МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет

«Московский институт электронной техники»

Институт микроприборов и систем управления

Семичастнов Константин Владиславович

Магистерская работа

по направлению 09.04.01 «Информатика и вычислительная техника»

Разработка SecurityOS для платформы RISC-V с расширением WorldGuard

Студент _____ Семичастнов К. В.
Руководитель, к.т.н. _____ Лупин С. А.

Москва 2025

Аннотация

...

Abstract

...

Содержание

...

Введение

Актуальность

В настоящее время почти каждое вычислительное устройство подвержено проблеме безопасности данных. Примером могут служить такие устройства как: телефоны, планшеты, ПК, консоли, устройства умного дома (IoT), автомобили, смарт-карты, банкоматы, серверы, и т.д. Для обеспечения защиты пользовательских данных могут применяться различные методы, такие как программная проверка полномочий, шифрование, использование выделенных физических носителей. Но самым надежным способом обеспечить безопасность является предоставление доверенной среды исполнения (ДСИ) с архитектурной поддержкой. Например, TrustZone в архитектуре ARM, или WorldGuard в архитектуре RISC-V.

Однако, для обеспечения доверенной среды исполнения, помимо аппаратной поддержки, необходимо программное обеспечение (Доверенная Операционная Система - Secure OS), которая будет исполняться в выделенной среде. Поэтому потребность в легковесной, безопасной и открытой операционной системе, которая способна, работая совместно с Универсальной Средой Исполнения (Liunx OS), обеспечить Доверенную Среду Исполнения для сохранности чувствительных пользовательских данных является актуальной.

Предмет исследования

Предметом исследования является доверенная операционная система для СнК на архитектуре RISC-V с расширением WorldGuard

Объект исследования

Объектом исследования являются доверенные системы исполнения для СнК на архитектуре RISC-V

Цель исследования

Целью работы является создание Доверенной Операционной Системы для обеспечения Доверенной Среды Исполнения для СнК на архитектуре RISC-V

Задачи исследования

Для достижения поставленной цели поставлены следующие основные задачи:

- Анализ современных ДСИ и Доверенных Операционных Систем.
- Разработка Capability-Based модели безопасности ОС
- Разработка архитектуры Доверенной ОС
- Программная Реализация Доверенной ОС с Capability-Based моделью безопасности
- Разработка и реализация Фреймворка Доверенных Приложений
- Эксперементальная проверка работоспособности разработанной Доверенной

Операционной системы
- Эксперементальная проверка устойчивости к атаками на ДСИ

Методы исследования

В ходе проведения диссертационных исследований были использованы методы компьютерного моделирования СнК syntacore-scr9 с помошью эмулятора QEMU с расширением WorldGuard ОС Linux в качестве УСИ.

Научная новизна

Научная новизна диссертационной работы заключается в создании первой открытой Доверенной Операционной Системы для СнК на архитектуре RISC-V с расширением WorldGuard

Практическая значимость работы

Практическая значимости диссертационной работы заключается в обеспечении Доверенной Среды Исполнения для СнК на архитектуре RISC-V с расширением WorldGuard благодаря использованию Доверенной Операционной Системы

Достоверность полученных результатов и выводов

Достоверность полученных результатов и работоспособности разработанной Доверенной ОС базируется на корректном использовании методов исследования и подтверждается экспериментальными результатами.

Личный вклад автора

Все основные результаты диссертационной работы, включая положения, выносимые на защиту, получены автором диссертации лично или при его непосредственном участии.

Положения выносимые на защиту

- Программная реализация Доверенной Операционной Системы для СнК на архитектуре RISC-V с расширением WorldGuard
- Программная реализация Фреймворка Доверенных Приложений
- Результаты устойчивости к атаками на ДСИ

Публикации автора по теме

:(

Структура работы

Выпускная квалификационная работа состоит из введения, четырех глав, заключения, списка литературы из ___ наименований и приложения. Общий объем диссертации - __ страницы, включая __ рисунка и __ таблиц

Список аббривеатур

- ДСИ (TEE) - Доверенная Среда Исполнения (Trusted Execution Environment)
- УСИ (REE) - Универсальная Среда Исполнения (Rich Execution Environment)
- СнК (SoC) - Система На Кристале (System On Chip)
- ОС (OS) - Операционная Систем (Operating System)
- IoT - Internet Of Things (Интернет Вещей)
- DRM - Digital Rights Management (Управление Цифровыми Правами)
- OSHW - Open Source Hardware (Аппаратное Обеспечение с Открытым Исходным Кодом)
- ISA - Instruction Set Architecture (Архитектура Набора Команд)
- RTL - Register Transfer Level (Уровень Регистровых Передач)
- RISC - Reduced Instruction Set Computer (Вычислитель с Сокращённым Набором Команд)
- TCB - Trusted Computing Base (Доверенная Вычислительная База)
- PMP - Physical Memory Protection (Защита Физической Памяти)
- FPGA - Field Programmable Gate Array (Программируемая Пользователем Вентильная Матрица)
- ПО - Программное Обеспечение
- TA - Trusted Application (Доверенное Приложение)
- OTA - Over-the-Air (Обновления по сети интернет)
- TLS - Transport Layer Security (Безопасность Транспортного Уровня)
- SSL - Secure Sockets Layer (Уровень Защищённых Сокетов)
- ADAS - Advanced Driver-Assistance Systems (Усовершенствованная Система Помощи Водителю)
- V2X - Vehicle-to-everything (Транспортное средство-ко-всему)
- CCC - Confidential Cloud Computing (Конфиденциальные Облачные Вычисления)
- SMC - Secure Monitor Call (Вызов Защищенного Диспетчера)
- EPC - Enclave Page Cache (Кэша Страниц Анклава)
- VM (ВМ) - Virtual Machine (Виртуальная Машина)
- SGX - Software Guard Extensions
- SEV - Secure Encrypted Virtualization
- TZ - TrustZone
- WG - WorldGuard
- CSR - Control and Status Registers (Контрольные и Статусные Регистры)
- SBI - Supervisor Binary Interface (Бинарный Интерфейс Супервизора)
- SEE - Supervisor Execution Environment (Среда Выполнения Супервизора)
- TOR - Top of Range (Верхняя Граница Диапазона)
- NA4 - Naturally Aligned Four-byte (Естественно Выровненные Четыре Байта)
- NAPOT - Naturally Aligned Power-of-Two (Естественно Выровненные по Степени Двойки)
- CPU (ЦП) - Central Processing Unit (Центральный Процессор)

Глава 1. Основы и мотивация для создания открытой доверенной операционной системы для СнК на архитектуре RISC-V

1.1 Основы и мотивация

1.1.1 Общие сведения о доверенных средах исполнения

1.1.1.1 Введение в доверенные среды исполнения

Практически все современные вычислительные устройства, начиная от смартфонов и ПК, до автомобилей и серверных систем, используют несколько операционных систем одновременно на одном процессоре. Такие вычислительные среды обычно состоит из обычной среды исполнения, в которой работают основная операционная система и пользовательские приложения, и отдельной безопасной среды исполнения, предназначенной для защиты конфиденциальных данных и кода. Основная цель такого разделения - обеспечить аппаратную изоляцию, позволяющую безопасно выполнять конфиденциальные вычисления, такие как криптография, управление цифровыми правами (DRM) или обработка платежей без возможности вмешательства внешних компонентов системы или потенциальных злоумышленников.

При такой конфигурации с двумя средами обычная операционная система управляет повседневными задачами, в то время как конфиденциальные операции выполняются в защищенной среде. Такое разделение имеет решающее значение для обеспечения безопасности и целостности конфиденциальных данных и операций. Обычный мир (или Нормальный мир), в котором работает основная операционная система, обычно считается ненадежным по сравнению с защищенным миром, который спроектирован так, чтобы быть безопасным и изолированным.

Концепция доверенных сред исполнения (TEE) стала важнейшим компонентом современных архитектур. TEE обеспечивают безопасную среду для выполнения конфиденциального кода и обработки конфиденциальных данных, изолированную от обычной среды исполнения. Эта изоляция обеспечивается аппаратными механизмами, гарантирующими, что даже в случае полной компроментации основной операционной системы или приложений в нормальном мире - безопасность конфиденциальных данных в защищенном мире остается неизменной.

Таким образом, доверенные среды исполнения являются фундаментальным компонентом современных вычислительных сред. Обеспечение необходимой изоляции и защита конфиденциальных данных и кодв делает их незаменимыми в современных реалиях.

1.1.1.2 Эволюция доверенных сред исполнения

С момента появления - доверенные среды исполнения претерпели значительные изменения, обусловленные необходимостью безопасного выполнения кода и

конфиденциальности данных в современных вычислительных системах. Концепция TEE возникла как ответ на растущий спрос на безопасные среды, способные защитить от различных типов атак и угроз.

Самыми ранними формами TEE были специализированные защищенные сопроцессоры или специальные аппаратные модули, такие как смарт-карты и доверенные платформенные модули (TPMS). Эти ранние реализации были разработаны для обеспечения безопасной среды для выполнения конкретных задач, таких как криптографические операции и безопасная аутентификация. Как правило, они были изолированы от основного процессора и обладали собственными защищенными возможностями хранения и обработки данных.

По сравнению со старыми версиями TEE, современные TEE стали более интегрированными с основным процессором и операционной системой. Нынешние Доверенные Системы Исполнения предлагают более продвинутые функции безопасности, такие как шифрование памяти, безопасная загрузка и механизмы проверки подлинности. Современные TEE также обеспечивают более гибкую и программируемую среду, позволяющую выполнять сложные приложения и сервисы.

Эволюция TEE позволила получить представление о разработке и внедрении Доверенных Сред Исполнения. Ожидается, что будущие разработки TEE будут направлены на устранение все новых возникающих угроз и вызовов. Кроме того, TEE, вероятно, станут еще более интегрированными с основными вычислительными системами, что позволит более эффективно и безопасно выполнять доверенный код и сохранять конфиденциальность данных.

1.1.1.3 Роль доверенных сред исполнения в современных архитектурах безопасности

Доверенные среды исполнения играют решающую роль в современных системах безопасности, обеспечивая безопасную среду для выполнения доверенного кода и обработки конфиденциальных данных. Современные TEE, такие как ARM TrustZone и Intel SGX, обеспечивают аппаратную изоляцию основного процессора. Такая изоляция позволяет выполнять сложные доверенные приложения в сочетании с богатой функционалом универсальной операционной системой.

Возможности современных TEE выходят за рамки простых криптографических задач. Они поддерживают широкий спектр сложных приложений, включая защищенный пользовательский интерфейс, сертификацию, аттестацию и доверенные вычисления в облачных инфрастуктурах.

Несмотря на их популярность и значительные преимущества, которые предлагают доверенные системы исполнения, спрос на TEE с прозрачными интерфейсами и открытым исходным кодом остается. Основными причинами этого спроса являются стремление преодолеть зависимость от поставщиков и повысить безопасность с помощью тщательных проверок. TEE с открытым исходным кодом могут быть тщательно изучены более широким кругом участников сообщества, что потенциально может привести к более безопасной реализации, поскольку уязвимости могут быть выявлены и устранены более эффективно.

Более того, поскольку вычислительные среды становятся все более разнородными и многоядерными, растет потребность в TEE, которые могут эффективно поддерживать такие архитектуры. Способность управлять разнообразными вычислительными ресурсами и обеспечивать их безопасность становится необходимым условием для

поддержания общего уровня безопасности современных систем.

1.1.2. Текущее состояние ДСИ в проприетарных архитектурах

1.1.2.1. Ограничения существующих ДСИ в проприетарных архитектурах

Традиционные доверенные среды исполнения в проприетарных архитектурах, таких как платформы ARM, Intel и AMD, накладывают ряд фундаментальных ограничений. Эти ограничения влияют как на гибкость решений по обеспечению безопасности, так и на более широкую технологическую экосистему.

Большинство проприетарных TEE тесно связаны с платформой поставщика оборудования, что создает среду сильной привязанности к поставщику. Потребители этих технологий, будь то системные интеграторы или разработчики приложений, зависят от производителя оборудования в плане долгосрочных обновлений безопасности, поддержки и совместимости с экосистемой. Эта зависимость ограничивает внедрение пользовательских функций и препятствует внедрению инноваций, поскольку все усовершенствования должны согласовываться с планом действий поставщика и процессом утверждения.

Реализации проприетарных TEE, как правило, имеют закрытый исходный код, а важные архитектурные детали остаются нераскрытыми. Отсутствие прозрачности означает, что пользователи и исследователи не могут в полной мере проводить аудит, изменять или проверять корректность и безопасность реализаций TEE. Кроме того, разработка надежных приложений зависит от жестко контролируемых инструментов поставщиков, SDK и проприетарных API, которые препятствуют переносимости, независимой проверке и росту экосистемы сторонних разработчиков.

Традиционные производители проприетарных процессоров предоставляют только фиксированный набор команд, практически без возможности настройки или расширения системными интеграторами. Такое отсутствие гибкости ISA замедляет реагирование на возникающие угрозы и ограничивает возможности исследователей в изучении альтернативных конструкций TEE.

Каждая запатентованная архитектура, как правило, обеспечивает свою собственную уникальную реализацию TEE, спецификации интерфейса и управление жизненным циклом. В результате, TEE, как правило, несовместимы между поставщиками или даже между различными линейками продуктов одного и того же поставщика. Такой изолированный подход приводит к фрагментации, усложняет разработку кросс-платформенных защищенных приложений и сокращает возможности для более широкой стандартизации и внедрения передовых методов обеспечения безопасности в масштабах всей отрасли.

1.1.2.2 Лицензирование в проприетарных архитектурах

Требования к лицензированию, связанные с проприетарными архитектурами, такими как ARM TrustZone и Intel SGX, играют основную роль в формировании экосистемы сред доверенного исполнения. Эти лицензии имеют важные экономические, юридические и технические последствия, которые влияют на каждый этап разработки и развертывания защищенных операционных систем.

Одним из важнейших последствий лицензирования является его непосредственное влияние на экономику разработки устройств и систем. Доступ к расширениям

безопасности или ДСИ обычно влечет за собой значительные лицензионные платежи, которые должны выплачиваться либо авансом в качестве затрат на разработку, либо постоянно в виде лицензионных отчисленый, привязанных к объемам производства. Для развивающихся компаний и инновационных проектов, работающих с ограниченными ресурсами, эти затраты могут стать существенными препятствиями для выхода на рынок. Даже для хорошо зарекомендовавших себя поставщиков эти сборы увеличивают общую стоимость продукта, снижая рентабельность и приводя к увеличению затрат для конечных пользователей.

Кроме того, наличие ограничений на лицензирование может ограничить масштабируемость. Например, эксперименты с новыми сферами использования, разработка пользовательских аппаратных расширений или внедрение модификаций продуктов для нишевых или региональных рынков могут стать непомерно дорогостоящими, если каждое изменение требует пересмотра условий или дополнительных затрат на лицензирование.

Помимо финансовых затрат, лицензионные соглашения четко определяют и часто ограничивают допустимые сценарии использования и профили разрабатываемых устройств. Эти ограничения могут касаться конфигураций оборудования, конкретных программных пакетов или географии производства и продажи. Они также могут препятствовать техническим инновациям, поскольку любое желаемое отклонение от эталонных платформ или требований к программному обеспечению поставщика, скорее всего, потребует повторной юридической проверки и новых переговоров о лицензировании.

