Романов Д.Р. Манипуляция данными в DRAM: как ROWHAMMER-атаки могут использоваться вирусами // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 3(53) с. 63–66

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

МАНИПУЛЯЦИЯ ДАННЫМИ В DRAM: КАК ROWHAMMER-АТАКИ МОГУТ ИСПОЛЬЗОВАТЬСЯ ВИРУСАМИ

Романов Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilio2003.dr@gmail.com

Rowhammer-атака — это серьёзная уязвимость в современных модулях DRAM, позволяющая изменять содержимое памяти без прямого доступа к ней. Эта атака использует быстрые повторяющиеся обращения к определённым строкам памяти, что вызывает сбои в соседних ячейках, приводя к несанкционированному изменению данных. Вирусы и вредоносное ПО могут эксплуатировать этот механизм для повышения привилегий, обхода защитных механизмов и нарушения работы системы. В статье рассматриваются принципы работы Rowhammer-атак, реальные примеры их использования и методы защиты, такие как коррекция ошибок, аппаратные и программные контрмеры.

Ключевые слова: Rowhammer, DRAM, манипуляция данными, битовые сбои, кибератаки, повышение привилегий, защита памяти.

DATA MANIPULATION IN DRAM: HOW ROWHAMMER ATTACKS CAN BE USED BY VIRUSES

Romanov D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilio2003.dr@gmail.com

The Rowhammer attack is a serious vulnerability in modern DRAM modules that allows changing the contents of memory without direct access to it. This attack uses fast repetitive accesses to certain memory lines, which causes failures in neighboring cells, leading to unauthorized data modification. Viruses and malware can exploit this mechanism to elevate privileges, bypass security mechanisms, and disrupt the system. The article discusses the principles of Rowhammer attacks, real-world examples of their use, and protection methods such as error correction, hardware and software countermeasures.

Keywords: Rowhammer, DRAM, data manipulation, bit failures, cyber attacks, privilege escalation, memory protection.

Введение

С развитием технологий безопасности операционных систем и процессоров злоумышленникам становится всё сложнее находить уязвимости для выполнения атак. Однако аппаратные уязвимости, такие как Rowhammer, представляют особую опасность, поскольку они воздействуют на саму структуру памяти, выходя за рамки традиционных методов защиты. Rowhammer-атака была впервые обнаружена исследователями в 2014 году и до сих пор остаётся актуальной угрозой для современных компьютеров, серверов и мобильных устройств.

Суть уязвимости заключается в том, что частый доступ к одной и той же строке памяти может привести к изменению данных в соседних строках из-за электромагнитных помех. Это явление, известное как "битовые сбои" (bit flips), можно использовать для изменения привилегий пользователя, обхода механизмов защиты и выполнения вредоносного кода. Более того, Rowhammer является уникальным типом атаки, который не требует традиционного программного эксплойта или уязвимости в операционной системе, а использует фундаментальные физические свойства компьютерной памяти.

Исследования показали, что Rowhammer может быть использована в реальных атаках. Например, злоумышленники могут эксплуатировать этот механизм для повышения прав доступа в системе, выполняя вредоносный код с привилегиями администратора. Вирусы, использующие Rowhammer, могут обходить песочницы и другие методы изоляции процессов, что делает их особенно опасными в многопользовательских средах и виртуальных машинах. Несмотря на предпринимаемые меры защиты, Rowhammer остаётся активной угрозой, требующей комплексного подхода к её нейтрализации.

Манипуляция данными в DRAM: как Rowhammer-атаки могут использоваться вирусами

Rowhammer-атака основана на особенностях работы современных чипов DRAM. В отличие от процессорной памяти (кэша), DRAM-хранилище использует конденсаторы для хранения битов информации. Эти конденсаторы расположены в ячейках памяти, сгруппированных в строки, которые хранят данные. Однако по мере увеличения плотности размещения транзисторов в современных чипах DRAM их чувствительность к электромагнитным помехам возросла. Это привело к тому, что частые обращения к определённой строке могут повлиять на данные в соседних строках, вызывая случайные изменения битов[1].

