kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Secure Hypervisor: безопасность без компромиссов

Kaspersky Secure Hypervisor

В современном мире профессиональные злоумышленники и целевые кибератаки стали повседневной реальностью. Поэтому, когда дело доходит до выбора и оценки встраиваемых систем, безопасность является ключевым фактором, который необходимо принимать во внимание.

Угрозы бывают разными: от атак на уязвимые интерфейсы до использования недокументированного или агрессивного поведения периферийного оборудования, такого как PCI и USB. После успешной атаки злоумышленник может пойти дальше, например, используя уязвимости операционной системы, создать потенциальную угрозу для критических процессов, которыми она управляет. Несмотря на уязвимости и обширную поверхность атаки у большинства популярных платформ, разработчики предпочитают использовать именно их из-за широкой распространенности и доступности программного обеспечения.

Технология виртуализации дает возможность существенно усилить системную безопасность, сохраняя при этом возможность использовать существующее программное обеспечение без каких-либо модификаций.

Общая информация

Kaspersky Secure Hypervisor (KSH) – это гипервизор второго типа, который работает поверх KasperskyOS и использует её механизмы безопасности. KSH предоставляет возможность запуска нескольких виртуальных машин (гостевых операционных систем) на одной физической машине, распределяя физические ресурсы между ними.

Основное преимущество использования виртуализации состоит в отделении потенциально ненадёжных гостевых операционных систем друг от друга и от критических сервисов, размещённых на той же физической машине. Это позволяет сократить поверхность атаки и свести к минимуму возможные последствия эксплуатации уязвимостей. Гипервизор защищен от гостевой ОС таким образом, что её вредоносные действия не могут причинить вред критическим службам или самому гипервизору.

Цели

- Повышение безопасности за счёт предоставления дополнительных гарантий безопасности во время запуска привычного рабочего окружения.
- Сокращение расходов благодаря использованию единой аппаратной платформы для нескольких гарантированно отделённых друг от друга гостевых систем.

Особенности

Компоненты KSH

Безопасный гипервизор работает поверх KasperskyOS и включает два компонента:

1. Приложение – менеджер виртуальной машины (Virtual Machine Manager – VMM), работающий в пользовательском режиме

Менеджер виртуальной машины отвечает за управление памятью, временем исполнения, работу с оборудованием, включая реальные физические и эмулируемые устройства, а также предоставляет механизмы взаимодействия виртуальной машины с сервисами KasperskyOS и другими виртуальными машинами.

2. Модуль микроядра

Модуль микроядра реализует минимально необходимый функционал, требующий доступа к привилегированным функциям процессора; при этом вся остальная обработка осуществляется в пользовательском режиме.

Средствами KasperskyOS решаются две основные задачи:

- Надежная изоляция виртуальных машин друг от друга и от сервисов KasperskyOS
- Контроль взаимодействий виртуальных машин с другими компонентами решения с использованием заданного для решения набора политик безопасности

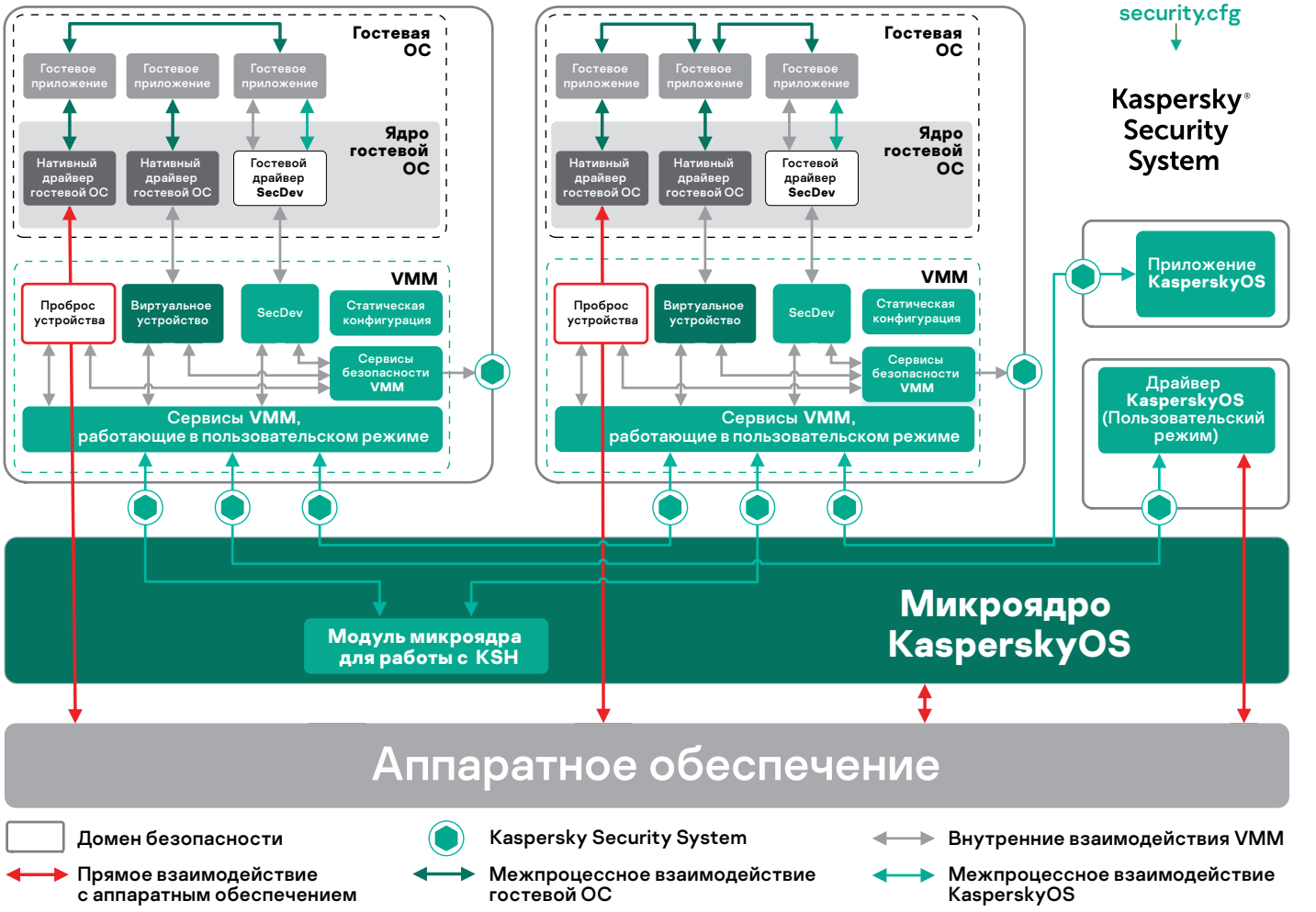
Средствами менеджера виртуальной машины осуществляется управление доступом к памяти, аппаратуре, авторизация выполняемых гостевой ОС действий и работа эмулируемых устройств в соответствии с заданными политиками безопасности.