Кроме того, наибольшую обеспокоенность у многих долгосрочных проектов вызывает неопределенность, связанная с использованием лицензий третьих лиц. Поставщики могут в одностороннем порядке изменять условия лицензирования, вводя новые ограничения, увеличивая затраты или даже полностью отказать в правах. Такая непредсказуемость особенно актуальна для продуктов, рассчитанных на длительный срок службы (например, промышленных контроллеров, автомобильных ЭБУ, медицинских устройств), где безопасная эксплуатация и техническое обслуживание могут потребоваться в течение десятилетия и более. Чрезмерная зависимость от внешнего лицензирования представляет потенциальную угрозу устойчивости проекта, его ремонтопригодности и даже соблюдению нормативных требований.

Таким образом, операционная гибкость оказывается ограничена. Это особенно проблематично в исследовательских средах (при быстром создании прототипов) и в промышленных приложениях на заказ (где необходимы эксперименты и быстрая итерация). Наличие эталонных разработок с закрытым исходным кодом и фирменного микропрограммного обеспечения еще больше ограничивает возможности пользователей по проверке или настройке низкоуровневых механизмов безопасности, препятствуя прозрачности и независимой проверке.

Эти ограничения в совокупности создают замкнутость вокруг проприетарных ДСИ, препятствуя функциональной совместимости и независимому росту экосистемы. Сотрудничество между независимыми поставщиками, исследовательскими институтами и сообществом разработчиков с открытым исходным кодом ограничено правовой неопределенностью и отсутствием доступа к базовым технологиям. В результате общий темп внедрения инноваций в области безопасных вычислений замедляется. Техническому сообществу не удается коллективно реагировать на новые угрозы или разрабатывать и внедрять новые средства защиты.

1.1.3. Перспективы RISC-V: открытость и расширяемость

1.1.3.1. Аппаратное обеспечение с открытым исходным кодом

В резком контрасте с этой устоявшейся парадигмой, зараждение движения за аппаратное обеспечение с открытым исходным кодом (OSHW), примером которого является появление и стремительный рост RISC-V, предлагает преобразующую альтернативу. RISC-V - это не реализация конкретного процессора, а ISA с открытым стандартом, что означает, что его базовая спецификация и связанная с ней документация находятся в свободном доступе для любого пользователя, который может использовать, внедрять, проектировать или расширять их без лицензионных сборов или ограничительных соглашений. Этот фундаментальный переход от патентованного контроля имеет глубокие последствия для полупроводниковой промышленности и за ее пределами.

Открытость, присущая RISC-V, способствует созданию действительно объединенной модели разработки. Это позволяет разнообразному мировому сообществу, включающему академических исследователей, отраслевые консорциумы, стартапы и признанные корпорации, вносить свой вклад в развитие ISA, разрабатывать широкий спектр основных реализаций (от глубоко встраиваемых микроконтроллеров до высокопроизводительных процессоров серверного класса) и делиться вспомогательными инструментами и программным обеспечением. Коллективные усилия ускоряют внедрение инноваций, облегчают изучение новых архитектурных особенностей и позволяют быстро изменять дизайн.

Кроме того, прозрачность, обеспечиваемая открытой ISA, имеет первостепенное значение в контексте безопасности. Благодаря общедоступности спецификации и тому, что многие основные реализации также имеют открытый исходный код (доступны в виде RTL), проекты могут быть тщательно изучены, проверены на наличие потенциальных уязвимостей в системе безопасности независимыми третьими сторонами и официально подтверждены. Такой подход значительно расширяет возможности выявления и устранения недостатков в системе безопасности. В отличие от того, чтобы полагаться исключительно на заявления одного поставщика, контролирующего запатентованный непрозрачный дизайн. Такая прозрачность имеет решающее значение для укрепления доверия, поскольку снижает опасения по поводу нераскрытых функциональных возможностей, преднамеренных бэкдоров или недокументированного поведения самого процессорного оборудования.

1.1.3.2. Архитектура набора команд RISC-V

Архитектура набора команд RISC-V является последним достижением в эволюции дизайна процессоров, предлагая современную, открытую и расширяемую основу для вычислений в широком спектре приложений. К основным характеристикам RISC-V ISA относятся ее приверженность принципам RISC, модульность и расширяемость, масштабируемость, а также ее открытый и бесплатный характер. Ее характеристики особенно важны при разработке защищенных систем, в том числе доверенной операционной системы, рассматриваемой в данной работе.

RISC-V - это, по сути, архитектура RISC. В основе этой философии проектирования лежит небольшой, высоко оптимизированный набор инструкций. Ключевые характеристики включают архитектуру загрузки-сохранения (load-store), при которой к памяти обращаются только явные команды загрузки и сохранения, кодировку команд фиксированной длины 32 бит, с возможностью сжатия до 16 бит для повышения плотности, и относительно большое количество регистров общего назначения. Такая простота не только способствует эффективной реализации аппаратного обеспечения с

потенциально более низким энергопотреблением и более высокими тактовыми частотами, но и снижает сложность формальной верификации и анализа безопасности, что потенциально приводит к созданию меньшей и более поддающейся проверке доверенной вычислительной базы (TCB) при проектировании безопасных сред исполнения.

Отличительной чертой RISC-V является его модульность. ISA разработана как небольшой базовый набор целочисленных команд, к которому могут быть добавлены стандартные дополнительные расширения. Эти расширения охватывают такие распространенные функциональные возможности, как умножение и деление (расширение M), атомарные операции (расширение A), операции с плавающей запятой одинарной и двойной точности (расширения F и D), сжатые инструкции (расширение C), векторные операции (расширение V) и манипулирование битами (расширение B). Помимо этих стандартных расширений, RISC-V явно резервирует пространство для кодирования пользовательских расширений. Такая расширяемость имеет решающее значение для безопасности, поскольку позволяет легко интегрировать специализированные расширения, ориентированные на безопасность. Расширение WorldGuard, которое занимает центральное место в этом тезисе, является примером такой архитектурной функции, повышающей безопасность, которая может быть включена в платформу RISC-V без изменения основной ISA.

RISC-V ISA спроектирован таким образом, чтобы ее можно было масштабировать на широкий спектр вычислительных устройств. Она поддерживает 32-разрядную (RV32) и 64-разрядную (RV64) реализацию. Такая масштабируемость позволяет использовать RISC-V в основе различных устройств - от встроенных микроконтроллеров и устройств IoT до высокопроизводительных серверов и суперкомпьютеров. Для систем безопасности это означает, что принципы и механизмы, разработанные для одного класса систем RISC-V, легко могут быть адаптированы и непосредственно применены к другим, что способствует созданию согласованной модели безопасности на различных платформах.

Таким образом, RISC-V ISA обеспечивает гибкую, прозрачную и экономически доступную основу. Принципы RISC, модульность, масштабируемость и, в частности, бесплатный и открытый подход создают благоприятную почву для инноваций в области безопасных вычислений, позволяя разрабатывать специализированные аппаратные расширения, такие как WorldGuard, и способствуя созданию экосистемы, в которой могут процветать открытые, безопасные операционные системы. Эти атрибуты непосредственно поддерживают цели данного исследования по созданию открытой доверенной операционной системы для СнК на ахритектуре RISC-V с расширением WorldGuard.

1.2. Постановка задачи

1.2.1. Текущее положение ДСИ в архитектуре RISC-V

1.2.1.1. Текущее состояние экосистемы безопасности RISC-V

Архитектура RISC-V, обладающая открытой и расширяемой природой, представляет собой сильную основу для создания безопасных вычислительных систем. Однако экосистема безопасности, окружающая RISC-V, в настоящее время находится на стадии зарождения, особенно по сравнению со зрелыми архитектурами, такими как ARM или x86. Эта незрелость проявляется в нескольких ключевых областях, которые создают как проблемы, так и возможности для разработки надежных доверенных сред исполнения.

Важной проблемой существующей экосистемы безопасности RISC-V является отсутствие зрелых и широко распространенных стандартизированных реализаций доверенной операционной системы (SecureOS) для RISC-V. Хотя существуют академические проектоы SecureOS и проектов, ориентированных на конкретных поставщиков, им не хватает зрелости, всеобъемлющего набора функций (например, полного соответствия Global Platform API), тщательного тестирования и широкой поддержки сообщества, характерных для устоявшихся экосистем ДСИ. Это вынуждает компании либо создавать эти компоненты с нуля, либо полагаться на решения, зависящие от конкретного поставщика и потенциально несовместимые друг с другом.

В то время как RISC-V определяет базовый ISA и аппаратные расширения, критически важные для безопасности, например, PMP, новые расширения, специфичные для ДСИ, такие как WorldGuard, все еще находятся на различных стадиях стандартизации.

Таким образом, в то время как RISC-V ISA предлагает фундаментальные компоненты для обеспечения безопасности, в ее экосистеме безопасности наблюдается нехватка готовых и стандартизированных решений ДСИ и инструментов управления. Это состояние подчеркивает значительные возможности и необходимость разработки открытых, надежных и стандартизированных безопасных реализаций ОС.

1.2.1.2. Текущее состояние расширения WorldGuard

Расширение RISC-V WorldGuard представляет собой активно развивающийся подход к обеспечению аппаратной безопасности на основе архитектуры RISC-V. Как новая спецификация, оно отражает открытый и расширяемый характер RISC-V, позволяя сообществу вносить свой вклад и итеративно совершенствовать его. Однако на момент написания работы WorldGuard еще не получил статус полностью ратифицированного стандарта RISC-V. Этот эволюционирующий характер подразумевает что спецификация все еще подвергается потенциальным доработкам и формализации в рамках сообщества RISC-V.

Несмотря на свой неутвержденный статус, расширение WorldGuard уже имеет доступные реализации в FPGA или эмуляторах, таких как QEMU. И предоставляют полный набор аппаратных функций, предназначенных для создания довереных сред исполнения и управления ими. Этих функций достаточно для поддержки концепции безопасных анклавов или *миров*. Реализованных механизмы имеют решающее значение для ДСИ, такие как изоляция памяти, различные уровни привилегий для различных контекстов исполнения и контролируемые переходы между ними. Эти возможности формируют фундаментальные строительные блоки, на основе которых может быть построена надежная система ДСИ.

1.2.1.3. Поддержка WorldGuard со стороны ПО

Однако в настоящее время в программной экосистеме WorldGuard существует значительный пробел, необходимый для использования этих аппаратных примитивов. Несмотря на то, что WorldGuard предоставляет аппаратные возможности для изоляции, существует явная нехватка стандартизированного программного обеспечения с открытым исходным кодом, такого как полноценная доверенная операционная система, специально разработанная для управления этими мирами, определенными WorldGuard, и предоставления приложениям функциональных возможностей ДСИ. Текущая поддержка программного обеспечения в значительной степени ограничивается проверкой концепций на низком уровне, академическими исследовательскими проектами или проприетарными для конкретных поставщиков,

которые не являются широко доступными или стандартизированными для более широкого внедрения в экосистему.

Отсутствие легкодоступной и открытой доверенной операционной системы означает, что разработчики не могут легко создавать, развертывать и управлять доверенными приложениями (TA), которые использовали бы аппаратные средства безопасности WorldGuard. Следовательно, потенциал WorldGuard по созданию надежных ДСИ на платформе RISC-V остается в значительной степени неиспользованным. Эта ситуация подчеркивает острую необходимость и возможность разработки доверенной операционной системы.

1.3. Актуальность и области применения

1.3.1. Стремительный рост RISC-V в коммерческой и промышленной сферах

1.3.1.1. Широкое Внедрение В Различных Областях Производства

Архитектура RISC-V получает все более широкое распространение, решительно переходя из области, представляющей преимущественно академический и экспериментальный интерес, в область ощутимого присутствия в широком спектре реальных коммерческих продуктов. Это очевидное проникновение в ключевые сектороы демонстрируют ее универсальность и растущее доверие отрасли.

Например, системы промышленного контроля и автоматизации производства все чаще используют RISC-V СнК. В быстро расширяющейся области обработки данных RISC-V находит применение и в локальных и периферийных облачных вычислительных платформах, где его открытый характер позволяет создавать индивидуальные решения и ускорители для конкретных приложений, способствуя повышению энергоэффективности и оптимизации производительности.

Кроме того, и сетевое оборудование, включая маршрутизаторы, коммутаторы и сетевые интерфейсные платы, чаще становится оснащено ядрами RISC-V для обработки пакетов и менеджментом слоями управления. Масштабируемость архитектуры делает ее подходящей для широкого спектра встраиваемой бытовой электроники, от маломощных микроконтроллеров в устройствах умного дома и портативных устройствах, до более сложных систем на кристаллах в автомобилестроении и мультимедийных устройствах.

Такое широкое внедрение в различных категориях продуктов подчеркивает, что RISC-V выходит за рамки узкоспециализированных приложений.

1.3.1.2. Отсутствие продуктов, интегрированных в систему безопасности

Несмотря на растущее повсеместное внедрение и универсальность RISC-V в различных областях, проблемой современного рынка является отсутствие глубоко интегрированных, поддерживаемых аппаратным обеспечением ДСИ в коммерчески доступных продуктах. Несмотря на то, что в настоящее время развертывается множество систем на кристаллах, основанных на RISC-V, в них отсутствуют функционал безопасности, который обычно присущ зрелым проприетарным архитектурам.

Ситуация резко отличается от таких экосистем, как ARM, где технология TrustZone является широко распространенным и фундаментальным компонентом многих процессоров, или архитектуры x86, которая предлагает надежные решения безопасности, такие как Intel Software Guard Extensions (SGX) и AMD Secure Encrypted Virtualization (SEV), широко встроенные в линейки продуктов.

Хотя базовые механизмы безопасности, такие как PMP, присутствуют в ядрах RISC-V, обеспечивая базовый уровень изоляции памяти, они не соответствуют полным возможностям и гарантиям, предоставляемым выделенным ДСИ. Отсутствие ПО для оснащенния ДСИ, в настоящее время ограничивает их применение в областях с жесткими требованиями к безопасности или требует нестандартных решений на заказ.

1.3.1.3. Мотивация к разработке доверенного ПО на базе RISC-V

Текущее состояние RISC-V, характеризующееся быстрым ростом, но заметным отсутствием готовых интегрированных продуктов для обеспечения безопасности, является убедительной мотивацией для разработки специализированных решений для обеспечения безопасности. Ключевыми факторами являются:

- Удовлетворение рыночного спроса:
  Критическая роль безопасности в аналогичных областях применения ARM и x86 указывает на то, что рынок предъявляет высокие требования к защищенным продуктам по мере развития архитектуры и распространения в коммерческих и промышленных областях. Для удовлетворения ожидаемого спроса на надежные вычислительные возможности необходима активная разработка.

- Формирование экосистемы:
  Участие в создании безопасных решений на базе RISC-V на ранних этапах дает значительную возможность влиять на разработку стандартов, внедрять лучшие практики и вносить вклад в развитие основополагающих технологий.

- Использование открытости RISC-V и расширений:
  Открытый характер RISC-V ISA в сочетании с развивающимися архитектурными расширениями, ориентированными на безопасность, такими как WorldGuard, облегчает создание защищенных операционных систем с открытым исходным кодом, а также программных пакетов доверенных приложений.

