Бютнер С.И. Эксплуатация уязвимостей в алгоритмах энергосбережения процессоров для атак // Международный журнал информационных технологий и энергоэффективности.– 2025. – Т. 10 № 3(53) с. 154–157

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.5

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ В АЛГОРИТМАХ ЭНЕРГОСБЕРЕЖЕНИЯ ПРОЦЕССОРОВ ДЛЯ АТАК

Бютнер С.И.
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: serafimkavasaki@gmail.com

С развитием процессоров и переходом к многоядерным системам, алгоритмы энергосбережения становятся важной частью их архитектуры. Эти алгоритмы направлены на оптимизацию потребления энергии в зависимости от нагрузки, однако в последние годы было выявлено несколько уязвимостей, которые могут быть использованы для атак. Статья рассматривает, как злоумышленники могут эксплуатировать недостатки в алгоритмах энергосбережения процессоров, приводящие к утечке информации, производительным атакам и сбоям системы. Также рассматриваются методы защиты, включая усовершенствования алгоритмов и аппаратные решения.

Ключевые слова: Уязвимости, алгоритмы энергосбережения, процессоры, атаки, многоядерные системы, утечка информации, защита.

EXPLOITING VULNERABILITIES IN PROCESSOR POWER-SAVING ALGORITHMS FOR ATTACKS

Buetner S.I.
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: serafimkavasaki@gmail.com

As processors evolve and move to multi-core systems, power management algorithms become an essential part of their architecture. These algorithms aim to optimize energy consumption based on load, but in recent years, several vulnerabilities have been discovered that can be exploited for attacks. This article discusses how attackers can exploit weaknesses in processor power management algorithms leading to information leakage, performance attacks, and system crashes. It also explores protection methods, including algorithm improvements and hardware-based solutions.

Keywords: Vulnerabilities, power management algorithms, processors, attacks, multi-core systems, information leakage, protection.

Введение

В последние десятилетия процессоры стали гораздо более мощными и энергоэффективными благодаря многочисленным достижениям в области микроархитектуры. Одним из ключевых факторов повышения энергоэффективности является использование алгоритмов энергосбережения, которые регулируют работу процессора в зависимости от его нагрузки. Эти алгоритмы позволяют процессорам автоматически снижать потребление энергии при низкой нагрузке и увеличивать производительность при повышении требуемых вычислительных мощностей. Тем не менее, несмотря на очевидные преимущества таких

решений, исследования показали, что алгоритмы энергосбережения могут стать уязвимыми к различным типам атак. Эксплуатация этих уязвимостей может привести к утечке конфиденциальной информации, сбоям в системе или даже к целенаправленным атакам, направленным на разрушение работы процессора и его компонентов.

В отличие от других уязвимостей, таких как те, что связаны с ошибками в операционных системах или программном обеспечении, уязвимости в алгоритмах энергосбережения более трудно обнаружимы, так как они часто скрыты внутри низкоуровневых функций управления энергопотреблением. Такие уязвимости могут быть использованы злоумышленниками для проведения атак, которые могут быть неочевидными и продолжаться в течение длительного времени без заметных последствий для пользователя. Важно понимать, что алгоритмы энергосбережения не только оптимизируют расход энергии, но и в некоторых случаях управляют состоянием кэш-памяти, производительностью процессора и временем отклика, что дает атакующим возможность манипулировать этими параметрами для получения несанкционированного доступа к данным или для снижения производительности системы.

Эксплуатация уязвимостей в алгоритмах энергосбережения процессоров для атак

Среди основных типов атак, направленных на алгоритмы энергосбережения процессоров, можно выделить несколько ключевых. Одной из них является атака на канал побочных воздействий, при которой злоумышленники используют изменения в энергопотреблении процессора для получения информации о выполняемых вычислениях. Например, при использовании алгоритмов энергосбережения процессор может снижать свою тактовую частоту или отключать некоторые ядра, что изменяет потребляемую мощность. Эти изменения могут быть зафиксированы с помощью специальных датчиков или анализом времени отклика системы, что позволяет злоумышленникам собирать информацию о процессе вычислений. Таким образом, даже при отсутствии прямого доступа к данным процессора, хакеры могут извлечь конфиденциальную информацию[1].

