DOI 10.37882/2223-2966.2025.03.32

НОВЫЙ СИСТЕМНО-АРХИТЕКТУРНЫЙ ПОДХОД В ОБЛАСТИ СОЗДАНИЯ ДОВЕРЕННОЙ СРЕДЫ ВЫЧИСЛЕНИЙ СТАЦИОНАРНЫХ И БОРТОВЫХ СУПЕРКОМПЬЮТЕРОВ

NEW SYSTEM-ARCHITECTURAL APPROACH IN THE FIELD OF CREATING A TRUSTED COMPUTING ENVIRONMENT FOR STATIONARY AND ON-BOARD SUPERCOMPUTERS

A. Molyakov

Summary. The article describes a system-architectural approach in the field of creating a trusted computing environment for stationary and on-board supercomputers, based on the methodology of managing processes by hardware hypervisors and transactional memory controllers, characterized by the construction and formalization of algorithmic solutions for monitoring request processing at all levels of the hierarchy, allowing to solve the scientific problem of supervenience (security of interconnected interface layers).

Keywords: operation timing, hardware transactional memory, secure multi-domain hypervisor, execution context.

Моляков Андрей Сергеевич
кандидат технических наук, доцент,
Российский государственный гуманитарный университет, г. Москва
andrei_molyakov@mail.ru

Аннотация. В статье описывается системно-архитектурный подход в области создания доверенной среды вычислений стационарных и бортовых суперкомпьютеров, основанный на методологии управления процессами аппаратными гипервизорами и контроллерами транзакционной памяти, отличающийся построением и формализацией алгоритмических решений мониторинга обработки запросов на всех уровнях иерархии, позволяющий решить научную проблему супервентности (безопасности взаимосвязанных интерфейсных слоев).

Ключевые слова: тайминг операций, аппаратная транзакционная память, защищенный мультидоменный гипервизор, контекст выполнения.

Введение

Какие трудности возникают при обеспечении информационной безопасности в контексте внедрения супер-ЭВМ? Необходимо изучить, как использование суперкомпьютерных инновационных технологий повлияет на формирование географически распределенных вычислительных систем, особенно в вопросах предотвращения несанкционированного доступа.

Требования к уровню подготовки пользователей и специалистов по безопасности значительно повышаются. Это объясняется тем, что суперкомпьютеры представляют собой сложные распределенные архитектуры, работающие с глобально адресуемой памятью и обрабатывающие колоссальные массивы данных. Для эффективного взаимодействия с их специализированным программным обеспечением (ПО) требуются дополнительные знания и обучение.

Суперкомпьютерные центры все чаще взаимодействуют с государственными организациями, учитывая их стратегическую роль в национальных вычислительных системах. Обрабатываемая ими информация включает данные различного уровня конфиденциальности, что диктует необходимость усиления мер безопасности для предотвращения утечек.

Высокая производительность суперкомпьютеров усложняет обнаружение вредоносного ПО, что затрудняет выявление подозрительной активности.

1. Классы защиты стационарных и бортовых супер-ЭВМ

Основные стратегии, направленные на решение задач в области создания суперкомпьютеров, предполагают существенное повышение степени параллелизма в аппаратных решениях при одновременном снижении затрат на выполнение отдельных операций [1]. Наряду с этим активно внедряются передовые технологии передачи данных, современные подходы к трехмерной сборке электронных компонентов и др. Эти меры дополняются интеллектуальными методами повышения устойчивости систем к сбоям.

Комплексное решение проблемы безопасности заключается в разработке суперкомпьютеров, оснащенных аппаратными средствами, которые обеспечивают многоуровневую защиту данных и программного обеспечения. Необходимо определить метрики для различных конфигураций стационарных и бортовых суперкомпьютерных вычислительных систем.

Выделим три основных класса стационарных суперкомпьютерных систем:

— *Тип 1: малый промышленный кластер* — ОЗУ: 250–500 ТБ, глобально-адресуемая память: 50–100 ПБ, бисекционная пропускная способность канала: 50–100 Гб/с, используются «легкие» ядра;
— *Тип 2: средний кластер* — ОЗУ: 500 ТБ — 1 ПБ, глобально-адресуемая память: 50–100 ПБ, бисекционная пропускная способность канала: 100–250 Гб/с, применяются «средние» ядра;
— *Тип 3: стратегический класс* — ОЗУ: 50–100 ПБ, глобально-адресуемая память: 50–100 ПБ, бисекционная пропускная способность канала: 500 Гб/с — 1 Тб/с, используются «тяжелые» ядра.

