KasperskyOS®

Большинство современных вычислительных систем, в том числе в составе объектов критически важной инфраструктуры, интернета вещей и межмашинного взаимодействия, имеют специфические требования к безопасности, обусловленные свойствами этих вычислительных систем и особенностями их использования.

Для выполнения этих требований в системе должны быть реализованы тщательно продуманные политики безопасности. Их строгое соблюдение играет ключевую роль в обеспечении безопасности системы. Но если вопрос только в политиках, то почему системы всё ещё небезопасны?

Операционные системы общего назначения не приспособлены для поддержки тонких настроек политик безопасности каждого критичного приложения. А система специального назначения способна обеспечить применение политик с определёнными гарантиями.

На рынке наблюдается дефицит продуктов, которые могут поддерживать применение различных политик безопасности в защищаемых системах. KasperskyOS позволяет восполнить этот пробел, предоставляя высоконадёжную безопасную платформу, способную обеспечить применение любых назначенных политик для критичных приложений.

KasperskyOS создает среду, в которой уязвимости и ошибки кода больше не представляют угрозы. Защитный компонент Kaspersky Security System (KSS) контролирует взаимодействие между всеми частями системы, делая эксплуатацию уязвимостей бесполезной для злоумышленников.

Цели

Цель KasperskyOS – обеспечить защиту программных и информационных систем от вредоносного кода, вирусов и хакерских атак. Эти угрозы могут привести к потере или утечке конфиденциальных данных, снижению производительности или отказу в обслуживании. Кроме того, KasperskyOS снижает риски, связанные с ошибками в программах, а также со случайными или преднамеренными повреждающими действиями.

Особенности

µ-ядро. Минимальный объем кода, достаточный для работы механизмов ядра, позволяет обеспечить более строгий контроль качества кода ОС.

Гарантированная изоляция. Система гарантирует изоляцию доменов безопасности и отделение свойств безопасности от функциональных компонентов.

Унифицированный механизм межпроцессного взаимодействия (IPC). Микроядро обеспечивает наличие единого механизма IPC.

Строго определенные типизированные интерфейсы. Для каждого приложения или драйвера должны быть статически определены интерфейсы взаимодействия. KSS проверяет корректность всех IPC сообщений в соответствии с этими определениями интерфейсов.

Наше решение позволяет сделать систему безопасной, не снижая при этом её надёжность.

Статическая настройка безопасности. Все процессы и доступные для них типы взаимодействий заранее настроены и выверены до начала работы системы.

Полное посредничество. Все межпроцессные взаимодействия проходят через микроядро, которое проверяет их с помощью Kaspersky Security System (KSS). KSS вычисляет вердикт о возможности доступа, руководствуясь настройками безопасности.

Отказ по умолчанию. Любое действие, не предусмотренное политиками безопасности, запрещено по умолчанию.

Драйверы пользовательского пространства. Драйверы, ядра и приложения изолированы друг от друга; драйверы запускаются как непривилегированный код, и ошибка в одном драйвере не оказывает негативного влияния на систему в целом. Также есть возможность ограничить доступ драйвера к физическому устройству.

Kaspersky Security System

Одним из наиболее важных компонентов KasperskyOS является Kaspersky Security System (KSS). Это движок, выполняющий вычисление вердиктов политик безопасности, который может работать одновременно с различными типами таких политик (ролевой и мандатный контроль доступа, контроль потоков управления, политики доменов и типов, политики на основе темпоральных логик и пр.). KSS может быть настроен в соответствии с конкретными требованиями заказчика. Чем более детализированы политики, тем выше уровень контроля и безопасности всей системы.

Kaspersky Security System основан на принципе изоляции безопасных компонентов от функциональных в рамках одной информационной системы. Такой подход гарантирует безопасную работу системы независимо от того, каким образом реализованы функциональные компоненты, и позволяет создавать доверенные системы с использованием недоверенных компонентов. В результате политики безопасности могут быть изменены без внесения каких-либо изменений в функциональные компоненты. KSS – это больше, чем защита от зловредов: он также предотвращает нарушение правил безопасности.

