Аппаратные основы адаптивной безопасности: технологии изоляции и их интеграция в современные системы защиты

С. И. Земков[1], Н. А. Гревцев[2], П. А. Чибисов[3]

[1]НИЦ «Курчатовский институт» - НИИСИ, Москва, Россия, zemkov@cs.niisi.ras.ru;

[2]НИЦ «Курчатовский институт» - НИИСИ, Москва, Россия, ngrevcev@cs.niisi.ras.ru;

[3]НИЦ «Курчатовский институт» - НИИСИ, Москва, Россия, chibisov@cs.niisi.ras.ru

Аннотация. Статья исследует аппаратные основы адаптивной безопасности — подхода к созданию систем, архитектурно устойчивых к атакам. Рассматриваются ключевые технологии изоляции (TEE, SEV, TPM) и их интеграция в адаптивные системы безопасности. Делается вывод о необходимости комплексного подхода, сочетающего аппаратные гарантии с динамическим программным анализом и оркестрацией.

Ключевые слова: адаптивная безопасность, аппаратная изоляция, доверенные среды выполнения

1. Введение

Экспоненциальный рост сложности и масштаба киберугроз заставляет постоянно пересматривать устоявшиеся подходы к защите информации. Классические методы кибербезопасности, основанные на статичных периметрах и сигнатурном анализе, оказываются недостаточно эффективными для отражения современных целевых атак. В качестве ответа сформировалась адаптивная модель безопасности, основанная на принципе «предполагай нарушение». Её суть — не только в прогнозировании и предотвращении угроз, но и в постоянной готовности к инциденту: она обеспечивает непрерывный мониторинг, анализ поведения и контекстно-зависимое автоматизированное реагирование для сдерживания атаки и минимизации ущерба даже внутри условно скомпрометированной среды.

В то же время развивается иной, архитектурно-ориентированный вектор, который ставит во главу угла не реагирование на нарушение, а его принципиальную невозможность за счёт проектирования систем, устойчивых к компрометации. Этот подход, известный как кибериммунитет, часто опирается на принципы изоляции компонентов (схожие с архитектурой MILS — Multiple Independent Levels of Security and Safety [1]), минимальных привилегий и верифицируемой безопасности. Таким образом, если адаптивная безопасность делает систему устойчивой к последствиям взлома, то кибериммунитет стремится сделать её архитектурно невзламываемой.

В основе таких систем лежат аппаратные механизмы доверия и изоляции, однако защита от киберугроз может дополняться программными средствами, реализующими принципы изоляции и минимизации доверенной вычислительной базы, например, кибериммунной операционной системой KasperskyOS и изолированными средами выполнения AWS Nitro Enclaves. В статье проводится обзор технологий Trusted Execution Environments (TEE), шифрования памяти AMD SEV и систем измерения целостности на базе TPM. Анализируется их роль в создании доверенных сред выполнения и обеспечении достоверной телеметрии, критически важной для оркестрации механизмов безопасности.

2. Основные аппаратные технологии изоляции применимые для адаптивной безопасности

Для построения систем по принципам адаптивной безопасности требуется использование аппаратных технологий изоляции — механизмов создания защищенных сред выполнения. В главе рассматриваются три ключевых подхода: TEE, архитектура Haven и шифрование памяти AMD.

2.1 Trusted Execution Environment

Trusted Execution Environment — это аппаратно изолированная зона в процессоре, обеспечивающая конфиденциальность и целостность кода и данных даже при компрометации ОС. TEE использует изоляцию

(например, Intel SGX) и криптографическую удаленную аттестацию для проверки своей корректности [2].

В работе [3] рассматривается многообразие подходов к реализации TEE в архитектуре RISC-V, от программных решений (например, Keystone), использующих стандартные механизмы защиты, до архитектур, требующих глубоких аппаратных модификаций (Sanctum, HECTOR-V). Это разнообразие объясняется стремлением к компромиссу между силой изоляции, производительностью и масштабируемостью. Легковесные проекты могут быть уязвимы к сложным микроархитектурным атакам таким как Spectre [4], тогда как более защищенные системы теряют в универсальности и производительности из-за требований к нестандартному оборудованию.

2.2 Архитектура Haven

Архитектура Haven [5] расширяет TEE, помещая в анклав SGX не только приложение, но и минимальную ОС (LibOS). Это позволяет запускать legacy-приложения без изменений, полностью изолируя их от скомпрометированной основной ОС.