Отдельно определим класс бортовых суперкомпьютеров — ОЗУ: 100–200 ТБ, глобально-адресуемая память: 1–10 ПБ, бисекционная пропускная способность канала: 10–50 Гб/с, используются «сверхлегкие» ядра. Этот класс включает два подтипа: одноплатные и многоплатные бортовые вычислительные модули.

Суперкомпьютерные системы являются критически важными для решения сложных вычислительных задач в различных областях, от климатического моделирования до геномики. Каждый из указанных типов систем имеет свои особенности и предназначения.

Малые кластеры идеально подходят для научных исследований и образовательных целей, где требуется высокая производительность при ограниченных бюджетах.

Средние кластеры предоставляют баланс между мощностью и экономией, что делает их подходящими для крупных организаций и исследовательских институтов, работающих с объемными данными. Их способность обрабатывать более сложные вычислительные задачи позволяет активно использовать эти системы в различных отраслях, включая финансы и биомедицину.

Стратегический класс суперкомпьютеров может справляться с задачами, требующими огромных вычислительных мощностей, такими как симуляции ядерных взрывов или исследование свойств новых материалов.

Бортовые суперкомпьютеры, благодаря своей компактности и энергоэффективности, находят применение в авиации и космических исследованиях, позволяя проводить сложные вычисления непосредственно на борту.

Защита суперкомпьютеров в значительной мере зависит от их классовой принадлежности.

Малые кластеры, как правило, имеют более ограниченные ресурсы и задачи, что позволяет применять менее сложные механизмы защиты. Однако даже они подвержены угрозам, и необходимо учитывать аспекты физической безопасности и управление доступом, чтобы минимизировать риски.

Средние кластеры требуют усиленной защиты, так как часто используются в научных и коммерческих исследованиях. Здесь важно внедрение многоуровневых систем безопасности, включая шифрование данных и мониторинг сети.

Стратегический класс суперкомпьютеров выполняет ключевые функции в государственных и оборонных структурах. Защита таких систем должна быть многофакторной и включать как физические меры, так и передовые технологии в области кибербезопасности. Это необходимо для обеспечения конфиденциальности и целостности данных, а также для защиты от целенаправленных атак, которые могут угрожать национальной безопасности.

По сравнению со стационарными суперкомпьютерами бортовые супер-ЭВМ обладают ограниченными ресурсами, поэтому набор режимов защиты и т.п. для них основывается на сочетании минимальных потерь производительности и достижении базового уровня безопасности.

2. Научная проблема супервентности

В сфере инженерии и производства, рассматривая разработку защищенных суперкомпьютеров, известна научная проблема супервентности: взаимодействие между изменениями в программном обеспечении и настройками аппаратного обеспечения становится ненадежным и неуправляемым, что обусловлено высокой асинхронностью и сложными связями при обработке больших массивов данных [2, 3].

Кроме того, существуют теоретические и концептуальные ограничения, связанные с действующими подходами, установленными ФСТЭК России и другими регулирующими документами. При использовании исключительно вербальных описаний возникает трудность в создании модели верификации, которая бы учитывала трассировку и временные характеристики операций на нижнем уровне иерархии команд.

Необходима интеграция различных аспектов безопасности и функционирования систем, что подразумевает более глубокое исследование и разработку подходов к анализу. Важным направлением становится разработка методов формальной верификации, которые позволят создать надежные и безопасные модели взаимодействия программного и аппаратного обеспечения. Эти принципы и подходы должны учитывать не только функциональные, но и нефункциональные аспекты, такие как безопасность, производительность и устойчивость к внешним воздействиям.

Решением является внедрение языков описания систем, которые предлагают более строгие синтаксси-

ческие и семантические правила для формализации взаимодействий. Кроме того, необходимо учитывать специфику многоуровневых архитектур суперкомпьютеров, где сегменты памяти и операционной обработки могут иметь разные уровни доступа и защиты. Разработка и внедрение новых стандартов на уровне архитектуры может сыграть ключевую роль в обеспечении совместимости и безопасности.

Проектирование защищенных суперкомпьютерных систем в стационарном и бортовом исполнении систем требует взвешенного подхода, где нефункциональные требования становятся не менее важными, чем функциональные. Безопасность данных, например, требует внедрения многоуровневых механизмов защиты, которые могут обеспечить безопасное взаимодействие различных компонентов системы.

