УДК 004.056
Д. Мазурчак; В. Тимощук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ МЕХАНІЗМУ ІЗОЛЯЦІЇ ПАМ'ЯТІ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ВІРТУАЛІЗОВАНИХ МЕРЕЖЕВИХ СЕРЕДОВИЩАХ

UDC 004.056
D. Mazurchak; V. Tymoshchuk

INVESTIGATION OF MEMORY ISOLATION TECHNIQUES FOR IMPROVING THE SECURITY OF VIRTUALIZED NETWORK SYSTEMS

У міру зростання масштабів хмарних дата-центрів і щільності віртуалізації саме порушення ізоляції пам'яті між віртуальними машинами та мережевими компонентами стає джерелом внутрішніх загроз, що важко виявляються класичними засобами мережевого моніторингу. Еволюція механізмів Virtualized Network I/O (VNIO) від повної віртуалізації до паравіртуалізованих рішень на основі virtio-net, vhost-net та vhost-user дозволила суттєво підвищити пропускну здатність VNIO-шляху, однак це відбулася ціною послаблення ізоляції між компонентами. У моделях VM-to-vSwitch (VM2vS) та vSwitch-to-VM (vS2VM) процеси віртуального комутатора (vSwitch) або самі віртуальні машини (VM) отримують прямий доступ до чужої пам'яті через механізми спільних буферів та відображення сторінок, що створює умови для DMA-атак, побічних каналів і порушення ізоляції орендарів у багатокористувацьких хмарних середовищах. Традиційні підходи до підсилення безпеки, зокрема використання vIOMMU або перенесення обробки даних у kernel space не забезпечують прийнятного балансу між безпекою та продуктивністю й часто призводять до помітного падіння пропускної здатності VNIO.

У роботі запропоновано архітектурну модель vSwitch-to-Hypervisor (vS2H). Ключова ідея полягає в перенесенні критичних операцій обробки дескрипторів пакетів із користувацького процесу vSwitch безпосередньо в гіпервізор. У межах моделі vS2H vSwitch позбавляється прямого доступу до пам'яті VM, а гостьові VM не працюють зі спільними I/O-буферами vSwitch. Єдиним посередником між пам'яттю орендарів і I/O-пам'яттю мережевих компонентів виступає гіпервізор, який уже є привілейованим і контрольованим елементом віртуалізаційної платформи. Такий підхід зберігає сумісність з інтерфейсом virtio, істотно зменшує поверхню атаки, локалізує можливі компрометації в межах одного рівня та мінімізує ризики витоку даних через спільні області пам'яті.

Ефективність моделі vS2H було експериментально оцінено на стенді на базі QEMU/KVM [1], Open vSwitch із підтримкою DPDK та генератора трафіку TRex. Результати вимірювань показали, що для каналу передачі даних запропонований механізм забезпечує середній приріст пропускної здатності близько 11% порівняно з класичним vhost-user. У сценаріях із розгортанням високопродуктивних DPDK-застосунків усередині VM спостерігається покращення стабільності обробки трафіку завдяки зменшенню конкуренції за CPU-ресурси між vSwitch та гостьовими VM. Отримані результати свідчать, що архітектура vS2H є перспективним напрямом розвитку безпечних VNIO-механізмів.

Література

1. Interactive cybersecurity training system based on simulation environments / D. Tymoshchuk et al. Measuring and computing devices in technological processes. 2024. No. 4. P. 215–220. URL: https://doi.org/10.31891/2219-9365-2024-80-26 (date of access: 30.11.2025).