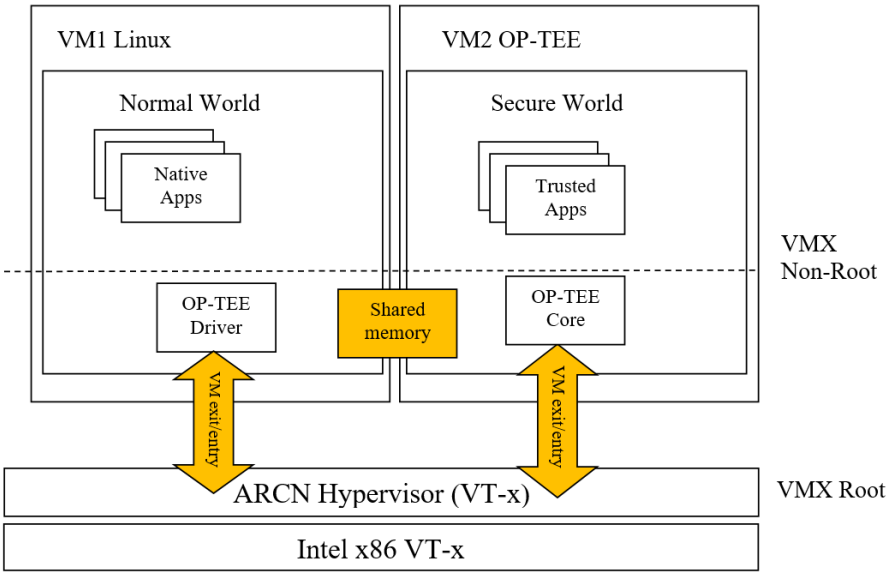

Рис. 4. Архітектура з двома VM та використанням ACRN Hypervisor

Як показано на рис. 4, ми маємо дві віртуальні машини, які працюють під керуванням ACRN гіпервізора. Перша VM1 – це звичайний світ – OS Linux, друга VM 2 – це OP-TEE.

ACRN створює ізольовану область пам'яті для TEE і шлях зв'язку для взаємодії двох віртуальних машин, але для повної підтримки поведінки ARM Trusted Firmware ACRN Hypervisor був модифікований для вирішення наступних проблем [8, 9]:

– необхідно забезпечити буфер shared memory. Тому ACRN гіпервізор був модифікований для створення такого буферу;

– організувати безпечну доставку та обробку переривань між звичайними та захищеними світами, безпечну доставку переривань та захист пам'яті на основі Intel VT-x. Ця підтримка також була додана на рівні ACRN гіпервізора.

Для підвищення безпеки як ACRN, так і OP-TEE образи були розміщені у зашифрованому регіоні жорсткого диску та ввімкнена підтримка Secure Boot.

Інтеграція як ACRN, так і OP-TEE була виконана з використанням наступних компонентів:

– Intel x86 VT-x: 9th Generation Intel® Core i7 Processors, 9850H;
– Normal World OS: Ubuntu LTS 24.04.1;
– OP-TEE 4.3.0.

Висновки

Запропонований варіант інтеграції OP-TEE на Intel x86 платформу з використанням двох віртуальних машин на базі ACRN гіпервізора.

Normal world та secure world працюють в окремих віртуальних машинах, вони повністю ізольовані на рівні операційних систем. З точки зору безпеки, така архітектура буде більш захищеною від хакерських атак в порівнянні з аналогічними рішеннями.

Побудована архітектура системи надає більше модульності та забезпечує легке перенесення на інші платформи та легке оновлення компонентів.

Список літератури:

1. GlobalPlatform, Inc.: TEE System Architecture Version 1.2 (Nov 2018), GPD SPE 009.
2. ARM Security Technology, Building a Secure System using TrustZone, ARM, Technology Copyright © 2005-2009 ARM Limited. All rights reserved. PRD29-GENC-009492C.
3. 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.
4. Kickstart Embedded. OP-TEE: What a Beginner Needs to Know. Sep. 13, 2022. [Online]. Available: https://kickstartembedded.com/2022/09/13/op-tee-part-1-what-a-beginner-needs-to-know/.
5. Intel. KGT Architecture. [Online]. Available:https://www.intel.com/content/www/us/en/developer/articles/technical/kgt-architecture.html.
6. Intel. Intel Supervisor Mode Execution Protection (SMEP) Datasheet. [Online]. Available: https://edc.intel.com/content/www/us/en/design/products/platforms/processor-and-core-i3-n-series-datasheet-volume-1-of-2/001/intel-supervisor-mode-execution-protection-smep/.
7. Intel. ACRN Hypervisor Documentation [Online]. Available: https://eci.intel.com/docs/3.0/components/acrn-hypervisor.html.
8. Шулік П. В., Федюшин О.І. Організація довіренного середовища виконання з використанням QEMU та TRUST DOMAIN EXTENSIONS від INTEL // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 15-ї міжнар. наук.-техн. конф., 24–25 квітня 2025р., м. Баку, м. Харків, м. Жиліна. Т. 3. Харків : Impress, 2025. С. 97. https://doi.org/10.32620/ICT.25.t3.
9. Шулік П. В. Використання віртуальних машин для організації захисту інформації на платформах INTEL // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 15-ї міжнар. наук.-техн. конф., 24–25 квітня 2025р., м. Баку, м. Харків, м. Жиліна. Т. 3. Харків : Impress, 2025. С. 98. https://doi.org/10.32620/ICT.25.t3.

Надійшла до редколегії 11.03.2025

Відомості про авторів:

Шулік Павло Вікторович – канд. техн. наук, Харківський національний університет радіоелектроніки, ст. викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: pavlo.shulik@nure.ua; ORCID: https://orcid.org/0009-0004-6200-2172

Федюшин Олександр Іванович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: oleksandr.fediushyn@nure.ua; ORCID: http://orcid.org/0000-0002-3600-405X

В'юхін Даніїл Олександрович – Харківський національний університет радіоелектроніки, ст. викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: daniil.viukhin@nure.ua; ORCID: https://orcid.org/0009-0009-8442-9587

Морозов Олексій Юрійович – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: oleksii.morozov@nure.ua; ORCID: https://orcid.org/0009-0005-6482-7810