Производительность систем должна оптимизироваться с учетом архитектуры суперкомпьютеров. Это включает в себя эффективное управление памятью, чтобы уменьшить узкие места, и оптимизацию параллельной обработки для достижения максимальной производительности.

Специфика многоуровневых архитектур также подразумевает необходимость в динамическом пересмотре доступа к ресурсам, чтобы предотвратить перегрузки и обеспечить устойчивость к сбоям.

В связи с этим мы разрабатываем новый системно-архитектурный подход для создания доверенной вычислительной среды стационарных и бортовых суперкомпьютеров, который основан на методологии управления процессами с помощью аппаратных гипервизоров и контроллеров транзакционной памяти. Он уникален тем, что включает механизмы многоуровневого контроля, идентификации и верификации, обеспечивая безопасность любых преобразований и трансляций операций гипервизором при взаимодействии с аппаратными компонентами, что позволяет решить научную задачу супервентности взаимосвязанных интерфейсных уровней суперкомпьютеров.

Такой комплексный подход направлен на повышение надежности и безопасности вычислительных процессов в высокопроизводительных системах, что является ключевым аспектом в современном компьютерном проектировании и архитектуре вычислительных устройств. Все изменения и обработка операций гипервизором при работе с аппаратными ресурсами должны осуществляться в безопасном режиме.

3. Методологии управления процессами аппаратными гипервизорами и контроллерами транзакционной памяти

В качестве спецификации системы используется структура Крипке. Какой эффект появляется с точки зрения научно-технологического решения? В чем выигрыш? Мы оцениваем состояния запускаемых процессов с точки зрения контроля доступа на уровне транзакционной памяти.

Операции выполняются в определенном режиме работы процессора и обращаются только к выделенным им сегментам памяти данных и программ, а не случайно перемещаются по всей оперативной памяти.

Транзакционная память гарантирует атомарность и изолированность параллельно выполняемых задач, а также привязывает сегменты данных и программ к определенному домену защиты [4]. Матрица состояний процессов распределена так по доменам защиты, что были получены наилучшие показатели стабильности и защищенности. Для каждого класса супер-ЭВМ заданы показатели защищённости и уязвимости.

Мы разрабатываем объяснительную методологию с элементами семантической, поскольку каждый маркер описывает, какое действие выполняется в системе, а проверка истинности принимаемых решений на каждой возможной интерпретации правил политик безопасности осуществляется с помощью математических выражений темпоральной логики.

Информационный смысл маркеров состоит в том, что каждую i-ю угрозу можно описать и формализовать в виде конъюнкции предикатов из восьми логических переменных.

Контекст выполнения операции — это набор кортежей, состоящий из восьми логических переменных. Набор коллекций представляет собой конъюнкцию предикатов, заданных на множестве кортежей.

Таким образом, *физический смысл контекста* — это формализованный набор тегов при работе с процессорными модулями и контролерами аппаратной транзакционной памяти — Dom_id, s, Ord, Context_type, Context_id, TCU, TR [5].

Основная особенность суперкомпьютеров заключается в их способности эффективно обрабатывать огромные объемы данных, которые постоянно изменяются, а также справляться с интенсивными потоками входящей информации.

В связи с этим проверка корректности принимаемых решений на всех возможных интерпретациях учитывает специфику суперкомпьютеров, включая временную сложность, связанную с параллельными вычислениями, и пространственную сложность, обусловленную множеством процессорных ядер и их взаимосвязей.

В чем отличие от традиционных подходов? Благодаря применению темпоральной логики механизмы верификации становятся динамичными, учитывая временные аспекты событий. Система адаптирует наборы модальных правил для реагирования на сигнальные события.

Взаимодействие и контроль доступа отслеживаются через набор уникальных признаков — маркеров, представленных в виде кортежей логических переменных. Конфигурации системы формируют множество траекторий на структурах Крипке с использованием маркеров.

Для создания доверенной программной среды на недоверенной аппаратуре предлагается использовать верификатор команд процессора, который проверяет корректность выполнения инструкций на аппаратном уровне. Это дополняется использованием многомодульного гипервизора и контроллеров аппаратной транзакционной памяти, обеспечивающих изоляцию доменов и контроль транзакций, что особенно важно для защиты от атак, направленных на нарушение целостности данных.