1.3.2. Области применения доверенного ПО в современных вычислительных системах

1.3.2.1. Основной функционал безопасности в современных продуктах

Современные компьютерные продукты, от мобильных устройств и автомобильных систем до облачной инфраструктуры и интернета вещей, требуют в качестве базовых требований надежный набор функций безопасности. Эти функции имеют решающее значение для защиты конфиденциальных данных, обеспечения целостности системы и поддержания доверия пользователей. Ключевыми из этих важных функций безопасности являются:

- Безопасная загрузка (secure boot):
  Этот процесс гарантирует, что каждый программный компонент, загружаемый во время запуска системы, от начального загрузчика до ядра операционной системы, является подленным. Он устанавливает цепочку доверия (chain of trust),

предотвращая выполнение несанкционированного или вредоносного кода на самых ранних этапах работы системы.

- Целостность встроенного ПО и программного обеспечения:
  Помимо безопасной загрузки, необходимы и механизмы для постоянной проверки целостности компонентов ПО перед запуском. Это защищает от угроз и атак, которые могут модифицировать системные компоненты после загрузки.

- Управление криптографическими ключами:
  Надежная генерация, хранение, защита и использование криптографических ключей являются основополагающими в доверенном ПО. Ключи лежат в основе большинства служб безопасности, включая шифрование данных, цифровые подписи, защищенную связь (TLS/SSL) и идентификацию устройств.

- Безопасное хранение:
  Конфиденциальные данные, такие как учетные данные пользователя, личная информация, ключи шифрования и служебные данные приложений, должны быть надежно защищены. Механизмы безопасного хранения обеспечивают конфиденциальность и целостность, даже если универсальная операционная система или носитель информации скомпрометированы.

- Аттестация:
  Эта возможность позволяет устройству предоставлять удаленному серверу информацию, подтверждающую его подлинность.

- Обновления по воздуху (OTA):
  Возможность удаленного и безопасного обновления встроенного ПО для внедрения новых функций и поддержания долгосрочной безопасности и функциональности устройства.

Эти функции больше не являются узкоспециализированными требованиями, а являются неотъемлемой частью проектирования и эксплуатации современных вычислительных систем, что обусловлено ценностью обрабатываемых данных и меняющимся ландшафтом угроз.

3.1.2.2. Потенциал RISC-V в защищённых сценариях применения

Сочетание открытости и расширяемости RISC-V с открывает широкие возможности для проникновения на рынки, где традиционно доминируют запатентованные ISA. Во многом это связано с потенциалом создания прозрачной системы, обеспечивающей безопасность и верифицируемость, способствующие повышению доверия. Нераскрытый потенциал проявляется в многочисленных сценариях применения, требующих высокого уровня надежности:

- Персональные устройства:
  смартфоны, планшеты, ноутбуки и носимые устройства могут использовать откртытую ДСИ на RISC-V для защиты конфиденциальных пользовательских данных, таких как биометрические данные, финансовые данные и личные сообщения.

- Автомобильные системы:
  Современные автомобили с их сложной сетью электронных блоков управления, управляющих всем, от передовых систем помощи водителю (ADAS) до информационно-развлекательных систем и систем связи V2X, требуют надежной

изоляции и безопасности для обеспечения безопасности пассажиров, защиты от несанкционированного доступа и сохранности данных об автомобиле.

- Конфиденциальные облачные вычисленая (CCC):
  на базе RISC-V могут быть обеспечены безопасные анклавы для обработки конфиденциальных данных в мультитенантных облачных средах, обеспечивая защиту "data-in-use" (когда даже поставщик облачных услуг не может получить доступ к расшифрованным данным).

- Экосистема Интернета вещей (IoT):
  Обширный и разнообразный характер устройств интернета вещей, включающий устройства "умного дома", промышленные системы управления, портативные технологии и мониторы критически важной инфраструктуры, так же требуют бережного отношения к имеющейся информации.

- Оборона и аэрокосмическая промышленность:
  Спрос на поддающуюся верификации безопасность и целостность цепочки поставок делает открытые аппаратные и программные решения привлекательными и для критически важных систем военного и аэрокосмического типа.

- Финансовые технологии (FinTech):
  Безопасные интерфейсы RISC-V могут стать основой решений банковской и финансовой сферы, обеспечивая безопасность транзакций, криптографических ключей и обеспечивая безопасные механизмы аутентификации для мобильного банкинга и платежных систем.

1.4. Сравнение с существующими архитектурами

1.4.1. ARM TrustZone: Централизованная модель безопасного мира

1.4.1.1. Обзор ARM TrustZone

Технология ARM TrustZone обеспечивает аппаратное разделение системы на кристалле на две отдельные среды выполнения: нормальный мир (Normal World / NWd) и безопасный мир (Secure World / SWd). Это разделение достигается на уровне процессора с помощью специального режима монитора (Monitor Mode) и аппаратного обеспечения системного уровня, контролирующего доступ к памяти и периферийным устройствам на основе текущего мира исполняющего ядра. В нормальном мире обычно используется богатая функционалом операционная система (Rich OS), такая как Linux или Android, в то время как в безопасном мире используется меньшая по размеру и более надежная операционная система (Trusted OS или Secure OS). Эта доверенная ОС, в свою очередь, управляет и запускает доверенные приложениями (Trusted Applications / TAs). Переходы между нормальным и безопасным миром осуществляются с помощью инструкции *SMC*. Оба мира могут работать на одном и том же процессорном ядре, а аппаратное обеспечение гарантирует, что программное обеспечение обычного мира не сможет напрямую получить доступ к ресурсам, выделенным для безопасного мира.

1.4.1.2. Преимущества ARM TrustZone

- Развитая экосистема и широкое внедрение:
  TrustZone доступна уже много лет и широко используется на самых разных

устройствах, особенно в мобильных и встраиваемых системах. Результатом стала развитая экосистема с обширным набором инструментов, документацией, опытом разработчиков и легкодоступными реализациями защищенных ОС.

- Эффективное переключение контекста:
  Аппаратный механизм переключения между обычным и защищенным миром, с помощью инструкции SMC и специальной аппаратной поддержки, в целом эффективен, так как аргументы для TA передаются через регистры. Это позволяет осуществлять переходы с относительно низкой задержкой при обращении к TA.

- Хорошо поддерживаемые отраслевые стандарты:
  Реализации TrustZone соответствуют отраслевым стандартам, в частности, тем, которые определены стандартами GlobalPlatform. Эти стандарты определяют API и поведение системы для ДСИ, обеспечивая совместимость между различными доверенными приложениями и реализациями Secure OS, облегчая разработку общего программного стека ДСИ.

1.4.1.3. Недостатки ARM TrustZone

- Централизованная архитектура:
  Защищенный мир в TrustZone работает как единый монолитный объект, управляемый одним экземпляром Secure OS. Все защищенные операции со всех ядер проходят через этот централизованный защищенный мир, что может привести к снижению производительности, если многим приложениям или ядрам обычного мира одновременно требуются защищенные службы.

- Высокая стоимость полного цикла взаимодействия:
  Полный запрос от обычного Normal world приложения в пользовательском пространстве (EL0) к доверенному приложению в пользовательском пространстве (EL0) защищенного мира и ответ на него трубуют восемь переключений контекста с использованием различных уровней привилегий и режима мониторинга. Это значительно увеличивает общую задержку и накладные расходы на запросы в secure world, даже несмотря на то что сами переключения контекста имеют аппаратную оптимизацию.

- Блокирование на защищенных операциях:
  Когда приложение нормального мира на определенном ядре выполняет вызов SMC в Secure World, это ядро блокируется, переключая исполнение в Secure World. Это может негативно сказаться на быстродействии и производительности приложения нормального мира, работающего на этом ядре.

- Ограниченная масштабируемость в многоядерных системах:
  в то время как отдельные ядра могут переключаться в защищенный мир, общая модель предполагает использование одного экземпляра Secure OS, управляющей всем защищенным миром на всех ядрах. Это может привести к конкуренции за общие защищенные ресурсы и сложностям в управлении параллельными защищенными операциями, что потенциально ограничивает масштабируемость в высокопараллельных многоядерных сценариях.

- Уязвимость к атакам по сторонним каналам: Несмотря на аппаратную изоляцию, совместное использование базовых физических аппаратных ресурсов (таких как кэш-память, контроллеры памяти и шины) между нормальным и защищенным миром по-прежнему может привести к уязвимостям для side-channel атак, что может привести к утечке информации.

1.4.2. Intel Software Guard Extensions (SGX): Изоляция на базе анклавов.

1.4.2.1. Обзор Intel SGX

Intel Software Guard Extensions (SGX) позволяют создавать анклавы - частные области памяти, изолированные в адресном пространстве приложения. Эти анклавы защищены центральным процессором, обеспечивая аппаратно-принудительную конфиденциальность и целостность кода и данных, находящихся внутри них, даже от привилегированного программного обеспечения, такого как операционная система или гипервизор. Память, связанная с анклавом, шифруется процессором, и при исполнении расшифровывается налету. Приложения могут выборочно размещать чувствительные участки своего кода и данных в этих анклавах, обеспечивая гранулярную изоляцию для каждого процесса.

1.4.2.2. Преимущества Intel SGX

SGX предлагает значительную гибкость, поскольку приложения могут определять и управлять своими анклавами независимо, позволяя множеству анклавов из разных приложений сосуществовать в системе. Технология включает мощные возможности шифрования памяти для данных внутри анклавов и предоставляет надежные механизмы удаленной аттестации. Аттестация позволяет удаленной стороне проверить подлинность и целостность программного обеспечения, работающего внутри анклава. Ключевой архитектурной особенностью является то, что SGX не требует отдельной, выделенной доверенной операционной системы. Анклавы функционируют как защищенные среды пользовательского режима, управляемые, но недоступные для доступа хостовой ОС.

1.4.2.3. Недостатки Intel SGX

Основным ограничением SGX является, как правило, небольшой размер кэша страниц анклава (EPC) - защищенной области ОЗУ, где хранятся страницы анклава, что может влиять на производительность и возможность портирования больших приложений. Модель программирования для SGX сложна, часто требует значительной реструктуризации кода и потенциально создает проблемы совместимости с существующими библиотеками или приложениями. Анклавы SGX ограничены выполнением только в пользовательском режиме (кольцо защиты ring-3), что означает, что полноценная, привилегированная доверенная операционная система не может быть размещена внутри анклава SGX. Кроме того, SGX стала целью многочисленных side-channel атак и атак, использующих спекулятивное исполнение, что требует постоянных исследований и мер по их митигайциям. Накладные расходы на производительность, связанные с операциями входа в анклав (ECALL) и выхода из него (OCALL), а также шифрованием памяти, также могут быть существенным фактором для определенных рабочих нагрузок.

1.4.3. AMD Secure Encrypted Virtualization (SEV): Шифрование памяти на уровне ВМ

1.4.3.1. Обзор AMD SEV

Технология зашифрованной виртуализации AMD Secure Encrypted Virtualization

разработана для усиления безопасности в виртуализированных средах. Это достигается путем предоставления полного шифрования памяти для гостевых виртуальных машин (ВМ), тем самым защищая их от потенциальных угроз, исходящих от скомпрометированного вредоносного гипервизора. SEV в первую очередь ориентирована на сценарии облачных вычислений, где первостепенное значение имеет надежная изоляция между несколькими арендаторами, сосуществующими на общем физическом оборудовании. Память каждой гостевой ВМ может быть зашифрована с использованием уникального ключа, управляемого безопасным процессором AMD (AMD Secure Processor), обеспечивая конфиденциальность данных даже в случае несанкционированного доступа гипервизора к страницам памяти гостевой системы.

1.4.3.2. Преимущества AMD SEV

Одним из значительных преимуществ SEV является практически бесшовный способ обеспечения защиты виртуальных машин. Гостевые операционные системы и их приложения обычно требуют незначительных изменений или не требуют их вовсе для использования зашифрованной памяти. Технология использует надежное, аппаратно-ускоренное AES-шифрование для памяти ВМ. Этот процесс шифрования и дешифрования выполняется в режиме реального времени выделенным аппаратным обеспечением при обращении к памяти, с целью обеспечения конфиденциальности данных гостевой ВМ во время их нахождения в DRAM или при передаче.

1.4.3.3. Недостатки

Несмотря на свою эффективность в защите памяти ВМ, архитектура SEV, ориентированная на шифрование всей ВМ, делает ее по своей сути неподходящей для роли доверенной среды исполнения в контексте изоляции отдельных приложений. Ее основная ориентация на безопасность виртуализации означает, что она работает с гораздо более грубой гранулярностью - вся ВМ, по сравнению с анклавными моделями, Intel SGX, или отдельными архитектурами безопасного мира ARM TrustZone. Следовательно, SEV - это, по сути, механизм защиты ВМ от недоверенного гипервизора, а не предоставление выделенной изолированной среды для запуска конкретных доверенных приложений с детальным контролем в рамках одной операционной системы, что является основным вариантом использования TEE. Это различие ограничивает ее применимость для сценариев, требующих изоляции на уровне приложений и специфической модели программирования для выполнения доверенного кода, отличной от основной ОС.

1.4.4. RISC-V Physical Memory Protection (PMP): Изоляция по уровням исполнения

1.4.4.1. Обзор RISC-V PMP

Physical Memory Protection - это стандартный аппаратный механизм, определённый в спецификации привилегированной ISA RISC-V. Он предоставляет средства для контроля прав доступа к областям физической памяти. PMP позволяет привилегированному программному обеспечению, например, выполняющемуся в Машинном режиме (M-mode), определять множество областей памяти, каждая из которых имеет специфические права доступа (Чтение, Запись, Исполнение). Эти права могут быть установлены независимо для различных уровней привилегий (M-mode, S-mode, U-mode). Конфигурация PMP управляется через набор CSR регистров: *pmpcfgN* - для конфигурации областей и *pmpaddrN* для адресов областей.

1.4.4.2. Преимущества RISC-V PMP

- Стандартное расширение:
  Являясь частью базовой привилегированной ISA, PMP доступна на всех процессорах RISC-V, предлагая базовые возможности защиты памяти без необходимости использования пользовательских расширений.

- Аппаратная безопасность:
  Проверки прав доступа выполняются аппаратно при каждом обращении к памяти, что обеспечивает низкие накладные расходы на производительность и надёжное применение определённых политик защиты памяти.

- Изоляция на уровне привилегий:
  PMP эффективна для установления фундаментальных границ изоляции между различными режимами привилегий. Например, она может предотвратить доступ приложений Пользовательского режима (U-mode) к памяти ОС режима S-mode или областям SEE M-режима.

- Гибкое определение регионов:
  PMP поддерживает различные способы конфигурирования регионов, включая TOR, NA4, NAPOT.

1.4.4.3. Недостатки RISC-V PMP

- Изоляция, ориентированная на уровни привилегий:
  PMP обеспечивает изоляцию на основе уровней привилегий (M, S, U). Она по своей сути не предоставляет механизмов для изоляции программных компонентов, работающих в пределах одного и того же уровня привилегий, и не устанавливает отдельные домены безопасности, независимые от уровня привилегий, что является фундаментальным требованием для TEE. Таким образом, сам по себе механизм PMP не подходит для полноценных реализаций TEE.

- Ограниченное количество регионов:
  Стандарт RISC-V определяет небольшое количество записей PMP (8, 16, или до 64 для RV64). Это ограниченное количество может быть недостаточным для сложных систем, требующих гранулярного разделения множества областей памяти.

- Преимущественно статическая конфигурация:
  Записи PMP обычно настраиваются программным обеспечением M-режима на ранней стадии загрузки. Хотя PMP и перенастраиваема, она не предназначена для высокодинамичного создания и управления изолированными областями памяти во время выполнения менее привилегированными субъектами, как это часто требуется TEE для функциональности, подобной анклавам, или для управления несколькими доверенными приложениями.