Для успешного выполнения Rowhammer-атаки злоумышленники используют специальный программный код, который быстро и многократно активирует определённые строки памяти, добиваясь появления битовых сбоев в соседних ячейках. Вредоносное ПО, использующее этот метод, может изменять критически важные данные, например, таблицы доступа пользователей или ключи аутентификации, что позволяет обходить стандартные механизмы безопасности[2].

В 2015 году исследователи Google показали, что Rowhammer можно использовать для получения root-доступа в операционной системе Linux. Они создали Proof-of-Concept эксплойт, который позволял обычному пользователю с низкими привилегиями изменять критически важные области памяти ядра, что приводило к захвату системы. В дальнейшем появилось множество вариаций атак, в том числе атаки через JavaScript, которые позволяли злоумышленникам использовать Rowhammer даже в браузере без необходимости локального доступа к устройству[3].

Опасность Rowhammer-атак заключается в том, что они могут применяться в различных сценариях. Например, вредоносные программы могут использовать эту уязвимость для выхода из песочницы, что представляет угрозу для виртуальных сред, браузеров и мобильных приложений. В случае с облачными сервисами Rowhammer-атака может быть использована для выхода за пределы виртуальной машины и компрометации других клиентов, работающих на той же аппаратной платформе[4].

Для защиты от Rowhammer-атак разработчики аппаратного и программного обеспечения внедряют различные методы защиты. Один из наиболее эффективных способов — использование механизмов коррекции ошибок (ECC, Error-Correcting Code), которые позволяют обнаруживать и исправлять случайные изменения битов в памяти. Однако не все системы поддерживают ECC, а его реализация увеличивает стоимость оборудования.

Другим способом защиты является программное ограничение доступа к памяти с высокой частотой. Например, современные версии операционных систем включают специальные алгоритмы, которые обнаруживают аномально частые обращения к памяти и блокируют потенциально вредоносные процессы. Также исследуются аппаратные решения, такие как увеличение физического расстояния между строками памяти или использование новых материалов, менее подверженных помехам[5].

Несмотря на эти меры, Rowhammer остаётся актуальной угрозой, поскольку новые исследования показывают способы обхода существующих механизмов защиты. Например, некоторые атаки позволяют обойти ECC-коррекцию за счёт одновременного изменения нескольких битов, а программные контрмеры могут быть нейтрализованы вредоносным кодом, имитирующим легитимные процессы.

С развитием технологий искусственного интеллекта и машинного обучения Rowhammer может стать ещё более опасной. Автоматизированные системы анализа уязвимостей способны находить оптимальные способы эксплуатации битовых сбоев, делая атаки более эффективными и труднообнаруживаемыми. Это создаёт дополнительные вызовы для специалистов по кибербезопасности, требуя постоянного совершенствования методов защиты.

Заключение

Rowhammer-атаки представляют собой уникальную угрозу в сфере информационной безопасности, так как они воздействуют непосредственно на аппаратное обеспечение, обходя традиционные программные механизмы защиты. Их особенность заключается в том, что они используют физические свойства компьютерной памяти, что делает их особенно сложными для обнаружения и предотвращения.

Несмотря на то, что исследователи предлагают различные методы защиты, включая коррекцию ошибок, программные контрмеры и аппаратные решения, Rowhammer остаётся активной угрозой, которая продолжает развиваться. Злоумышленники находят новые способы обхода защитных механизмов, а развитие облачных технологий и виртуализации делает возможным использование Rowhammer-атак в масштабных сценариях.

Для эффективной защиты систем необходимо использовать комплексный подход: внедрение ECC, постоянное обновление программного обеспечения, мониторинг активности памяти и повышение осведомлённости пользователей о рисках. Только комбинированные меры могут снизить вероятность успешной атаки и защитить критически важные данные от манипуляции с помощью Rowhammer.

Список литературы

1. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.

2. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.
3. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
4. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
5. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.

References

1. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch-Bruevich, 1996.
2. Chmutov M. V. et al. A study of the current IT infrastructure of an organization for the subsequent transition to a cloud architecture //Information security of the regions of Russia (IBRD-2017). Conference proceedings, 2017, pp. 535-537.
3. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High–tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. - pp. 70-76.
4. Lesnova E. M., Pestov I. E. Method development error detection and correction for a distributed information network based on big data //Regional Informatics and information Security. - 2018. – pp. 236-240.
5. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelec communications in science and education (APINO 2023). – 2023. – pp. 345-348