Для адаптивных систем Haven демонстрирует важный принцип: создание доверенных контейнеров для сложных рабочих нагрузок. Однако, высокое потребление аппаратных ресурсов и зависимость от микроархитектуры ограничивают прямое применение этой технологии, так что она ценна только в качестве исследовательской модели.

2.3 Шифрование памяти AMD

В основе технологии AMD SME/SEV, представленной группой исследователей из AMD [6], лежит шифрование данных в оперативной памяти на уровне процессора. SEV предоставляет каждой виртуальной машине уникальный ключ шифрования, который генерируется и хранится внутри защищённого аппаратного модуля процессора и недоступен гипервизору. Данные виртуальной машины автоматически шифруются и расшифровываются контроллером памяти при обращении к ОЗУ, что обеспечивает конфиденциальность даже при компрометации гипервизора. При этом базовая версия SEV не обеспечивает защиту целостности данных, которая реализуется в расширениях SEV-ES и SEV-SNP.

В контексте адаптивной безопасности этот подход создает дополнительный барьер, повышая стоимость атак на конфиденциальность. Однако данная технология защиты пассивна и уязвима к атакам на архитектурном уровне, поэтому может быть использована как часть более широкой системы мониторинга и ответа.

3. Архитектурные подходы к адаптивной безопасности

В главе рассматриваются подходы к построению адаптивных систем безопасности на архитектурном уровне. Анализируется роль аппаратных механизмов (таких как TPM) в обеспечении доверенной телеметрии для непрерывного контроля целостности, а также обсуждаются принципиальные ограничения изолированных сред, требующих дополнительных методов поведенческого анализа для обнаружения скрытых угроз.

3.1 Адаптивные системы измерения целостности

Адаптивные системы целостности на основе TCG, предложенные Sailer et al. [7], используют аппаратный модуль TPM для создания криптографически верифицируемой цепочки измерений всех критических компонентов системы с момента ее загрузки. Это обеспечивает удаленную аттестацию и проверку соответствия эталону.

В контексте адаптивной безопасности эти непрерывные измерения становятся ключевым источником доверенной телеметрии. Система анализирует их в реальном времени, обнаруживая несанкционированные изменения и автономно запуская ответные действия, такие как изоляция узла.

3.2 Проблемы безопасности анклавов

Исследование Schwarz et al. [8] показало, что защищенные анклавы (например, Intel SGX) могут быть использованы для создания скрытного вредоносного ПО. Такое ПО становится невидимым для традиционных средств защиты, использующих анализ памяти или сигнатуры. Это доказывает, что аппаратная изоляция не самодостаточна. Для противодействия необходимо внешнее наблюдение: адаптивные системы, анализирующие аномалии в поведении (сеть, вызовы API), могут обнаружить злоупотребление доверенной средой.

4. Интеграция аппаратной изоляции в адаптивные системы безопасности

4.1 Принципы интеграции аппаратной изоляции

Анализ рассмотренных работ позволяет выделить ключевые принципы интеграции аппаратных механизмов изоляции в адаптивные

системы безопасности:

• Многоуровневая изоляция: комбинирование различных технологий (SGX, SEV, TPM) для создания защитных барьеров на разных уровнях системы.

• Динамическая аттестация: непрерывная верификация целостности изолированных компонентов.

• Адаптивное управление доступом: автоматическое изменение прав доступа на основе оценки рисков в реальном времени.

• Оркестрация безопасности: координация работы различных механизмов защиты через единую систему управления.

4.2 Развитие адаптивной безопасности как кибериммунитета

Кибериммунитет — это архитектурная парадигма, проектирующая системы, изначально устойчивые к атакам. Признавая невозможность абсолютной защиты, подход фокусирует усилия на критических компонентах, компрометация которых недопустима. Это становится возможным благодаря использованию встроенных механизмов строгого разделения и контролируемого взаимодействия всех подсистем.

Искусственные иммунные системы (AIS) применяют биологический принцип распознавания «свой/чужой» (self/nonself) для обнаружения аномалий в IT-средах. Как отмечено в обзоре [9], архитектура таких систем основывается на кодировании данных (антигенов/антител), алгоритмах генерации детекторов (например, негативной селекции) и эволюционном механизме для адаптации к новым угрозам. Последующие исследования [10] развивают эту тему, предлагая конкретные архитектурные решения для IDS, вдохновленные иммунной системой, включая использование не только теории «свой/чужой», но и теории опасности (Danger Theory).