1.4.5. RISC-V WorldGuard расширение: Децентрализованная изоляция.

1.4.5.1. Обзор RISC-V WorldGuard

RISC-V WorldGuard - это аппаратное расширение, предназначенное для обеспечения надежного разделения памяти и исполнителей. Оно предлагает более гранулярный подход к изоляции по сравнению с традиционными моделями двух миров, такими как

в ARM TrustZone. WorldGuard обеспечивает возможность создания множества независимых изолированных доменов выполнения, называемых мирами (worlds). Этим мирам могут быть назначены различные привилегии и ресурсы, а на многоядерных системах разные миры потенциально могут работать параллельно на отдельных ядрах ЦП. Расширение предоставляет механизмы для контроля доступа к областям памяти и периферийным устройствам, обеспечивая изоляцию между мирами на аппаратном уровне.

1.4.5.2. Преимущества RISC-V WorldGuard

- Децентрализованный дизайн и масштабируемость:
  Архитектура поддерживает множество независимых миров, повышая масштабируемость и гибкость, особенно для многоядерных процессоров и многопользовательских сред. Каждое ядро может работать в контексте отдельного мира, обеспечивая истинный параллелизм между изолированными средами.

- Открытость и прозрачность:
  Являясь частью открытой архитектуры набора команд (ISA) RISC-V, WorldGuard выигрывает от разработки и верификации сообществом, что ведет к прозрачным реализациям решений безопасности.

- Расширенные возможности и совместимость:
  WorldGuard предлагает расширенный набор функций безопасности по сравнению с более простыми моделями. Например, конфигурация с двумя мирами может точно эмулировать модель TrustZone, облегчая использование устоявшихся API, таких как GlobalPlatform TEE API.

- Неблокирующие безопасные сервисы:
  Возможность выделять определенные ядра для безопасных миров (например, для Secure OS) позволяет выполнять неблокирующие вызовы из других миров (например, из Rich OS, такой как Linux), улучшая отзывчивость системы по сравнению с архитектурами, требующими переключения мира на том же ядре.

- Множество одновременно работающих ДСИ:
  Дизайн по своей сути не ограничивает сосуществование и одновременную работу нескольких экземпляров TEE, каждый из которых потенциально обслуживает различные требования безопасности или различные Rich OS.

1.4.5.3. Недостатки RISC-V WorldGuard

- Ранний этап стандартизации и зрелости экосистемы:
  WorldGuard является относительно новым расширением. Стандартизация продолжается, а широкое распространение аппаратных реализаций и всесторонней программной поддержки все еще находится в процессе.

- Потребность в стеке безопасного ПО: <br Одних только аппаратных возможностей WorldGuard недостаточно. Полное решение TEE требует наличия надежной и специально разработанной Secure OS, сред выполнения, инструментов разработки доверенных приложений, механизмов безопасной загрузки и драйверов. Эта фундаментальная экосистема в настоящее время существует в основном на экспериментальных стадиях.

1.4.6. Сводка и сравнительный анализ

1.4.6.1. Сводка

В следующей таблице представлено наглядное сопоставление рассмотренных архитектур и механизмов, обеспечивающих создание доверенных сред исполнения (ДСИ), по ряду ключевых аспектов.

Характеристика	Intel SGX	AMD SEV
Основной механизм изоляции	Анклавы, защищаемые ЦП (память и исполнение)	Шифрование памяти виртуальных машин
Гранулярность изоляции	Функции/модули приложений	Целые виртуальные машины
Типичная программная модель	SDK для разработки анклавов, управление со стороны ОС	Гипервизор управляет зашифрованной гостевой ОС
Открытость (Архитектура/Спец.)	Проприетарная технология Intel	Проприетарная технология AMD, интерфейсы могут быть открыты
Достаточна для ДСИ?	Нет (ориентирован на анклавы)	Нет (ориентирован на ВМ)
Ключевое преимущество	Сильная изоляция приложений от ОС/ гипервизора	Сильная изоляция ВМ от гипервизора
Ключевое ограничение	Исполнение только в режиме ring-3	Не применима нигде кроме защиты ВМ

Продолжение таблицы

ARM TrustZone	RISC-V PMP	RISC-V World Guard
Аппаратное разделение на защищенный и нормальный миры	Права доступа к областям памяти, конфигурируемые из М-режима	Аппаратно-определённые, изолированные миры исполнения
Уровень ОС (Защищенная ОС vs. Обычная ОС)	Регионы физической памяти	Настраиваемая (например, на уровне ОС для каждого Мира)
Полноценная Защищенная ОС в Защищенном мире	Прошивка/монитор М-режима конфигурирует регионы	Полноценная Защищенная ОС в выделенном Мире
ISA лицензируется; реализации проприетарные	Открытый стандарт RISC-V	Открытый стандарт RISC-V
Да	Нет (только как базовый компонент)	Да
Зрелая, общесистемная модель ДСИ	Базовый, гибкий примитив защиты памяти	Открытая, гибкая изоляция на основе Миров для RISC-V
Проприетарная экосистема, лицензирование	Сама по себе недостаточна для ДСИ	Новизна, отсутствие ПО для экосистемы

1.4.6.2. Сравнительный анализ

Данный сравнительный анализ существующих архитектур и механизмов,

обеспечивающих создание ДСИ, выявляет различные подходы к достижению изолированного исполнения. Каждый из подходов имеет свои особенности, влияющие на разработку Secure OS:

- ARM TrustZone предлагает хорошо зарекомендовавшую себя модель для комплексной защищенной ОС, работающей параллельно с основной ОС, разделяя систему на защищенный и нормальный миры. Несмотря на эффективность, её развертывание привязано к проприетарной архитектуре ARM и связанным с ней моделям лицензирования.

- Intel SGX ориентирована а защиту кода и данных конкретных приложений внутри анклавов, изолируя их от потенциально вредоносной ОС или гипервизора. Эта модель, обеспечивая детальную защиту для целевых участков приложений, не предназначена для размещения полноценной, независимой Secure OS, как это преследуется в настоящей работе. Кроме того, лежащее в основе аппаратное обеспечение и микрокод представляют собой значительную и сложную проприетарную TCB.

- AMD SEV нацелена на защиту целых виртуальных машин путем шифрования их памяти, ограждая их от скомпрометированного или недоверенного гипервизора. Это ценно для облачных сред, но, подобно SGX, изоляция SEV, сфокусированная на виртуальных машинах, не предназначена для модели с двумя совместно функционирующими ОС (Защищенной и Обычной), типичной для ДСИ в стиле TrustZone и модели рассматриваемой в данной работе.

- Механизм защиты физической памяти (PMP) в RISC-V является стандартным функционалом, обеспечивающим фундаментальный, аппаратно-управляемый контроль доступа к регионам памяти. PMP - это неотъемлемый строительный блок для любой безопасной системы на RISC-V, включая ДСИ, так как он позволяет изолировать память. Однако одного лишь PMP недостаточно для определения отдельных миров исполнения или предоставления комплексной архитектурной поддержки, необходимой для полноценной ДСИ. PMP в основном служит M-режиму для сегментации доступа к памяти для менее привилегированных режимов и не имеет встроенных механизмов для переключения между мирами или сложного управления привилегиями сверх стандартных режимов RISC-V.

- Расширение World Guard для RISC-V специально разработано для удовлетворения потребности в надежной, аппаратно-обеспечиваемой инфраструктуре ДСИ на открытой архитектуре RISC-V. Позволяя создавать множество изолированных миров, оно предоставляет прямой архитектурный аналог таким концепциям, ARM TrustZone, и потенциально предлагает более децентрализованные возможности изоляции.

Chapter 2. Core Principles of Trusted Execution Environment and Threat Model

TEE Overview

Definition and Core Principles

Trusted Execution Environment

- descrption: secure area of a main processor ...
- list core principles

Isolation

- separaion on Rich Environment and Trusted Environment

Integrity

- guarantees that the code and data within it are untampered

Confidentiality

- Data and code inside the TEE are kept confidential
- No software outside the TEE can access data inside the TEE

Secure Storage

- storage of sensitive data even when powered off

Attestation

- integrity approval from remote server

Trusted Execution

- Only authorized and verified code can run within the TEE

Minimal Trusted Computing Base (TCB)

- minimizing ccomponents that must be trusted
- root of trust

Security Requirements and Design Goals

Core Components

- ...

Isolated Execution Unit

- dedicated CPU core
- or isolated CPU state

Normal World

- where Rich Execution Environment runs

Secure World

- where Trusted Execution environment runs

Trusted Applications

- Applications running inside the TEE that perform sensitive tasks

Secure Storage

- data stored outside TEE and always encrypted
- but keys can never leave TEE

Memory Isolation

- RAM is divided to Normal, Secure and Shared areas
- Normal area can not be accesed by TEE
- Secure area can not be accessed by REE
- only shared area can be used to transfer data

Cryptographic Engine

- hardware or software module providing secure cryptographic functions

Attestation Mechanism

- hashes of TEE components signed with secure keys

Secure APIs

- Interfaces through which normal applications or the Rich Execution Environment can request services from the TEE

Threat Model

Normal World Assumptions

untrasted OS

- The Normal World is assumed to be fully untrusted
- Normal World can be compromised by malware, user-level or kernel-level rootkits

- No sensitive data can be placed in Normal World

Hostile OS

- The Normal World may attempt to attack the TEE by using privileged access
- read or tamper with TEE memory
- intercept or replay communication with the TEE
- Launching DoS (Denial of Service) attacks against TEE services

Limited Visibility

- The TEE assumes that the Normal World cannot access TEE data

Control over Non-secure resources

- Normal World is responsible for forwarding requests between trusted applications in the TEE and external sources / user

Schedule priorities

- The Normal World may refuse to schedule or service TEE requests
- so by desigh - not Normal world should call TEE, but TEE should check requests by itself

Attack vectors

Direct Memory Access Attacks

- If DMA engines (e.g., from peripherals) are not properly restricted, they might access Secure World memory
- Usage of IOMMU is crucial

Side-Channel Attacks

- Exploit indirect information leakage (timing, power, electromagnetic radiation, cache behavior)
- like Meltdown, Spectre, Red Bleeding
- Constant-time algorithms in the TEE, side-channel resistant hardware, noise introduction, cache partitioning or flushing techniques should be used

Physical Attacs

- Physical attacs Using power glitches, clock glitches, voltage variations, or electromagnetic interference to cause faults
- Physical access combined with Normal World privileges could help mount attacks like probing or injecting malicious signals

API Exploitation

- Malicious Normal World software crafts malicious inputs or sequences of calls to the Secure World, causing buffer overflows, logic bugs, or privilege escalation within the

Secure World
- Strict input validation robust secure OS design should be used

Man-in-the-Middle Attacks

- The communication channel between Normal and Secure World is a major interface
- Normal World manipulates, replays, or drops messages to confuse or exploit Secure World services
- Use cryptographic nonce, session tokens, to validate integrity and freshness

Denial of Service Attacs

- Flooding Secure World with calls, starves it of resources, or blocks communication
- Rate limiting, watchdog timers, graceful degradation

Boot and Firmware Attacks

- Compromise of bootloader or firmware update process can undermine Secure World trust (load malicious secure OS or patch trusted apps).
- Secure boot, cryptographic verification of firmware and Secure World images should be used

World Guard Extension

Overview of the World Guard Concept

...

- *chapter 1 from wg spec*

RISC-V ISA WorldGuard

ISA WorldGuard Extensions

- *chapter 2.0 from wg spec*

WorldGuard CSRs

- *chapter 2.1*

One world per hart

- *chapter 2.2*

Response to permission violations

- *chapter 2.5*

Non-ISA WorldGuard Hardware Platform Components

WorldGuard Markers and Checkers

- *chapter 3.0*

Generic WG Checker

- *chapter 3.1.0*

Configuration Register Memory Map

- *chapter 3.1.1*

Rule Slot Format

- *chapter 3.1.2*

Error-reporting registers

- *chapter 3.1.4*

Operation of the Checker

- *chapter 3.1.5*

Checker Reset

- *chapter 3.1.6*

Boot Sequence and Chain of Trust

RISC-V Boot Sequence Overview

Background on RISC-V System Booting

- Explains the general concept of booting in RISC-V systems. This includes initialization of hardware, loading of firmware components, and establishing the runtime environment for subsequent software layers. It discusses the challenges and constraints in secure boot design.
- An introduction outlining the overall boot process in the RISC-V system integrating both the Secure OS and the Rich OS (Linux)

First Stage Bootloader (FSBL)

- Describes the role of the First Stage Bootloader in the secure boot process
- It is responsible for initial hardware setup, integrity verification of subsequent images, and loading the next boot stage into memory
- This stage is often stored in One-Time Programmable (OTP) memory, establishing the Root of Trust.

OpenSBI Initialization

- Details how OpenSBI initializes the RISC-V Supervisor Binary Interface and prepares the system for both the Secure OS and the Rich OS
- This section explains how OpenSBI manages multi-core initialization while isolating the first core for the Secure OS.

Secure OS Startup

- Describes the booting and initialization of the Secure OS on the first core
- setup of secure and non-secure memory

Rich OS Startup

- Outlines the initialization and booting of the Rich OS (Linux) on the remaining cores
- Explains how linux starts and initializes a driver for communication with Secure World
- Then continue booting as normal

Chain of Trust

Principles of Secure Boot and Chain of Trust

- Introduces fundamental concepts behind establishing a chain of trust
- where each stage of the boot process verifies the integrity and authenticity of the next
- Explains how root keys and cryptographic signatures enforce this trust model.

RISC-V Root of Trust

- Discusses hardware and firmware components acting as roots of trust on RISC-V platforms
- Includes details on embedded ROM or OTP memory used for storing immutable secrets and the first authenticated boot stage.

One-Time Programmable (OTP) Memory

- Examines the use of OTP memory technologies in storing cryptographic keys, bootloader code, or other critical data that forms the immutable basis of system trust
- Explains how this hardware feature prevents modification and enhances security guarantees.

Secure Boot Implementation

- describes that secure boot is out of scope of this project, but that Secure OS is implemented with consideration of Chain Of Trust, and that there is no limitaion of implementing it in future work

---

Chapter 3: Design and Implementation of the Secure Operating System

Interface Considerations

TEE Client API: Inter-World Communication Interface

OP-TEE on RISC-V

- *1.0 from TEE-Client-Api.md*

Develop own minimal GlobalPlatform TEE interface

- *2.0 from TEE-Client-Api.md*

Experemental of Research Prototypes

- *3.0 from TEE-Client-Api.md*

Rationale for Adopting a Global Platform-based API Subset

- Presents the justification for selecting a carefully chosen subset of the Global Platform TEE Client API.

System Architecture Overview

- section provides a high-level perspective on how the Secure OS is structured and how it interacts with the Normal World and hardware.

High-Level Architecture

Architectural Layers

- Introduces the layered nature of the system, from hardware/firmware (OpenSBI) to the Secure OS, and then to the Normal World OS (Linux).
- Emphasizes the isolation between the Secure World and the Normal World.

Secure vs. Normal World Overview

- Explains how the Secure OS permanently occupies the first CPU core while Linux runs on the remaining cores.
- Highlights the roles and responsibilities of each world, along with the boundary-enforcement mechanisms.