Приведем несколько факторов, обеспечивающих доверительность и безопасность функционирования в недоверенной среде:

1) Аппаратная транзакционная память обеспечивает атомарность и изоляцию параллельных задач, связывая данные и программы с конкретными доменами защиты, включая поддержку мультидоменного режима с учетом уровней привилегий;
2) Мониторинг событий на всех уровнях иерархии выполнения запросов. Гипервизор транслирует операции, а верификатор команд контролирует их выполнение, предотвращая несанкционированный доступ к памяти;
3) Модуль верификации работает на более высоком уровне привилегий, чем ядро управляющей операционной системы и монитор виртуальных машин, обеспечивая прямое взаимодействие гипервизора с контроллерами памяти и процессорами;
4) Гипервизор создает изолированную среду исполнения, контролируя доступ к файловой системе, сетевым протоколам и распределению ресурсов. Изолированность гарантирует, что параллельные задачи не влияют на результаты транзакций, обеспечивая разделение адресных пространств пользователей;
5) Запросы связываются с тегами, которые фиксируют контекст выполнения и временные ограничения. Теги накапливают информацию о трассе запроса, а доступ контролируется через предикаты и маркеры;
6) Изменения в логической структуре тегов сигнализируют о подозрительной активности.

Заключение

Разработка новых теоретико-методологических и программно-технических подходов, а также принципов обеспечения защиты, учитывающих архитектурные, функциональные и другие особенности супер-ЭВМ, имеет важное значение для решения актуальной научной проблемы — проблемы супервентности, что позволяет создавать доверенную среду для выполнения вычислений в стационарных и бортовых суперкомпьютерных системах, играющих ключевую роль в развитии отрасли «Информационная безопасность» критической информационной инфраструктуры Российской Федерации. Это подчеркивает практическую значимость исследований в данной области.

Наш системно-архитектурный подход в области создания доверенной среды вычислений стационарных и бортовых суперкомпьютеров основан на использовании формальных методов анализа и синтеза безопасных конфигураций системы.

Это позволяет минимизировать риски, связанные с ошибками в параллельных вычислениях, и обеспечивает корректность работы на всех этапах выполнения задач.

В отличие от традиционных подходов, где верификация часто ограничивается статичными моделями, реализация нашей методологии базируется на динамической адаптации к изменениям в системе, что особенно важно для суперкомпьютеров с их высокой степенью изменчивости данных.

Ключевым элементом является интеграция темпоральной логики с механизмами многоуровневого контроля доступа, что позволяет отслеживать не только текущее состояние системы, но и её эволюцию во времени. Это достигается за счёт использования маркеров, которые фиксируют изменения в конфигурациях и обеспечивают прозрачность взаимодействия между компонентами гипервизора и контроллеров аппаратной транзакционной памяти. Более того, без интеграции с аппаратной транзакционной памятью и введения многоуровневого контроля невозможно было решить задачу обнаружения и идентификации разного типа киберугроз на всех уровнях иерархии выполнения запросов (команд) супер-ЭВМ.

ЛИТЕРАТУРА

1. Molyakov A.S. A Prototype Computer with Non-von Neumann Architecture Based on Strategic Domestic J7 Microprocessor / A.S. Molyakov // Automatic Control and Computer Sciences. — 2016. — № 50(8). — PP. 682–686.
2. Molyakov A.S. New Multilevel Architecture of Secured Supercomputers / A.S. Molyakov // Current Trends in Computer Sciences & Applications 1(3) — 2019. — Режим доступа: https://lupinepublishers.com/computer-science-journal/special-issue/CTCSA.MS.ID.000112.pdf , свободный.
3. Molyakov A.S. Based on reconfiguring the supercomputers runtime environment new security methods / A. Molyakov // Advances in Science, Technology and Engineering Systems. — 2020. — Vol. 5(3). — P. 291–298. — DOI 10.25046/aj050338.
4. Моляков А.С. Инновационный вариант развития защищенных супер-ЭВМ для решения важных задач фундаментальной медицины и инженерии в России / А.С. Моляков // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. — 2022. — № 4–2. — С. 88–93. — DOI 10.37882/2223–2966.2022.04–2.26.
5. Molyakov A.S. Secured supercomputer technologies in Russia: functional computing units based on multithread-stream cores with specialized accelerators / A.S. Molyakov // Lecture Notes in Networks and Systems. — 2023. — Vol. 448. — P. 559–566. — DOI 10.1007/978-981-19-1610-6_49.

Журнал «Современная наука: актуальные проблемы теории и практики»