УДК 004.056.5 URL: https://ptsj.bmstu.ru/catalog/icec/insec/1030.html

HYPERWALLET: КРИПТОВАЛЮТНЫЙ КОШЕЛЕК КАК БЕЗОПАСНОЕ ПРИЛОЖЕНИЕ НА БАЗЕ ГИПЕРВИЗОРА

Д.А. Вахромеев vakhromeevda@student.bmstu.ru
Е.В. Глинская glinskaya@bmstu.ru
SPIN-код: 5430-3023

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Рассмотрена платформа VirtSecIO, организованная на основе гипервизора и предназначенная для повышения безопасности криптовалютных кошельков. Используя технологии виртуализации, платформа VirtSecIO минимизирует поверхность атаки и предоставляет безопасную среду для цифровых транзакций. В исследовании обсуждаются архитектура, производительность, ограничения и направления будущей работы, необходимой для расширения возможностей платформы. Исследование охватывает архитектуру VirtSecIO, включая уровень гипервизора, безопасный путь выполнения и модуль доверенной платформы (TPM). Практическое применение платформы демонстрируется на примере кошелька HyperWallet. Рассмотрены производительность, ограничения и направления будущих исследований, такие как поддержка USB и расширение функциональности для других безопасных приложений.

Ключевые слова: защищенный криптовалютный кошелек, гипервизор, защищенная связь, защита от атак, виртуализация, безопасность транзакций, изолированная среда, аппаратная безопасность

Введение. Криптовалютные кошельки критически важны для управления цифровыми активами, однако они часто становятся мишенью для злоумышленников. Увеличение сложности киберугроз требует надежных мер безопасности для защиты личных ключей пользователей и данных транзакций. Платформа VirtSecIO позволяет решить эту задачу, используя гипервизор для создания изолированных сред выполнения для операций с кошельками, тем самым повышая безопасность без необходимости применения специализированного оборудования [1].

Архитектура VirtSecIO. Платформа VirtSecIO создает безопасную виртуальную среду, которая изолирует операции с кошельками от хост-системы. Эта архитектура разработана для снижения риска атак, использующих уязвимости в операционной системе или приложениях. К ключевым компонентам платформы относятся следующие [2].

1. Уровень гипервизора. Ядро VirtSecIO управляет виртуальными машинами и обеспечивает изоляцию между безопасными модулями и операцион-

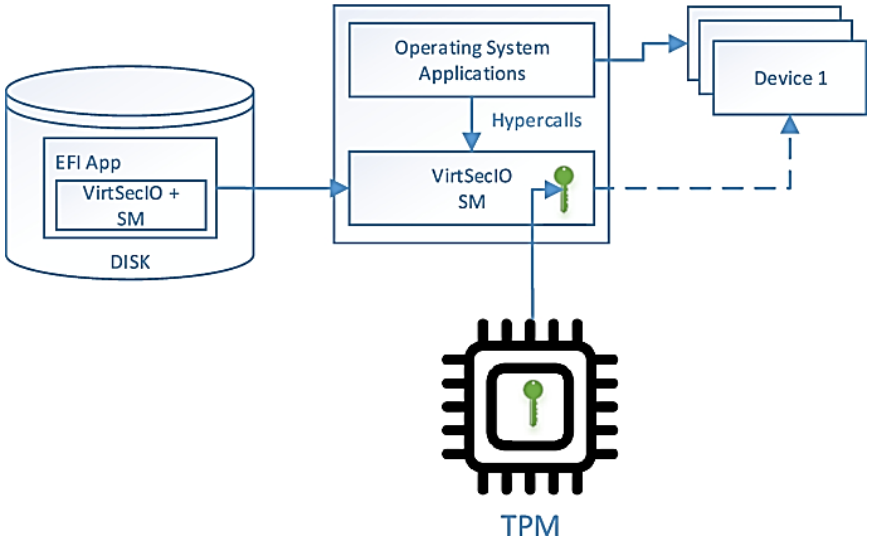
 ISSN 2541-8009

ной системой хоста. Этот уровень работает с минимальными накладными расходами, что позволяет эффективно выполнять безопасные приложения.