Core System Components

Kernel, Resource Managers, and TEE Services

- Details the internal architecture of the Secure OS, covering the Secure Kernel, resource managers (for tasks, memory, and IPC), and TEE service layers.
- Describes how these components collectively provide security, resource allocation, and runtime services to Trusted Applications.

Shared Memory and IPI-Based Communication

- Introduces the fundamental inter-world communication channels, such as shared rings/buffers used for request and response queues.
- Describes how RISC-V inter-processor interrupts (IPIs) are employed for signaling events and synchronizing data transfer between Normal and Secure Worlds.

Memory Layout and Addressing

Physical and Virtual Addressing

- Provides a high-level overview of how the Secure OS configures its page tables and manages physical/virtual addresses.
- Explains how memory mappings differ between the Secure World and the Normal World.

Isolation Mechanisms

- Details how World Guard extension enforces secure boundaries at the hardware level.
- Shows how the Secure and Normal Worlds remain isolated, preventing unauthorized access to protected pages.

Shared Memory Queues

- Explains the reserved memory regions that serve as shared buffers for secure–normal communication.
- Highlights concurrency concerns and locking strategies for ring-buffer manipulation.

Secure OS Execution Flow

Boot Process Overview

- Summarizes the critical steps in transitioning from OpenSBI to the Secure OS, and eventually handing over the remaining cores to Linux.
- Points to more detailed discussion in the “Secure Boot Process and Initialization” section.

Inter-World Transitions

- Outlines the mechanism by which execution moves between Secure and Normal Worlds (e.g., SMC calls, interrupts).
- Covers validation checks before granting world transitions and how the OS ensures secure state persistence.

Scheduling in Secure OS

- Highlights how the Secure OS manages tasks and threads in a uniprocessor environment (the first core).
- Discusses scheduling policies, context switching logic, and how TEE tasks do not interfere with Linux scheduling.

Security and Policy Enforcement

Capability-Based Security Model

- Introduces the core concepts behind object handles, secure syscalls, and fine-grained access control.
- Explains how capabilities are validated and enforced at runtime to prevent privilege escalation.

World Guard Integration

- Consolidates the hardware-based checks provided by the World Guard extension with the Secure OS's software policy.
- Provides an overview of failure handling when unauthorized accesses or invalid world transitions occur.

TA Lifecycle

Creation

- Describes how Trusted Applications (TAs) are registered or loaded by the Secure OS.
- Explores memory allocation, initial code setup, and the procedure for spawning a TA process or thread.

Compute

- Outlines how a TA executes in the Secure OS, including interaction with system calls, access to resources, and concurrency.
- Discusses how TAs can communicate with other tasks or the Normal World during their operational phases.

Teardown

- Explains the orderly shutdown of a TA, covering handle cleanup, memory deallocation, and final status reporting.
- Ensures that no sensitive data remains accessible and that the system reclaims all resources.

WorldGuard Integration

WorldGuard Configuration

World Configuration (Two-World Model)

- Overview of how the system hardware and memory are split between Secure World and Normal World.

- Explanation of the two-world design rationale, focusing on isolation guarantees.
- Definition of the roles of each world (e.g., Secure OS vs. Linux).
- Description of how World IDs (or similar identifiers) are assigned and managed.

WorldGuard Checker Configuration for Secure Isolation

- Overview of the hardware/software checker mechanism for enforcing world-based isolation.
- Configuration of Secure RAM slots and memory regions:
    - Secure memory partitioning approach.
    - Locking down memory regions to the Secure World
- Setting up enclave/partition boundaries:
    - Handling multiple enclaves (if applicable) within the Secure World.
    - Policy for controlling access across enclaves or from Normal World.
- Integration of memory attributes (e.g., read/write/exec permissions) with WorldGuard checks.

Integration with the Secure OS

Error Reporting

- Mechanisms to detect and report WorldGuard-related violations (e.g., unauthorized access attempts).
- Logging and reporting structure within the Secure OS for debugging and auditing.
- strategies for halting offending tasks in case of critical errors.

Managing World Transitions

- Description of the control flow when switching between Normal World and Secure World.
- Handling interrupt-driven transitions across worlds.
- Use of specific CPU instructions or registers to invoke transitions (if applicable).
- Ensuring minimal overhead while maintaining security guarantees.

Communication Pages

- Shared memory pages allocated with permissions for both worlds:
    - Shared memory region layout and alignment considerations.
    - Ensuring read/write restrictions are enforced by WorldGuard.

Secure Boot Process and Initialization

- This section describes how the Secure OS is bootstrapped, transitioning from platform firmware (OpenSBI) to a fully initialized secure environment.
- It covers early assembly-level initialization, kernel relocation, MMU enablement, and higher-level subsystem initialization, ultimately concluding with the handover to any “rich OS” components.

Secure OS Early Initialization

OpenSBI Handover

- Explanation of the OpenSBI boot protocol, which provides the Secure OS with the initial register context (e.g., a0, a1 containing specific parameters).
- SBI boots FW_PAYLOAD_PATH (TEEOS futher) on boot core, making this core secure
- High-level overview of how the Secure OS entry point (_start) is invoked by OpenSBI.
- Handling or storing system parameters (such as the device tree pointer) for further use.

Setting Up the Stack and Basic Memory Layout

- Allocating a stack in physical memory for secure execution.
- How the assembly code (head.S) calculates the stack location (via PAGE_SIZE * 6).
- Ensuring stack alignment for correct RISC-V operation.

First Kernel Relocation

- performing a “relocation” step due to pie (position-independent executable) nuances.
- Creating an identity mapping (physical == virtual) at the kernel load address while also mapping the kernel at its designated virtual base (KERNEL_VIRTUAL_BASE).
- Use of large page mappings (e.g., 2MB or 1GB mappings) for simplicity during early boot.

Enabling the MMU

- Explanation of how the SATP register is configured
- Ensuring the kernel text, data, and bss segments are accessible at both the physical region and the kernel virtual address.

Secure OS Initialization

- Once the minimal MMU and basic mapping are established, the Secure OS transitions to its primary C environment for final setup.

Register Console

- Initializing and registering the console driver (e.g., SBI console) as the primary I/O channel.
- Setting up early debug/log printing to assist with error reporting.

Initialize Page Tables

- Creation and configuration of more granular page tables beyond the initial large block mappings.
- Structures for dynamic region registration and page-level protections.

Second Kernel Relocation (If Needed)

- Further re-mapping kernel virtual addresses after early-boot.
- Cleanup of temporary mappings used during the first relocation phase.

Initialize Trap Handler

- Setting up the vector table or exception table to handle synchronous exceptions and interrupts.
- Registering fault handlers, system call handlers, and other critical exception vectors.

Initialize Timers

- Configuring RISC-V timer CSRs or platform-specific timer hardware.
- Setting up the early tick or scheduling timers.

Initialize Page Allocator

- Creation of a physical page allocator (pmm_init()) to manage secure RAM.
- Data structures (e.g., contiguous free-lists, bitmaps) for tracking page usage.

Initialize Slab Allocator

- A higher-level memory allocator (kmalloc or slab-based).
- Allocation of kernel objects (e.g., tasks, threads, pipes) efficiently.

Initialize Scheduler

- Setup of the scheduler data structures to manage secure OS threads or tasks.
- Timer-driven scheduler hooks using the timer subsystem.

Initialize Root Task

- Creation of the root task (or initial user-mode process in the Secure World).
- Loading or spawning any essential system services.

Initialize Normal World Communication Channel

- Setting up shared memory regions or queues for Normal World <-> Secure World communication.
- Configuring interrupt mechanisms or other signaling channels (e.g., IPI).

Initialize Trusted Applications

- Loading and initializing built-in or pre-installed Trusted Applications (TAs).
- Setting up an environment for TAs, including memory isolation, scheduling, and system call interfaces.

Rich OS Initialization

Initialization by OpenSBI

- Handing control back to OpenSBI to continue its normal boot flow for a Linux or other rich OS.
- TEEOS setups itself and does special ecall that indicates that it has finished
- SBI boots NWD_FW_PAYLOAD_PATH (REEOS futher) on other cpus

Core Startup

- after returing to sbi on secure core - sbi will start second non secure core
- second core will start Linux Kernel, and Linux will hotplug other cores by itself
- Linux will not try to run on first secure core, because it was marked "secure" at the begining of OpenSBI startup

OpenSBI modifications

...

Cross-World Communication

- This chapter describes the mechanisms enabling data exchange and signaling between the Secure OS running on the primary CPU core(s) and the Normal World (e.g., Linux). It focuses on the shared memory queues, the message structure used for TEE commands, and the IPI mechanism for sending interrupts across RISC-V cores.

Shared Memory Queues

- One of the fundamental mechanisms for communication between the Secure World (SWd) and Normal World (NWd) is through shared memory queues. This approach allows concurrent message passing without requiring complex locking operations.

Lock-Free Queue Algorithm

- *https://pskrgag.github.io/post/mpmc_vuykov/*

Shared Memory Ring Buffers

- Overview of how the queues are physically placed in shared memory pages accessible to both SWd and NWd.
- Ring buffer layout: circular array of message slots, head/tail pointers, and optional “sequence” fields for synchronization.
- Memory alignment considerations for preventing false sharing or alignment-related issues.

Requests Queue

- A dedicated ring buffer where the Normal World places requests that the Secure World must handle.
- Steps for enqueuing:

    1. Normal World driver writes the message into the ring slot.
    2. Driver updates the queue head pointer using an atomic operation.
    3. IPI sent (or polling mechanism invoked) to notify Secure World.

Responses Queue

- A separate ring buffer for the Secure World to provide responses or event notifications back to the Normal World.

- The Secure World writes its response into the ring slot, increments the tail pointer, and relies on NWd polling.

Canary Around Shared Pages

- Canary pages are placed around Shared pages with no access bits, so any access by overflowing will trap

Shared Memory Regions

- Aside from the primary queues, certain larger buffers or data structures may be shared.

Memory Region Allocation

- allocation is done by calling secure operation TEE_CMD_ID_MAP_SHARED_MEM
- allocation is done in Secure World, it will allocate pages and set access to Secure world and normal world
- then Secure OS will map pages to Secure Kernel address space to be able to access them
- them Linux should map these pages to Linux Kernel address space

Memory Region Deallocation

- deallocation is done by calling secure operation TEE_CMD_ID_UNMAP_SHARED_MEM
- Secure World will deallocate pages, and remove access from both Secure world and Normal world
- them Secure os will unmap pages from Secure Kernel address space
- then Linux should unmap pages from Linux Kernel address space

Data transfer

- since memory is mapped to Linux Kernel and Secure OS, Operating Systems can transfer data just by regular memory reads and writes

Message Structure

- All commands passed through the request/response queues typically adhere to a consistent message format. This section details the wg_tee_cmd structure, which encapsulates TEE operation parameters and results.

struct wg_tee_cmd

This structure holds command identifiers, session tracking, error codes, and additional parameters.

field id

- uint32_t id
- Identifies the type of TEE operation.
- Possible values include:
    - TEE_CMD_ID_OPEN_SESSION
    - TEE_CMD_ID_CLOSE_SESSION

- TEE_CMD_ID_INVOKE_CMD
- TEE_CMD_ID_MAP_SHARED_MEM
- TEE_CMD_ID_UNMAP_SHARED_MEM

field seq

- uint32_t seq
- filed seq is a unique identifier of command
- it's value is generated just by atomically incremented sequence counter

field session_id

- uint32_t session_id
- Identifies which session within a TA this command belongs to.
- Allows a single TA to manage multiple open sessions simultaneously.

field func_i

- uint32_t func_id
- each Trusted Application implements it's own functionality, and TA can do multiple actions
- field func_id describes what action to do inside TA

field err

- uint32_t err
- Used by the Secure World to return error codes or status results.
- possible results include indicating success, permission failures, or other errors.

field uuid

- uint8_t uuid[16]
- A unique identifier for the Trusted Application.
- Used during TEE_CMD_ID_OPEN_SESSION to select the correct TA.

field paddr

- uint64_t paddr
- A physical address relevant to TEE_CMD_ID_MAP_SHARED_MEM; indicates the start page to map as shared.
- field remain unused for other command IDs.

field num_pages

- uint32_t num_pages
- The number of contiguous pages to map starting at paddr, for TEE_CMD_ID_MAP_SHARED_MEM.
- field remain unused for other command IDs.

field shmem_id

- uint32_t shmem_id
- A handle returned by the Secure OS to reference a mapped shared memory region.
- Allows subsequent TEE_CMD_ID_UNMAP_SHARED_MEM to unmap region

struct wg_param params

- Holds 4 arguments (each is 24 bytes).
- Simple arguments are stored directly
- memory references are stored as three 64-bit values (size, offset, world_id).

padding

- field padding has size of 96 bytes
- Reserved space to align the structure to 256 bytes overall.
- Prevents unwanted compiler padding from interfering with the queue alignment.

IPI Based Signaling

- While the shared queues provide a data structure for messages, an Inter-Processor Interrupt (IPI) mechanism triggers real-time notifications.

RISC-V IPI Mechanism

- High-level overview of the RISC-V interrupt controller and how software sets an IPI to a target hart.
- Explanation of relevant CSRs, memory-mapped interrupt lines, or OpenSBI calls for sending IPIs.
- Typical flows: setting a bit in the IPI register or invoking sbi_send_ipi with a hart mask.

Normal to Secure World Signaling

- Procedure in which the Linux driver or NWd service:

    1. Fills out wg_tee_cmd struct
    2. push struct in the request queue.
    3. Triggers an IPI to the secure hart via an OpenSBI call.
    4. Waits for response by polling the response queue

Secure to Normal World Signaling

- Due to the RISC-V architecture constraints, the simplest approach is for the Secure OS to place responses in the response queue without any other signaling of Normal World
- An IPI back is restricted because of limitations of RISC-V ISA - we can not distinguish Secure OS notification IPI from other types of IPI, so Linux will not be able to handle IPI correctly
- so the NWd driver periodically checks the response queue
- The requesting thread is then woken, a result is available.

TEE API

Global Platform API

Introduction to Global Platform API

- *introduction from OP-TEE Global Platfrom API spec*

TEE Client API

TEE Contexts

- *contexts chapter*

TEE Sessions

- *sessions chapter*

TEE Shared Memory

- *shared memory chapter*

TEE API Specification

TEEC_UUID

- describe ...

TEEC_Result

- describe ...

TEEC_Context;

- describe ...

TEEC_Session;

- describe ...

TEEC_Value;

- describe ...

TEEC_RegisteredMemoryReference;

- describe ...

TEEC_Parameter;

- describe ...

TEEC_Operation;

- describe ...

TEEC_SharedMemory;

- describe ...

TEEC_InitializeContext

- describe ...

TEEC_FinalizeContext

- describe ...

TEEC_OpenSession

- describe ...

TEEC_CloseSession

- describe ...

TEEC_InvokeCommand

- describe ...

TEEC_AllocateSharedMemory

- describe ...

TEEC_ReleaseSharedMemory

- describe ...

Linux Driver Implementation

- This section details the design and implementation of the Linux driver responsible for communication with the Secure OS.
- The driver uses the kernel's TEE subsystem interfaces to expose the Secure OS functionality to user-space applications.
- It establishes shared queues for request and response messages, initializes kernel threads for communication polling, handles incoming replies, and provides TEE-driver–compliant operations such as open session, close session, and invoke command.