В работе [11] показано, как принципы кибериммунитета реализуются в микросервисных архитектурах. Их естественная изоляция компонентов сама по себе увеличивает безопасность ситемы, однако для повышения устойчивости к киберугрозам необходимы централизованные защищенные механизмы. Такие механизмы должны контролировать все взаимодействия между сервисами, предотвращая распространение атаки при компрометации одного из них.

5. Заключение

Проведенный анализ позволяет сделать вывод о том, что эффективная адаптивная безопасность не может быть достигнута исключительно за счет программных решений и надстроек над существующей инфраструктурой. Современный уровень угроз требует пересмотра маршрута построения вычислительных систем. Ключевым направлением становится проектирование безопасности на аппаратном уровне, начиная с этапа разработки микросхем и процессоров.

Необходимо закладывать в архитектуру аппаратных компонентов специализированные механизмы изоляции, доверия и измерения целостности, такие как защищенные среды выполнения, криптографическое шифрование памяти на уровне процессора и аппаратные модули доверия. Внедрение этих механизмов позволяет создать доверенную и верифицируемую платформу, которая будет способна предотвращать проникновение и противостоять угрозам в уже скомпрометированной системе. Такой подход позволяет гарантировать доверенность критически важных компонентов адаптивной безопасности — агентов мониторинга, систем анализа и механизмов автоматизированного реагирования. Это требует тесного сотрудничества между разработчиками микропроцессорной техники, производителями аппаратных платформ и архитекторами систем программной безопасности.

Публикация выполнена в рамках государственного задания НИЦ «Курчатовский институт» - НИИСИ по теме № FNEF-2024-0003.

Hardware foundations of adaptive security: isolation technologies and their integration into modern protection systems

S. I. Zemkov, N. A. Grevtsev, P. A. Chibisov

Abstract. The article explores the hardware foundations of adaptive security—an approach to creating systems that are architecturally resilient to attacks. It examines key isolation technologies (TEE, SEV, TPM) and their integration into adaptive security systems. The conclusion emphasizes the necessity of a comprehensive approach that combines hardware guarantees with dynamic software analysis and orchestration.

Keywords: adaptive security, hardware isolation, trusted execution environments

Литература

1. Alves-Foss J. et al. The MILS architecture for high-assurance embedded systems // International journal of embedded systems. – 2006. – Vol. 2. – No. 3-4. – P. 239-247.
2. Hoekstra M., Lal R., Pappachan P., Phegade V., Del Cuvillo J. Using innovative instructions to create trustworthy software solutions // Proc. of the Network and Distributed System Security Symposium (NDSS 2013). 2013.
3. Boubakri, M.; Zouari, B. A Survey of RISC-V Secure Enclaves and Trusted Execution Environments. Electronics 2025, 14, 4171.
4. P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg,M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, “Spectre attacks: Exploiting speculative execution,” Communications of the ACM, vol. 63, pp. 93–101, 2020.
5. Baumann A., Peinado M., Hunt G. Shielding applications from an untrusted cloud with Haven // ACM Transactions on Computer Systems (TOCS). 2015. Vol. 33. No. 3. Pp. 1–26.
6. Kaplan D., Powell J., Woller T. AMD Memory Encryption. White paper, 2016.
7. Sailer R., Zhang X., Jaeger T., Van Doorn L. Design and implementation of a TCG-based integrity measurement architecture // Proc. of the 13th USENIX Security Symposium. 2004. Pp. 223–238.
8. Schwarz M., Li S., Weiser S., Gruss D. Practical enclave malware with Intel SGx. arXiv preprint arXiv:2002.05649, 2020.
9. Smith J., Johnson M. A survey of artificial immune system based intrusion detection // Journal of Network and Computer Applications. 2015. Vol. 52. Pp. 1–20.
10. Wilson P., Taylor S. Artificial immune systems in local and network cybersecurity: An overview of intrusion detection strategies // Proc. of the International Conference on Cybersecurity. 2021. Pp. 45–62.
11. Соболев С. П. Кибериммунный подход к разработке. Иллюстрация применения на базе микросервисной архитектуры // Вестник СПбГУ. Серия 10. Прикладная математика. Информатика. Процессы управления. 2024. № 1.