2. Безопасный путь выполнения. Платформа VirtSecIO предоставляет контролируемую среду для выполнения транзакций с кошельками, обеспечивая, чтобы важные операции проводились вдали от потенциальных угроз, исходящих от хост-системы или вредоносного программного обеспечения.

3. Минимальная поверхность атаки. Включив только необходимые драйверы устройств и функциональности, платформа VirtSecIO ограничивает потенциальные точки входа для злоумышленников, что затрудняет использование уязвимостей.

4. Модуль доверенной платформы (TPM). Безопасный криптовалютный кошелек HyperWallet, разработанный с использованием платформы VirtSecIO, хранит личный ключ пользователя в модуле TPM (см. рисунок). Эта функция аппаратной безопасности усиливает защиту чувствительной информации.



Модуль доверенной платформы (TPM):

Operating System Applications — приложения операционной системы; Hypercalls — гипервызовы; VirtSecIO SM — модуль безопасности VirtSecIO; Device 1 — устройство 1; EFI App — приложение UEFI; VirtSecIO + SM — VirtSecIO с модулем безопасности; DISK — диск; TPM — модуль доверенной платформы

HyperWallet: Кейс-исследование. Инструмент HyperWallet служит практическим приложением платформы VirtSecIO, демонстрируя ее возможности в реальном сценарии. Он функционирует как аппаратный кошелек для циф-

ровой валюты, позволяя пользователям безопасно подписывать транзакции, не раскрывая свои личные ключи [3]. Интеграция стороннего приложения, такого как Metamask, облегчает генерацию и передачу транзакций в сеть цифровой валюты, действуя как посредник, который минимизирует поверхность атаки на HyperWallet.

Оценка производительности. Производительность VirtSecIO оценивали с точки зрения скорости транзакций и использования ресурсов. По результатам оценки можно сделать следующие выводы:

– скорость транзакций в основном зависит от внешних факторов, таких как задержка сети и время, необходимое для сканирования QR-кодов. Внутренняя скорость обработки HyperWallet эффективна, при этом уровень гипервизора обеспечивает минимальные задержки [4];

– скорость работы центрального процессора и скорость ввода-вывода не оказались значительными ограничивающими факторами для HyperWallet, следовательно, платформа может эффективно обрабатывать большие объемы транзакций без ущерба для безопасности [5].

Ограничения и планы на будущее. Хотя платформа VirtSecIO показывает многообещающие результаты, в настоящее время она не поддерживает протокол USB, что ограничивает его использование на стандартных настольных системах [6]. Это ограничение сдерживает возможность подключения различных аппаратных кошельков и периферийных устройств, которые могли бы улучшить пользовательский опыт [7]. Будущая работа будет сосредоточена на следующих действиях:

– изучении поддержки протокола USB (исследовании целесообразности интеграции поддержки USB для обеспечения более широкой совместимости устройств и повышения их функциональности [8]);

– улучшении возможностей (расширение возможностей платформы для учета более широкого спектра безопасных приложений, помимо криптовалютных кошельков, потенциально включая безопасные сообщения и решения для хранения данных);

– оценках безопасности (проведение дальнейших оценок безопасности для выявления и устранения потенциальных уязвимостей в архитектуре VirtSecIO [9]).

Заключение. Платформа VirtSecIO представляет собой значительное достижение в области безопасности криптовалютных кошельков. Используя технологии виртуализации, она предоставляет надежное решение для снижения рисков, связанных с управлением цифровыми активами. Разработка инструмента HyperWallet как безопасного приложения демонстрирует практическое применение VirtSecIO для повышения безопасности пользователей

 ISSN 2541-8009

[10]. Продолжение исследований и разработок будет иметь решающее значение для устранения текущих ограничений и расширения областей применения платформы VirtSecIO.