Driver Overview and Registration

- Before diving into the shared queues and communication routines, the driver must be discoverable by the Linux kernel and properly registered within the TEE subsystem:

Linux Driver Initialization

1. The device tree node "riscv-wg/nwd_channel" is parsed to read the physical addresses of the shared request and response queues (SQ and CQ).
2. Memory for the driver control structure (struct wgtee) is allocated.
3. Shared queues are remapped into kernel space (ioremap) and initialized with the lock-free MPMC queue mechanism.
4. A TEE device (struct tee_device) is allocated and registered using tee_device_alloc() and tee_device_register().
5. The driver registers a set of callbacks (wgtee_ops), including open_session, invoke_func, etc., which allow user space to interact with the Secure OS through the standard TEE_IOCTL API.

- Key driver entry points: - module_init(wgtee_driver_init) — For device instantiation and registration. - module_exit(wgtee_driver_exit) — For cleanup and teardown.

Linux Driver Interface

- The Linux driver implements TEE-driver–compliant operations exposed via wgtee_ops: - get_version() — Returns the TEE driver version (implementation ID and capabilities). - open() / release() — Allocate or free per-context data (in wg_user_context). - open_session() — Handle TEE_CMD_ID_OPEN_SESSION. - close_session() — (Currently returns -ENODEV as a placeholder). - invoke_func() — Handle TEE_CMD_ID_INVOKE_CMD, forwarding parameters to the Secure OS. - cancel_req() — Not currently implemented.
- To accommodate the TEE subsystem's generic parameter structures (struct tee_param), the driver provides helper routines: - wg_convert_params_in() — Converts Linux TEE parameters into wg_param structures. - wg_convert_params_out() — Converts results back into Linux TEE param outputs.

Shared Queues from the Linux Side

- Shared memory queues form the primary communication channel between the Normal World (Linux) and the Secure World (Secure OS). There are two distinct types of queues in use:

Requests Queue

- The Requests Queue (SQ - Submission Queue) holds commands that the Normal World wishes to send to the Secure OS. For instance, when a user space application issues a TEE_IOCTL command (such as open session or invoke function), that request is packaged into a wgtee_cmd structure and placed into this queue.
- The queue is initialized via wg_communication_init().
- The driver uses mpmc_queue_push() to insert a command (wgtee_cmd) onto the queue.
- Each command is tagged with a unique sequence number (seq) to match responses.

Responses Queue

- The Responses Queue (CQ - Completion Queue) collects asynchronous responses sent back by the Secure OS. Whenever the Secure OS finishes handling a command from the SQ, it places a completed wgtee_cmd structure, including any output parameters or errors, onto the CQ.
- The driver polls this queue in a dedicated kernel thread.
- The mpmc_queue_pop() routine removes the next response command.

- The driver matches responses to ongoing requests by seq number.

Linux Communication Interface

- Communication with the Secure OS involves several key steps: initialization, creating the polling thread, enqueueing commands, waiting for replies, and finalizing when the system is shut down or the module is removed.

Communication Initialization

- The wg_communication_init() routine is responsible for:

1. Mapping the physical memory for the CQ and SQ into kernel virtual addresses (ioremap).
2. Initializing both mpmc queue data structures with mpmc_queue_init().
3. Starting a dedicated kernel thread (polling_thread) that continuously checks for completed commands in the CQ.

Queue Initialization

- Each queue (SQ and CQ) is implemented using the lock-free MPMC (Multiple Producer Multiple Consumer) circular queue: - Memory layout is backed by a contiguous region (one page for SQ, one page for CQ in the current setup). - mpmc_queue_init() sets up the ring buffer indices (head and tail) and ensures alignment. - ioremap_prot() is used to obtain a kernel virtual address for these pages.

Communication Polling kthread

- A single kernel thread (wg_polling_thread) handles responses from the Secure OS by:

1. Checking the CQ queue for any ready responses.
2. Matching each retrieved response to a waiting request via the seq field.
3. Signaling the appropriate completion object (struct completion) so the requesting context can proceed.

- The thread runs until the driver is unloaded or the system is halted.

Message Sending

- When a Normal World request is issued to the Secure OS (e.g., open session, invoke command, or close session):

1. The driver constructs a wgtee_cmd structure, populating fields such as id, func_id, parameters, etc.
2. A unique sequence number is generated with atomic_fetch_inc(&seq_number).
3. The request is placed into the SQ using wg_queue_push().
4. An IPI (sbi_send_ipi) is dispatched to wake up the Secure OS core.

Getting the Result

- Each inflight request has an associated completion entry (wg_completion_entry). The list of waiting requests is protected by a spinlock (waiting_lock). When the Secure OS

writes a response onto the CQ:

1. The polling thread pops it from the CQ.
2. The polling thread scans the waiting_requests list for a matching seq.
3. Once found, it copies fields into the original wgtee_cmd, calls complete() on the associated completion, and removes it from the waiting list.

Communication Finalization

- During driver removal (module_exit) or general teardown:

1. The polling thread is stopped (kthread_stop).
2. Mapped I/O memory for both queues is unmapped (iounmap).
3. The TEE device is unregistered, and any allocated kernel structures are freed.

Дизайн и реализация ядра Secure OS

- В данной секции рассматриваются основные аспекты проектирования и реализации ядра защищённой операционной системы (Secure OS).
- Предложенный подход основан на использовании объектно-ориентированного (capability-based) подхода и позволяет обеспечить высокий уровень изоляции между задачами (tasks) и сервисами (threads), а также гарантировать безопасность при взаимодействии с внешними ресурсами и другими компонентами системы.
- Рассмотрим детальную структуру, начиная с ключевых сущностей и механизмов управления.

Kernel Objects and Handles

- Взаимодействие с ресурсами внутри ядра построено вокруг объектной модели. Каждый объект в системе (например, задача, поток, виртуальный объект памяти, канал связи и т.д.) имеет свой уникальный дескриптор (handle). Доступ к функциональным методам объекта и внутреннему состоянию определяется набором capability-флагов (прав доступа).

Tasks (Processes)

- Задачи (tasks) являются основными изолированными сущностями в Secure OS.
- Они содержат собственное адресное пространство (vm_space) и набор потоков (threads).
- Кодовая составляющая задачи находится в пользовательском адресном пространстве безопасной среды (для Trusted Applications).
- Каждая задача имеет таблицу объектов (object_table), где регистрируются все ресурсы (включая каналы, объекты памяти и др.), предназначенные для её использования.
- создание задачи состоит из следующих этапов:

1. Создание пустой пользовательской задачи (task_create_empty) – формирование объектов структуры task, включая инициализацию отдельных полей (handle_page, object_table и т.д.).
2. Запуск задачи (task_run) – настройка защиты памяти для страницы дескрипторов (handle_page), установка состояния (TASK_SPAWNED) и добавление главного потока задачи в планировщик (sched_insert).

3. Уничтожение задачи (task_destroy) – освобождение адресного пространства (vm_space_destroy) и освобождение динамически выделенной памяти.

- Пример создания задачи на основе системного вызова task_spawn показывает, как пользователь может передать в ядро указатель на точку входа (ep) и handle задачи, а ядро создаёт в ней начальный поток и переводит задачу в состояние выполнения.
- *пример*

Threads

- Каждая задача содержит по крайней мере один поток (thread).
- Потоки отвечают за выполнение кода внутри адресного пространства задачи.
- При создании пользовательского потока ядро настраивает контекст выполнения (регистры, стек, текущее окружение и т.д.).
- При создании процесса (task), ядро создаёт «главный поток» задачи, устанавливая ему точку входа (ep). После этого поток регистрируется в списке потоков (list_head_add_tail) и может быть запланирован планировщиком.

Pipes (или Channels)

- Вместо классических «каналов» (pipes) в ядре используются объекты «channel» (двухсторонние каналы связи). Они создаются фабрикой (см. factory.c, syscall channel_create) и позволяют процессам или компонентам ядра обмениваться сообщениями по дескрипторам с установленными привилегиями.
- Канал представлен двумя концами (rx/tx), которые могут принадлежать одной или разным задачам.

Virtual Memory Objects

- Объекты виртуальной памяти (VM Object) отображают некоторый участок памяти (обычно физической) в адресное пространство задачи.
- В ОС реализован системный вызов vmo_create, который позволяет создавать vm_object через фабрику (factory_object).
- После создания объект регистрируется в таблице дескрипторов с соответствующими правами (OBJECT_CAP_TRANSFER, VMO_CAP_FULL и пр.), что позволяет разграничивать операции чтения, записи и копирования.

Synchronization Primitives

- В ядре имеется набор примитивов синхронизации
- spin_lock
- mutex
- semaphore
- Очереди ожидания (wait_queue_init, wait_object_many) – абстракция, позволяющая потокам ждать появление событий (например, данных в канале).

Task Management

- Механизм управления задачами (Task Management) в Secure OS определяет систему, в рамках которой задачи создаются, запускаются и завершаются.
- В коде ядра представлены несколько ключевых подсистем, реализующих данный

функционал.

Process Model

- Процессная (task) модель предполагает, что каждая задача имеет собственное адресное пространство и набор ресурсов, зарегистрированных в ядре.
- Создание задачи обычно происходит по запросу пользовательского процесса либо при создании сессии для новой TA, через системный вызов (task_create). Перед запуском задачи ядро выделяет нужные структуры данных, инициализирует объект задачи и подключает его к планировщику. При этом задача находится в состоянии TASK_CREATED, пока не будет вызвана функция task_spawn, переводящая её в состояние TASK_SPAWNED.

IPC Service

- В системе используется механизм IPC на основе каналов (channels). Каждая задача может получить дескрипторы двух сторон канала, позволящие выполнять операции чтения/записи (channel_read()/channel_send()).
- Кроме того, для организации группового ожидания сообщений служит вызов wait_object_many, позволяющий одним системным вызовом ожидать события от нескольких объектов.
- Пример кода root_task демонстрирует задачу, которая ожидает сообщения в канале kernel_channel. При появлении нового сообщения конструкция wait_object_many(...) возвращает события от одного или нескольких объектов.
- Затем сообщение извлекается (channel_read) и, результат работы, отправляется обратно (channel_send).

Root Task

- Root Task (root_task.c) является важной задачей, поддерживающей цикл обработки входящих запросов и сообщений от других процессов и ядровых сервисов. Здесь можно заметить:
- Использование структуры wait_entry для инициализации нескольких объектов ожидания (каналов).
- Циклическую обработку arriving-сообщений.
- Вызов nwd_proccess_message для обработки поступивших команд от Normal World
- Таким образом, root task служит центральной точкой обмена сообщениями между Secure OS и Normal World.

Scheduling

- Планировщик отвечает за распределение ресурсов процессора между потоками, находящимися в состоянии готовности к выполнению. В ядре реализованы базовые механизмы планирования, ориентированные на простоту и расширяемость.

Scheduling Service

- Scheduling Service управляет структурами данных, хранящими информацию о потоках (thread) и их состояниях.
- При создании потока он добавляется в очередь работы планировщика (sched_insert), где ему присваивается базовый приоритет и используется политика

Round-Robin (SCHED_RR), которая обеспечивает циклическое распределение времени процессора между всеми runnable-потоками.

Scheduling Policies

- В качестве политики планирования используется Round-Robin, чтобы обеспечить максимальную простоту и уменьшить количество доверенного кода, так как доверенные приложения не обладают сложной логикой, требующей более точной диспетчеризации
- В данной реализации (task_create_initial_thread инициализирует потоки с SCHED_RR) применяется классическая политика Round-Robin. Однако архитектура планировщика может быть расширена для поддержки: - Приоритетного планирования (приоритеты на основе критичности задачи). - Планирования на основе квантования времени (time-slices). - Специальных политик для реального времени (real-time scheduling).

Memory Management Subsystem

- Подсистема управления памятью (Memory Management Subsystem) обеспечивает надежную изоляцию памяти между задачами, а также предоставляет безопасный интерфейс распределения памяти в пространстве ядра и пользовательских задач.

Secure Memory Allocator

- Для работы с динамически распределяемой памятью в ядре используются следующие механизмы:

1. Kmalloc/kvfree (или kfree) для управления небольшими блоками памяти в пространстве ядра (см. пример в factory_destroy или task_create_empty).
2. Специализированные аллокаторы страниц (vm_allocate, vm_space_init_kernel, vm_space_init_user), которые выделяют виртуальные адреса и сопоставляют их с физической памятью, учитывая защитные атрибуты (VMA_READ, VMA_WRITE, VMA_USER).

- В момент инициализации задачи (task_create_empty) вызывается vm_space_init_user для подготовки пользовательского адресного пространства

Memory Isolation

- Механизм изоляции достигается с помощью:

1. Различных адресных пространств (space) для каждой задачи.
2. Управления таблицами страниц (mmu_switch_space), что позволяет ядру переключаться между контекстами задач и гарантировать, что одна задача не может получить доступ к памяти другой.
3. Контроля прав доступа к памяти при вызове vm_protect. Данная функция устанавливает соответствующие флаги (VMA_READ, VMA_WRITE) и обеспечивает недоступность памяти для неавторизованных задач.

- В коде виден пример, когда при запуске задачи (task_run) вызывается vm_protect для установки в памяти read-only доступа к странице дескрипторов (handle page). Таким образом, даже сама задача ограничена в манипуляции с полями, ответственными за управление дескрипторами, если это не предусмотрено

соглашениями по доступу.

File System

linear RAM fs

elf files

Capability-Based Security Model

- This chapter focuses on the design and implementation of the capability-based security model within the Secure OS.
- It explains how the system uses handles to encapsulate capabilities, how these handles are created and managed, and how capability-based access control is enforced through task manifests and the root task.

Handles as Encapsulated Capabilities

- Handles in the Secure OS function as references to system resources (objects). Each handle has associated permissions and metadata defining how it may be accessed or manipulated. Internally, handles map to kernel-managed descriptors that maintain the state, permission bits, and relevant object pointers.

Design Rationale

- Least Privilege Principle: Capabilities ensure that tasks and trusted applications only have the minimum set of privileges needed.
- Fine-Grained Access Control: Provides precise control over which resources can be accessed and how they are used.
- Composability: The handle-based model allows different system components (tasks, services, etc.) to dynamically create and share capabilities in a structured manner.

Objects

- Definition: Objects represent protected resources (e.g., memory regions, tasks, communication channels).
- Creation: created by a specialized factory object or created initally by kernel
- Management: The kernel and corresponding resource managers maintain object lifecycles (allocation, reference counting, destruction).

Object Handles

- Semantics: An object handle is an token referencing an underlying object.
- Handle Table: Each task or trusted application maintains a handle table
- Security Properties: Handles cannot be duplicated or guessed; only the kernel can create valid handles.

Factory Objects

- Factory Concept: There is a singleton act as “factory” capable of creating other objects (e.g., tasks, pipes, or memory objects).

- Controlled Creation: A Manifest ensures that only permitted tasks can spawn or instantiate new objects.
- Lifecycle: Factoty themselve is created by the kernel.

Object Methods

- Method Calls: Operations on objects (e.g., read, write, map) are exposed as system calls.
- Capability Checks: Before performing any operation, the kernel verifies that the caller's handle has sufficient permissions.
- Extensibility: New object types can not define custom methods, which stricts permission volations

Capability-Based Access Control

- The system enforces a strict capability-based security policy, ensuring only authorized handles may invoke methods on objects.