Технические требования

Требования к CPU:
- Memory Management Unit (MMU);
- IOMMU (SDMA для ARM) настоятельно рекомендуется для надежной изоляции аппаратных ресурсов.

Поддерживаемая архитектура:
x86, x86_64, ARMv5, ARMv7, ARMv8 и MIPS32.

Протестированные аппаратные платформы:
Intel Generic и Atom CPUs, NXP i.MX6 (Solo, Duo и Quad), NXP i.MX27, TI Sitara AM335x, TI Sitara AM43xx, HiSilicon Kirin620, MIPS24k.

Минимальный объём RAM зависит от решения. Рекомендуемый объём RAM 128 Мб.

Применение

- Корпоративные информационные системы
- Компьютерные системы специального назначения
- Интернет вещей
- Интеллектуальные энергосистемы
- Промышленные системы
- Телекоммуникационное оборудование
- Транспортные системы
- Объекты критически важной инфраструктуры

Патенты

US 7386885 B1, US 7730535 B1, US 8370918 B1, EP 2575318 A1, US 8522008 B2, US 20130333018 A1, US 8381282 B1, EP 2575317 A1, US 8370922 B1, EP 2575319 A1, US 9015797 B1, DE 202014104595 U1.

Преимущества

Проприетарное микроядро и независимый движок, обеспечивающий безопасность

В основе KasperskyOS лежит надёжное микроядро, которое допускает только определённый способ взаимодействий. Будучи компактным, оно может использоваться на различных платформах. В то же время, безопасный движок, будучи слабосвязанным, позволяет заменить проприетарное ядро другим, если это необходимо.

Многоуровневая совместимость

Поскольку система по большей части POSIX-совместима, использование нативного API даёт гарантию того, что поведение приложений будет безопасным. Разработчик может самостоятельно выбрать, как сохранить баланс между совместимостью программного кода и его безопасностью.

Обязательная идентификация и маркировка

Все приложения KasperskyOS имеют свою безопасную конфигурацию, без которой установить их невозможно. Аппаратное обеспечение и ресурсы уровня приложений (файлы, базы данных, сетевые порты и пр.) маркируются соответствующими атрибутами безопасности. Получить доступ к ресурсу, не имеющему метки безопасности, также невозможно.

Модульная архитектура

Модульный подход к архитектуре системы минимизирует размер доверенной кодовой базы и позволяет построить каждое отдельное решение на индивидуальной основе.

Безопасная архитектура приложений

Архитектура приложений основана на компонентной модели, благодаря чему разработка решения становится проще и удобнее.

Легко настраиваемые политики

Простой язык настройки позволяет легко задавать правила межпроцессного взаимодействия и контроля доступа.

Возможность проверки

Строгое соблюдение принципов безопасности при проектировании и внедрении системы позволяет верифицировать безопасность всех решений на базе KasperskyOS.

Изначально безопасная система

KasperskyOS была задумана и создана как безопасная. Она остается безопасной в течение всего своего жизненного цикла.

Экспертиза

- Определение целей безопасности и составление требований к безопасности
- Описание сценариев возможных неправильных/неправомерных действий и их последствий
- Построение моделей угроз
- Описание архитектуры системы со встроенными средствами защиты
- Тестирование на проникновение

Безопасные сервисы

- Безопасный Аудит
- Безопасная Загрузка
- Безопасное Обновление
- Безопасное Хранилище
- Безопасный Журнал
- Доверенный канал

Технологии безопасности

- Защита от вредоносных программ
- Белые списки
- Машинное обучение
- Система обнаружения/предотвращения вторжений
- DNS-фильтрация
- Соединение с KSN

Базовые технологии

- KasperskyOS
- Kaspersky Security System for Linux
- Kaspersky Secure Hypervisior

www.kaspersky.ru

АО «Лаборатория Касперского», Россия, Москва www.kaspersky.ru
Аналитика и отчеты о киберугрозах от экспертов «Лаборатории Касперского»:
www.securelist.ru
KasperskyOS®: os.kaspersky.ru

#kasperskyos
#truecybersecurity