Другим типом атаки являются так называемые атаки на производительность, когда алгоритмы энергосбережения используются для уменьшения мощности процессора или временного отключения некоторых его ядер в моменты, когда система должна работать на полную мощность. Злоумышленники могут инициировать такие атаки с целью замедлить работу целевой системы или нарушить её нормальную работу. Например, если вредоносное ПО может принудить процессор работать на низких частотах, это приведет к заметному снижению производительности, что особенно опасно в критических вычислительных задачах[2].

Также стоит отметить проблему утечек информации через "состояния энергосбережения". При переключении процессора в режим энергосбережения могут возникать несанкционированные изменения в его конфигурации, такие как состояния кеша или регистров, которые могут использоваться для восстановления частичной информации о данных, с которыми работал процессор до перехода в этот режим. В некоторых случаях это может привести к утечке криптографических ключей или паролей[3].

Кроме того, более сложные уязвимости могут проявляться при эксплуатации слабых мест в аппаратных решениях, таких как методы мониторинга или системы для детектирования и защиты от атак. Недавние исследования показали, что процессоры, поддерживающие определённые алгоритмы энергосбережения, могут иметь уязвимости, которые позволяют

нарушить их работу, в том числе при работе с многозадачностью, когда несколько программ одновременно используют различные режимы энергосбережения[4].

Защита от таких атак требует применения нескольких подходов. Во-первых, необходимо улучшение алгоритмов энергосбережения, чтобы минимизировать вероятность утечек данных через побочные каналы. Это включает в себя использование более сложных методов шифрования и проверок целостности данных в процессорах, чтобы сделать процессоры менее уязвимыми к такого рода атакам. Во-вторых, важно обновлять прошивки процессоров и использовать аппаратные решения для защиты, такие как специальные датчики и системы мониторинга, которые могут обнаружить попытки манипулировать режимами энергосбережения и предсказать возможные атаки. Также можно ограничить использование некоторых режимов энергосбережения в критических приложениях, где производительность важнее, чем экономия энергии, что поможет снизить риски[5].

Кроме того, операционные системы и приложения должны быть настроены так, чтобы они учитывали потенциал атак, использующих алгоритмы энергосбережения, и принимали дополнительные меры для защиты от них. Например, системы могут быть настроены для работы только в определённом диапазоне энергопотребления, чтобы избежать неожиданных изменений в режиме работы процессора. Также можно использовать сегментацию приложений и вычислительных ресурсов для того, чтобы гарантировать, что приложения с повышенными требованиями к безопасности не используют общие ядра или режимы энергосбережения, которые могут быть уязвимы к атакам.

Заключение

Уязвимости в алгоритмах энергосбережения процессоров становятся всё более важной темой в контексте безопасности современных вычислительных систем. Хотя алгоритмы энергосбережения играют ключевую роль в снижении потребления энергии и повышении эффективности работы процессоров, их уязвимости могут быть использованы для проведения атак, которые серьёзно угрожают безопасности данных и стабильности системы. Эксплуатация таких уязвимостей возможна через каналы побочных воздействий, манипулирование производительностью процессора и утечки информации. Для защиты от таких атак необходим комплексный подход, включающий как улучшение самих алгоритмов энергосбережения, так и использование аппаратных и программных средств защиты, которые могут минимизировать риски.

Список литературы

1. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262
2. 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.
3. 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.

4. 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
5. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.

References

1. Gelfand A.M. Ways of choosing stegocontainers for data transmission //Regional informatics and information security. - 2020. – pp. 260-262
2. Kushnir D. V. Research and development of methods for distributing confidential data over quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.
3. Lesnova E. M., Pestov I. E. Development of an error detection and correction method for a distributed information network based on big data //Regional informatics and information security. - 2018. – pp. 236-240.
4. 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
5. Petrova T. V. and others. Approaches to detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.