Permissions

- since syscalls act as object methods - there is a fixed number of methods that can be executed on object
- each handle has its own permission bits for each syscall
- Permission Propagation: When a handle is shared between tasks, permissions can only be stricted, to increased.
- Revocation: The kernel can invalidate or downgrade a handle's permissions at runtime if security conditions change.

Task Manifests

- Manifest Format: Each task has a manifest specifying its initial handles and allowed permissions on those handles.
- Initialization: On task creation, the kernel reads the manifest to populate the task's handle table.
- Dynamic Policy: The root task or a privileged controller can update or revoke handles from TA

Root Task

- Privilege Level: The root task is endowed with the highest level of privilege, including the ability to create new tasks and objects
- Handle Distribution: Upon launching a new trusted application, the root task provides the necessary initial handles listed in the manifest.
- Security Enforcement: The root task can audit or modify the capabilities of any other task if required.

Method Invocation

- Invocation Flow:

    1. Trusted application issues a syscall to invoke a method on a handle.
    2. Kernel checks handle validity and permission bits.
    3. Kernel executes the method if authorized; otherwise returns an error.

- Parameter Passing: Depending on the object type, additional data (e.g., memory buffer addresses or message payload) must be specified.
- Audit Logging: A log of handle usage may be maintained for debugging, accountability, and forensics.

Performance Implications

- Lookup Overheads: A balanced design attempts to keep handle operations lightweight to avoid excessive overhead.

Secure Syscalls

- The Secure Operating System exposes a set of privileged system calls (“secure syscalls”) available only to code running in the Trusted Execution Environment (TEE). These syscalls form the backbone of the secure OS abstraction layer and are fundamental to the capability-based model which enforces strict access and isolation. In this section, we describe the secure syscall mechanism, their capability enforcement, and the secure object operations made available to Trusted Applications (TAs).

Secure Entry Points

- The secure syscall interface is the only gateway through which TAs and system objects interact. These system calls are verified and dispatched via central syscall routing infrastructure based on a syscall table indexed by syscall number.

Background on OS System Calls

- A system call facilitates user mode code (in this case, Trusted Applications) to invoke kernel functionality in a controlled and verified manner. Syscalls operate strictly on handles referencing kernel-managed secure objects. The handle list is process-local and authorized through task manifests at TA launch time.

Secure Syscall Lifecycle

- Each secure syscall follows the canonical secure OS object lifecycle:

1. User passes handle(s) and optional state.
2. Kernel resolves the handle reference and asserts access rights using capability tags.
3. Operation is executed atomically.
4. Ownership of resulting objects or memory copies is well defined (copy vs. move semantics).
5. Errors from any stage are returned to the user-space Trusted Application. Syscalls involving inter-task communication (e.g., SYS_CHANNEL_WRITE or SYS_TASK_SHARE_HANDLE) often cooperate with internal kernel structures like queues or per-process handle pages. These components are designed to be strictly partitioned and race-free.

Argument Passing Format

- Syscall arguments are passed following the calling convention of the Secure OS, and include the handle identifiers, pointers to user data, data lengths, and capability-specific flags. Data is validated before being dereferenced or mutation occurs. Shared

memory is always accessed via secure copies using kernel-managed copy_from_user and copy_to_user primitives.

Validation of Handle Permissions

- Each syscall entry validates whether the calling task has the needed capabilities for the given object type. Handles are looked up in the invoking task's object table, and if the lookup fails or lacks the proper capability flags (TRANSFER, WAIT, SEND, RECV, etc.), the syscall returns an error. This fine-grained check ensures robust per-object and per-action filtering in line with the capability-based security model.
- Syscalls rely entirely on the underlying capability-based object model:
- Handles are opaque 32-bit values resolved into kernel pointers via per-task object tables.
- Each handle links to an internal object and permission mask.
- All syscall-side object accesses invoke a type + capability check. For example, in the `channel_write` syscall, the following enforcement occurs:

1. Validate caller owns the provided handle with `CHANNEL_CAP_SEND`.
2. Validate all message-passed handles include the `TRANSFER` capability.
3. Receiver will only receive transferred handles if it has adequate handle table space. This guarantees that:

- Object accesses are never implicit — they must be manifested in the task manifest.
- No object leaks across Trusted Application boundaries.
- Origin and access pathway of each resource is traceable through the handle fabric.

Syscall Specification

- Each system call operates on one or more kernel object handles. Object types include tasks, threads, virtual memory objects (VMOs), factory objects, and channels. Below is an overview of the currently defined syscalls.

SYS_LOG

- Logging interface for debugging output from the secure world.

SYS_VM_ALLOCATE

- Allocates anonymous virtual memory inside a task's virtual address space.

SYS_VMO_CREATE

- Requests creation of a virtual memory object (VMO) via a factory. The new handle is stored in user-writable memory. Capability `FACTORY_CREATE_VMO_CAP` must be present.

SYS_CHANNEL_CREATE

- Asks the factory to produce bidirectional channel endpoints. Returns two handle values referencing peer-connected `channel_endpoint` objects. Requires `FACTORY_CREATE_CHANNEL_CAP`.

SYS_CHANNEL_READ

- Attempts to retrieve a pending message from the associated channel endpoint. Caller must possess `CHANNEL_CAP_RECV`. The syscall verifies receiver-side buffer, optional handle array, and copies message from kernel space.

SYS_CHANNEL_WRITE

- Enqueues a message to be sent over a channel endpoint. Requires capability `CHANNEL_CAP_SEND`. Handles being transferred are verified for `OBJECT_CAP_TRANSFER`.

SYS_TASK_CREATE

- Asks a factory to create an empty task object (stub process). Returns a handle with `TASK_GET_SPACE_CAP` and `TRANSFER`. Initial state is `TASK_CREATED`.

SYS_TASK_GET_SPACE

- Grants the caller access to another task's virtual memory address space (typically for explicit handle passing or object serialization). Requires handle with `TASK_GET_SPACE_CAP`.

SYS_VM_MAP_VMO

- Maps an existing VMO into a task address space with specified offset and permissions.

SYS_VM_FREE

- Unmaps a virtual address range from a VM space.

SYS_TASK_SPAWN

- Spawns a previously created task. Initializes the main thread with a provided entry point. Transitions the task's state from `CREATED` to `SPAWNED`.

SYS_OBJECT_CLOSE

- Releases the given handle in the caller's object table.

SYS_OBJECT_WAIT_MANY

- Waits on multiple kernel objects, useful for synchronization/IPC.

SYS_PHYSMAPPER_MAP

- Maps physical memory ranges for I/O accesses, used by device drivers or MMIO facilities (access controlled based on TA manifest and task capabilities).

SYS_TASK_SHARE_HANDLE

- Allows handle transfer from one task to another. The handle is written along with an identifier string into a memory area expected by the recipient. Available only when receiver is in `CREATED` state. Enforced via handle-page layout in receiver's address context.

SYS_OBJECT_COPY

- Duplicates a handle within the same task, assigning the requested capability mask. Used to derive restricted-view handles (e.g. remove `TRANSFER`).

Trusted Application Framework

- The Trusted Application (TA) Framework provides a lightweight, secure runtime environment and development interface for writing user-mode Trusted Applications atop the Secure OS.
- It defines a standard C runtime environment enriched with system capabilities accessible via a handle-based capability model.
- Its primary role is to facilitate secure software development, ensuring alignment with both TEE security policies and performance constraints in constrained environments.

Standard Library for Trusted Applications

Standard Library Overview

- The standard library is a minimal libc equivalent tailored to the Secure OS TEE context. It provides essential functionality typically found in a standard C runtime, excluding non-secure system calls. Implemented entirely in secure world userspace, the library avoids dynamic linking or unnecessary runtime overhead. It includes: - Memory functions (e.g., memcpy, memset) - Formatting and I/O (e.g., printf) - Math functions (including support for hardware-accelerated routines if available) - Cryptographic primitives - Concurrent synchronization mechanisms - Container utilities (e.g., lists, maps) - Typed object and handle access abstraction

Handle Operations Specification

Channel Functions

- `channel_read` - Read data from a secure communication channel.
- `channel_write` - Send data over a secure communication channel.
- `channel_from_handle` - Cast a generic handle into a channel type.

Factory Functions (Fabric Object Handle Interface)

- `factory_init` - Prepare a factory object for spawning or object creation.
- `factory_create_vmo` - Create a Virtual Memory Object (VMO).
- `factory_channel_create` - Create a new communication channel.
- `factory_task_create` - Create and launch a new Trusted Application task.
- `factory_get_handle` - Retrieve system/manually assigned handles.

Object Functions

- `object_copy` - Duplicate a handle reference.
- `object_close` - Close and discard a handle.

Task Functions

- `task_spawn` - Spawn a new task using a manifest.
- `task_share_handle` - Share handle(s) with another task securely.

Memory Management Functions

- `vm_init` - Initialize virtual memory structures.
- `vm_map_vmp` - Map memory pages into a task's virtual space.
- `vm_free` - Free allocated virtual memory regions.

I/O Standard Library Specification

Printf-Compatible Functions

- `printf` - Wrapper using `tee_log` syscall.
- `sprintf` - Internal memory-safe string writing variant.
- `vprintf` - Variadic-style printf handler.

Logging Function

- `tee_log` - Internal secure log syscall (invokes `SYS_LOG`, tagged output).

Strings Standard Library Specification

String Utility Functions

- `memset`
- `memcmp`
- `memcpy`
- `memmove`
- `memchr`
- `strlen`
- `strchr`
- `strcmp`
- `strtol`
- These are implemented using size-optimized and alignment-aware techniques for low-overhead TA memory environments.

Math Standard Library Specification

Algebraic Functions

- `sqrt`, `pow`, `log`, `exp`, `abs`, `floor`, `ceil`

Trigonometric Functions

- `sin`, `cos`, `tan`, `asin`, `acos`, `atan`

Mathematical Constants

- `pi`, `e`, `inf`, `nan`

Complex Math Functions

- Complex number support is syntactically mirrored from real-number APIs.

Crypto Standard Library Specification

Hashing Functions

- `sha256(data, len)`
- `sha512(data, len)`
- `md5(data, len)`

Encryption/Decryption Functions

- in future work support for functionality like:
- `aes_encrypt`, `aes_decrypt` - Support for AES-GCM/CTR if hardware-accelerated
- `chacha20_encrypt`, `chacha20_decrypt`

Key Management and Derivation

- in future work support for functionality like:
- `hkdf` implementation
- Insecure vs. hardware-sealed key storage distinction

Random Number Generation

- in future work support for functionality like:
- `crypto_rng` - Hardware-backed RNG where available
- `crypto_rng_init_seed` - Optional API for seed injection

Container Standard Library Specification

- Note: Trees are all reentrant and zero-alloc in TA context

List Functions

- Singly Linked List: Init, Push, Pop, Find, Remove
- Doubly Linked List: Bidirectional traversal APIs with embedded nodes

Radix Tree Functions

- Insertion, deletion, lookup optimized for dense ID spaces

WAVL Tree Functions

- Self-balancing tree, relaxed AVL variant, with logarithmic insert/remove

Red-Black Tree Functions

- Balanced binary tree implemented using node-color rules

Concurrency Standard Library Specification

Atomic Operations

- `atomic_add_fetch`
- `atomic_sub_fetch`
- `atomic_or_fetch`, `atomic_and_fetch`
- `atomic_read`, `atomic_write`
- Memory barrier primitives: `smp_rb()` (read barrier), `smp_wb()` (write barrier)

Mutex API

- `mutex_init()`, `mutex_lock()`, `mutex_unlock()`, `mutex_destroy()`

Spinlock API

- `spinlock_init()`, `spin_lock()`, `spin_unlock()`, `spin_trylock()`

Semaphore API

- `sem_init()`, `sem_wait()`, `sem_post()`, `sem_destroy()`

Conditional Variables

- `cond_init()`, `cond_wait()`, `cond_signal()`, `cond_broadcast()`

Misc Library Functions Specification

Align Macros

- `align_up(x, a)`
- `align_up_ptr(p, a)`
- `align_down(x, a)`
- `align_down_ptr(p, a)`
- `is_aligned(x, a)`
- `is_aligned_ptr(p, a)`

Bit Manipulation

- `bit32(n)`, `bit64(n)`
- `is_power_of_two(x)`
- `clz32(x)` - Count Leading Zeros (32-bit)
- `clz64(x)` - Count Leading Zeros (64-bit)
- `log2(x)`

Compiler and Intrinsic Macros

- `barrier()` - Compiler-level memory fence
- `container_of(ptr, type, member)` - Offset-based typed accessor
- Standardized `__attribute__` usage for alignment/enforced inlining.
- `same_type()` - Static type matching check (debug-mode only)

Implementation Challenges and Optimizations

- This section discusses the practical challenges encountered during the development of the Secure OS and outlines optimizations applied to ensure a balanced trade-off between performance, security, and maintainability.
- It also examines developer tooling, build considerations, and key lessons learned from implementation.
- The intent is to provide transparency about the engineering process and to offer insights to future developers working in similar environments.

Performance vs. Security Trade-Offs

Balancing Isolation with Speed

- Design decisions around compartmentalization, memory isolation, and privilege levels.
- Trade-offs in choosing monolithic kernel vs microkernel OS
- Trade-offs in choosing user/kernel boundaries for TAs vs. monolithic kernel TAs.
- Security isolation for TAs vs. higher communication overhead through system call boundaries.

Inter-World Communication Overhead

- Overhead from shared region polling, memory copy costs, and IPI-based signaling.
- Use of lock-free ring queues to reduce latency.
- Minimizing trap/return paths for better inter-world round-trip latency.

Scalability Limits on a Single-Core Secure OS

- Implications of limiting Secure OS execution to a single core (core 0).
- Managing multiple active TAs and long-running calls to maintain responsiveness.
- Use of concurrent threads within Secure OS vs. thread serialization.

Memory Footprint Optimizations

Static Allocation vs. Dynamic Allocation

- When and why static memory regions were used (boot sequence, early kernel sections).
- Justification for dynamic allocation fallback features (slab and page pool management).
- Minimal boot allocator and on-demand zeroing mechanisms.

Slab Allocator and Page Pool Efficiency

- Custom lightweight slab allocator optimized for isolated heaps.
- Fit-to-size classes to reduce fragmentation.

Minimal Kernel Subsystem Design

- Avoiding traditional bloated kernel designs (e.g., no sysfs, vfs).
- Core components only: task/thread scheduling, IPC, memory isolation, syscalls.
- Benefits of small Trusted Computing Base (TCB) in verification and auditability.

Debugging Considerations

Logging from Secure OS

- Secure and minimalistic logging channel
- Multiple logging levels (panic, error, info, debug).

Debugging TAs in Isolation

- tracing
- remote debugger hooks (gdb)

Instrumentation Techniques

- Internal counters for scheduling decisions, memory allocations, syscall hit counts.
- Tracing memory allocator usage (per-task page count or slab lifetime tracking).

Fault Isolation and Crash Analysis

- Handling invalid syscalls in Secure OS and malformed commands from untrusted Linux driver.
- Watchdog for runaway tasks and per-task isolation to reduce blast radius.

Build System and Packaging for TAs

Trusted Application Build Flow

- TA toolchain constraints (compiler hardening in libtacore).
- Source tree layout that enforces separation of kernel, libraries, and apps.
- Manifests for capabilities, memory regions, and initial handles.
- Options for static TA linking into kernel image vs. runtime TA loading.
- Binary format (e.g., ELF) parsing from kernel for runtime spawning.