Литература

[1] Bertoni G. et al. Keccak. *Advances in Cryptology – EUROCRYPT 2013*, Springer, 2013. https://doi.org/10.1007/978-3-642-38348-9_19

[2] Johnson D. et al. The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, 2001, pp. 36–63. https://doi.org/10.1007/s102070100002

[3] Nofer M. et al. Blockchain. *Business & Information Systems Engineering*, 2017, vol. 59 (3). https://doi.org/10.1007/s12599-017-0467-3

[4] Nakamoto S. *Bitcoin: A peer-to-peer electronic cash system*. URL: https://bitcoin.org/bitcoin.pdf (accessed October 15, 2024).

[5] Wood G. et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap*., 2014. URL: https://ethereum.github.io/yellowpaper/paper.pdf (accessed October 15, 2024).

[6] Corduan J. et al. *A formal specification of the Cardano ledger*. URL: https://allquantor.at/blockchainbib/pdf/corduan2019formal.pdf (accessed October 15, 2024).

[7] Catalini C., Gans J.S. *Some simple economics of the blockchain*. URL: https://dl.acm.org/doi/10.1145/3361234 (accessed October 15, 2024).

[8] Praitheeshan P. et al. *Security analysis methods on ethereum smart contract vulnerabilities: a survey*. URL: https://arxiv.org/abs/1908.08605 (accessed October 15, 2024).

[9] Lee W.M. *Using the MetaMask Chrome Extension*. Beginning Ethereum Smart Contracts Programming, Apress, 2019. https://doi.org/10.1007/978-1-4842-5086-0_5

[10] Kiperberg M. Preventing malicious communication using virtualization. *J. Inf. Secur. Appl.*, 2021, vol. 61. https://doi.org/10.1016/j.jisa.2021.102871

Поступила в редакцию 24.10.2024

Вахромеев Даниил Александрович — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Глинская Елена Вячеславовна — старший преподаватель кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Научный руководитель — Басараб Михаил Алексеевич, д-р физ.-мат. наук, заведующий кафедрой «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Вахромеев Д.А., Глинская Е.В. Hyperwallet: криптовалютный кошелек как безопасное приложение на базе гипервизора. *Политехнический молодежный журнал*, 2025, № 02 (97). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1030.html

 ISSN 2541-8009

HYPERWALLET: CRYPTOCURRENCY WALLET AS A SECURE HYPERVISOR-BASED APPLICATION

D.A. Vakhromeev vakhromeevda@student.bmstu.r
E.V. Glinskaya glinskaya@bmstu.ru
SPIN-code: 5430-3023

Bauman Moscow State Technical University, Moscow, Russian Federation

The paper considers the VirtSecIO platform. It was organized based on a hypervisor and designed to improve security of the cryptocurrency wallets. The VirtSecIO platform uses virtualization technologies to minimize the attack surface and provides a secure environment for the digital transactions. The paper discusses architecture, performance, limitations, and future areas in expanding the platform capabilities. The study covers the VirtSecIO architecture and includes the hypervisor layer, secure execution path, and the trusted platform module (TPM). Practical application of the platform is demonstrated using the HyperWallet wallet as an example. The paper analyzes performance, limitations, and future areas for further research, such as the USB support and expanding functionalities for the other secure applications.

Keywords: secure cryptocurrency wallet, hypervisor, secure communication, attack protection, virtualization, transaction security, sandbox, hardware security

Received 24.10.2024

Vakhromeev D.A. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Glinskaya E.V. — Senior Lecturer, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Basarab M.A., Dr. Sci. (Phys.-Math.), Head of the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Vakhromeev D.A., Glinskaya E.V. Hyperwallet: cryptocurrency wallet as a secure hypervisor-based application. *Politekhnicheskiy molodezhnyy zhurnal*, 2025, no. 02 (97). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1030.html