Kernel Build System

- CMake based build system for Secure OS

Development Tooling Support

- QEMU and hardware launch wrappers (scripts for OpenSBI + Secure OS + Linux images).
- Secure OS runtime shell commands for debugging tasks and memory maps.
- Developer stubs and host-side tools for image generation, symbol resolution.

Testing and Validation

Unit Testing Secure OS Components

- Internal test cases for linked list manipulation, allocator correctness, timer behavior.
- Framework for checking invariants (vmspace protections, handle tables).
- Building unit tests into kernel image and controlled via boot parameters.

Integration Testing with Linux

- End-to-end TEE client interface validation: context creation, open session, invoke command.

Security-Oriented Tests

- Handle table fuzzing framework (e.g., reusing/releasing invalid handles).
- Fault injection infrastructure via Linux-side IPI storms, memory overwrites, syscall replay.

Summary of Implementation

Overview

- Summary of major challenges solved during implementation
- Design principles that proved effective (e.g., capability model, static memory layout).

Codebase Structure Summary

- Secure OS code structuring: split into - ta (contains trusted applications) - kernel (contains arch, lib, mem, sched, sync, tasks, tests) - libtee (contains user space library) - scripts (contains build scripts, codegeneration scripts, backtrace, etc)
- Tools and CMake-based build system granularity.

Opportunities for Improvement

- Feature hardening: memory encryption, exploit mitigations like stack canaries.
- Potential for multicore support within Secure OS given future WorldGuard changes.
- Technical debt around early bootloader glue code and MMU bring-up code.

Chapter 4: Evaluation and Security Analysis

Software Stack Setup

- This section provides a detailed description of the full software environment used to support and validate the Secure OS, focusing on emulation, build infrastructure, and integration with toolchains.
- This chapter is essential to reproduce the development setup and benchmark context.

Toolchains

- Description of RISC-V GCC or LLVM toolchain versions, secure OS and TA compilation flags, linker scripts used, and build script wrappers.

Development Environment

- Recommended dev environment setup: OS dependencies, Make/CMake/gcc versions, scripting helpers, debugging support (e.g., GDB hooks to Secure OS), and virtual machine setup, if applicable.

Emulation Environment

- A robust emulation setup using QEMU provides a virtual platform to simulate the RISC-V World Guard hardware and enables rapid development and testing.

QEMU with WorldGuard Support

- Explanation of QEMU version used and modifications or forks maintained to support the World Guard extension.

QEMU Configuration

- QEMU settings used during emulation: memory map, number of harts, device tree blob (DTB) settings, and boot arguments necessary to launch both Secure OS and Linux.
- Also covers usage of debugging options and UART output customization.

Linux

- A Secure World-aware Linux kernel build is a key part of the integration testing, providing the userland-controlled "Normal World" for Secure OS interaction.

Linux with WorldGuard Support

- Brief explanation of the version/fork of the Linux kernel used, including any upstream or out-of-tree patches to support Secure OS interaction and WorldGuard.

Linux Configuration

- Kernel config menu options (e.g., minimal init system, character device support, TEE driver integration) and explanation of chosen configurations.

Linux Image

- Process of creating the kernel image and initial RAM filesystem (initramfs); integration into QEMU boot flow and linkage with rootfs/init and Secure OS debug output collection.

Build System

- The build system is centralized and modular to build various components including the kernel, trusted applications, OpenSBI, and Linux.

CMake Configuration

- How the overall build system is managed using CMake files: compiler toolchains, cross-compilation targets, component path registration, and reusability across Secure OS kernel and TA build systems.

CMake Build System Design

- Code organization and dependency separation. Build phases: TA compilation, kernel linking, staging and image generation. Covers options or build presets (e.g., debug vs release), and the way it cooperates with toolchains and QEMU images.

Trusted Application (TA) Build Flow

- Explains how a TA is built, manifests are generated, linking to standard libraries, and embedding into final system images.

CI Integration

- Automated testing ensures regression-free development and reliable build stability.

Continuous Integration Setup

- Framework used for testing (e.g., GitHub Actions, GitLab CI, Jenkins), pipeline stages—such as QEMU boot test, TA invocation test—and artifacts generation.

Automated Testing Scripts

- Details on scripts and system outputs validated within CI. Boot success, basic syscall availability and secure/normal world boundary integrity.

Demonstration of Secure OS Functionality

- In this section, we showcase the practical use and integration of the Secure OS, including building the software stack, developing a minimal Trusted Application (TA), and demonstrating its execution using the Linux-side communication driver.

Building the Software Stack

- This subsection outlines detailed steps to build all required components for running the full software stack in a QEMU-based RISC-V emulated environment.

Cloning Project Repositories

- Steps to clone Secure OS, OpenSBI, Linux kernel, QEMU, and any required dependency sources.

Building the Cross Toolchain

- Building or fetching a RISC-V cross-compilation toolchain.
- Required versions and environment setup.

Building the WorldGuard-Enabled QEMU

- Building QEMU with required patches for WorldGuard support.
- Notes on configuration flags and validation of WorldGuard support.

Building the Patched OpenSBI

- Compilation of an OpenSBI fork with additional code to support WorldGuard boot flow.
- Integration of Secure OS handoff from M-mode.

Building a WorldGuard-Aware Linux Image

- Configuration options for enabling WorldGuard awareness in Linux.
- Applying required patches, configuring the kernel, and generating an image.

Building Secure OS

- Step-by-step instructions on configuring and compiling the Secure OS kernel.
- Overview of CMake-based build, memory layout specification, and output binaries.
- Preparing and including predefined TA manifests.

Assembling Bootable Image

- Integrating OpenSBI, Linux, and Secure OS into a QEMU-bootable image.
- Image layout overview and loading addresses.

Example Trusted Application: Simple Arithmetic TA

- Presents the practical development of a basic trusted application that offers simple arithmetic operations, to serve as a demonstrative example.

Writing a Simple Trusted Application

- Creating a minimal TA: hello world service (or similar).

Defining TA Manifest for Capability Model

- Creating a manifest describing required permissions and object handles.
- Integrating the TA in root task's manifest for launch.

Building the Trusted Application

- Using build system to compile and link the TA.
- Output format (ELF) and file placement for boot.

Demonstration and Execution

- This subsection illustrates booting full system with communication between Linux and Secure OS via the sample TA.

Booting the System

- Launching QEMU with appropriate flags and verifying CPU/world isolation.
- Boot logs highlighting OpenSBI handoff and Secure OS initialization.

Initializing the Linux Driver for Secure OS Communication

- Loading the Linux kernel module for Secure OS communication.
- Debug output validating setup of shared communication queues.

Opening a Session to Trusted Application

- Using the TEE Client API to initialize a session to the sample TA.
- Debug logs showing session creation and rendezvous with Secure OS.

Invoking the TA Function and Receiving Response

- Sending invoke command (e.g., multiplication request) from Linux-side.
- Observing execution through debug output from Secure OS and TA.
- Logging TA's output and Linux-side response resolution.

Visualizing Capability Enforcement (Optional)

- Showing an attempt to call unauthorized method or access restricted handle.
- Logging access denial via kernel enforcement logic.

Debugging and Logging Support

- Tail of secure log buffer dumped through secure syscall.
- Logging from TAs printed using standard I/O libraries.

Security Analysis

- In this section, we evaluate the security posture of the Secure OS by analyzing the resilience of its architecture to a variety of threats according to the threat model defined in Chapter 2.
- For each scenario, we describe the setup, the simulated or real attack, and the system's actual response.

- The analysis is grounded in practical testing on an emulation environment backed by software instrumentation and tracing.

Resilience against Normal World Attacks

- This subsection evaluates the Secure OS against a potentially hostile rich OS (Linux) running in the Normal World.

Unauthorized Access to Secure Memory

- Attack Setup: Linux kernel driver attempts to read/write physical page mappings belonging to Secure OS.
- Observation: Memory protection enforced with World Guard prevents access; bus errors raised correctly.

Unauthorized Access to Secure OS/TA Code

- Attack Setup: Linux attempts to scan Trusted Application code or Secure OS binary via /dev/mem or similar - - methods. Observation: Memory remains inaccessible due to hardware separation and lack of mapping in the normal world.

Attempts to Corrupt Shared Memory Queues

- Attack Setup: Malformed or oversized requests injected into shared communication pages.
- Observation: Secure OS validates request format; invalid requests rejected and logged, avoiding buffer overflows.

Exploiting CWC Protocol (Cross World Communication)

- Attack Setup: Linux attempts to race against a Secure OS processing request by overwriting in-flight messages.
- Observation: Lock-free queue only uses relative indexes in accesses, so it prevents reads and writes from unexpected pointers. So if index is corrupted (out of bounds) - it will be ignored

Resilience against Buggy Trusted Applications

- Important to ensure Secure OS protects itself even in case of flawed Trusted Applications.

Inter-TA Isolation

Attack Setup: One TA attempts to access memory or channel of another TA. Observation: Physical and logical isolation enforced; failed access due to missing capabilities; Secure OS rejects request.

Capability Enforcement Engine

Attack Setup: Malformed syscall using an invalid or forged handle; fuzzing against the Secure OS syscall interface. Observation: Consistent rejection due to absence of capability

introspection in root task's manifest.

TA Resource Misuse Protection

Attack Setup: Malicious or buggy TA requests excess memory, opens too many handles. Observation: Secure OS enforces per-task quotas; resource exhaustion attempts fail gracefully.

Side-Channel Attacks

Scenario: Timing variation attacks on Secure OS execution; cache access pattern leakage. Observation: Not possible separation due to architecture-level isolation (e.g., cores/cache).

Additional Attack Scenarios and Limitations

- This section groups attacks that are currently outside the full mitigation scope or require future hardening efforts.

Physical Attacks

Scenario: Direct DRAM probing, bus sniffer or glitching attacks on OTP or memory controller. Observation: Physical attack resistance not yet applied; relies on external platform features.

Complexity of Trusted Computing Base (TCB)

Exploration: How large and auditable is the TCB? Observation: Secure OS kernel remains minimal and auditable, but Trusted Applications contribute to overall TCB and must be vetted.

Chain of Trust Attacks

Scenario: Malicious OpenSBI image or Secure OS loader. Observation: Evaluation based on boot integrity; Secure Boot implementation assumed but not fully integrated in prototype.

Performance Evaluation

- This section evaluates the runtime behavior, efficiency, and resource usage of the Secure OS, with emphasis on inter-world communication, Trusted Application (TA) execution overhead, and system resource constraints in a constrained RISC-V environment.
- Measurements are taken on an emulated platform using WorldGuard-enabled QEMU.

Latency of Secure OS Operations

- This subsection presents a detailed breakdown of the latency involved in interaction between the Normal World (Linux) and the Secure World (Secure OS), following the GlobalPlatform API lifecycle: session open, command invocation, session close.
- Note: All latency measurements should include mean, standard deviation, and max/min values with multiple runs.

Session Open Latency

- Time required to open a session to a TA via `TEEC_OpenSession()`
- Includes context switch, message construction, capability validation, and TA instantiation
- Factors influencing latency (TA manifest size, cold start vs. warm start)

Command Invocation Latency

- Latency of `TEEC_InvokeCommand()` to a previously opened TA Session
- Breakdown of fixed syscall overhead, scheduling delay, and parameter marshalling
- Synchronous vs. asynchronous (if supported)

Session Close Latency

- Time to teardown the session and reclaim resources
- Includes cleanup of handles, session state, and Secure OS bookkeeping

Communication Performance

- Evaluation of the throughput and timing characteristics of the CWC (Cross World Communication) mechanism, emphasizing Serializable Command Queues backed by Shared Memory.

Throughput of CWC Channel

- Maximum achievable throughput of request/response cycles through shared memory queues
- Impact of message size

IPI Signaling Overhead

- Cost of using Inter-Processor Interrupt (IPI) for signaling between worlds
- Measurement of context switch delay due to IPI
- Comparison of IPI costs under load and idle scenarios

TA Context Switch Overhead

- Cost of switching between multiple TAs or restoring TA context for a scheduled operation

Kernel Entry/Exit Transition Overhead

- Benchmark the time overhead to perform Secure OS syscalls (without actual work)
- Use of synthetic minimal syscall to isolate context switch cost

Memory and Resource Footprint

- Analysis of memory usage of the Secure OS and associated components under typical workloads.

Memory Footprint of Secure OS

- Static memory usage (text/data/bss sizes)
- Dynamic memory usage at runtime (heap usage, page tables)
- Total footprint with N TAs loaded

Per-TA Resource Consumption

- Memory consumption per individual TA context
- Number of handles, stack size, VMO usage

Shared Queue Overhead

- Memory and CPU overhead of shared ring buffers for communication queues
- Lock-free implementation impact

Scalability Limits and Bottlenecks

- Maximum number of concurrently active TAs
- System behavior under memory pressure
- Fragmentation and memory management limitations

Future Work

- This chapter outlines promising directions for extending and improving the Secure OS platform for the RISC-V WorldGuard architecture. It includes technical enhancements, additional security features, hardware support expansions, and rigorous verification procedures.

Advanced TA Features

- This section discusses enhancements to the Trusted Application (TA) framework that would allow TAs to offer more sophisticated services while still retaining minimal TCB and robust isolation.

Secure Storage

- Introduce support for tamper-resistant persistent storage to enable confidential data access, including sealed key-value storage SDK for TAs.

Attestation

- Add support for both local and remote attestation with cryptographic proof of measurement and TA identity, potentially backed by a platform Root-of-Trust chain.

Root of Trust

- Define or integrate a hardware/software Root of Trust, including secure provisioning mechanisms and interaction with system boot.

Cryptographic Services

- Provide Trusted Applications with a standardized, hardware-accelerated crypto runtime offering: symmetric encryption/decryption, asymmetric crypto, hashing, digital signatures, and secure RNG.

Porting to Real RISC-V Hardware with WorldGuard

- Move from QEMU-based evaluation to physical RISC-V hardware that implements the WorldGuard extension for real-world performance measurements and evaluation under physically observable systems.
- Identify WorldGuard-compatible silicon platforms
- Implement board-specific OpenSBI and bootloader adaptations
- Hardware debugging framework integration

Performance and memory

Multicore Support for Secure World

- Extend the Secure OS runtime to allow execution on multiple cores, introducing challenges around synchronization, inter-core TA instance affinity, and capability tracking in a multithreaded environment.
- Secure world scheduling policy for multiple harts
- Shared state consistency between cores
- Scalability tuning and bottleneck analysis

Dynamic TA Loading

- Introduce support for on-demand loading and unloading of TAs to reduce secure world memory usage and enable more complex applications.
- TA cryptographic signature verification before loading
- TA manifest validation and integration with runtime capability system
- Secure memory isolation upon load/unload

Security enhancments

Formal Verification of Secure Components

- Augment Secure OS with formal verification techniques for core components, especially the kernel, capability system, and secure IPC primitives, in order to reduce the Trusted Computing Base risk and improve assurance.
- Kernel API model verification
- Memory safety guarantees via static analysis
- Proofs for capability propagation correctness

Enhanced Hardening Against Attacks

- Additional work on increasing robustness of the Secure OS and its communication mechanisms against advanced offensive threats.
- Side-channel mitigation techniques (cache partitioning, temporal fuzzing, constant-time algorithms)
- Memory fault injection resilience
- Kernel fuzzing and semi-automated stress testing
- System defenses against speculative execution and timing inference

Заключение

References

Appendices

Sample TA Code

TA Manifests

Secure OS Code

Secure Standard Library Code