Kaspersky Security System

Совместно с микроядром KasperskyOS работает специализированная подсистема Kaspersky Security System, которая вычисляет вердикты безопасности, определяющие возможность или невозможность той или иной операции. При вычислении вердиктов безопасности используется заданная для решения конфигурация безопасности, описанная на специально разработанном языке высокого уровня в терминах строгих и хорошо изученных математических моделей. В отличие от большинства других аналогичных систем, Kaspersky Security System дает возможность использовать большое количество формальных моделей одновременно, включая модель безопасности на базе мандатных ссылок, модель ролевого доступа, модели на базе конечных автоматов, различные диалекты темпоральной логики и др. Также есть возможность добавления новых моделей безопасности.

В решениях на базе KasperskyOS Kaspersky Security System является единственной точкой принятия решений безопасности, при этом вычисленные вердикты могут использоваться другими компонентами решения, в частности KasperskyOS и менеджером виртуальных машин. Такой подход позволяет максимально точно и подробно описать свойства безопасности решения, требуемые в каждом отдельном случае, исходя из конкретной модели угроз.

В рамках данного подхода гостевые ОС рассматриваются как недоверенные компоненты решения. Даже если гостевая ОС предпримет попытку атаки, такая атака будет обнаружена и заблокирована. При этом есть возможность предпринять необходимые действия по восстановлению нормального функционирования системы в целом.



Взаимодействие виртуальной машины с внешними компонентами

Как и любое другое приложение KasperskyOS, гостевая операционная система может формировать и получать IPC-сообщения и полноценно участвовать в работе системы наряду с другими её компонентами – под контролем базовых механизмов безопасности KasperskyOS.

Важной особенностью KSH является возможность осуществлять прозрачное и защищённое взаимодействие сервисов гостевой операционной системы с другими компонентами решения – как другими виртуальными машинами, так и приложениями и сервисами самой KasperskyOS.

Работа данного механизма основана на принципах межпроцессного взаимодействия KasperskyOS, реализующих модель типизированного Rendezvous IPC. В процессе обмена участвующие в нем агенты формируют сообщения, формат которых полностью описывает все особенности проводимой операции, после чего микроядро KasperskyOS обеспечивает доставку этих сообщений. В процессе доставки выполняется проверка возможности осуществления проводимой операции с использованием Kaspersky Security System. В случае положительного вердикта KSS сообщение доставляется, а в случае отрицательного передача блокируется и могут быть предприняты шаги по восстановлению штатной работы системы.

Чтобы осуществлять описанное взаимодействие, на уровне менеджера виртуальной машины KSH реализуется виртуальное устройство SecDev (Secure Device), которое предоставляет транспорт для проведения IPC.

Таким образом, драйвер устройства SecDev в гостевой ОС даёт возможность прозрачно и безопасно работать с внешними по отношению к ней компонентами. В настоящее время драйверы устройства SecDev разработаны для всех гостевых операционных систем, работа с которыми поддерживается KSH.

Работа с аппаратурой

Безопасный гипервизор использует в работе аппаратные технологии виртуализации Intel VT-x и VT-d. Использование VT-d не является обязательным (гипервизор может работать и без неё), но рекомендуется, поскольку без VT-d невозможно гарантировать изоляцию решений, использующих в своей работе функции DMA.

В работе с аппаратурой задействованы 2 механизма – проброс физических устройств и эмуляция. Каждый из подходов имеет свои преимущества и недостатки, поэтому в реальных решениях используется комбинированный подход, когда часть устройств эмулируется, а часть пробрасывается.

При пробросе устройств виртуальная машина получает непосредственный доступ к физическим аппаратным ресурсам устройства и полностью контролирует его работу своими средствами. В этом случае практически отсутствуют накладные расходы, связанные с работой устройства в виртуальном окружении, для устройства не требуется драйвер в KasperskyOS, но оно монопольно захватывается виртуальной машиной, так что его становится невозможно использовать из других виртуальных машин и прочих компонентов решения.

Подход, связанный с эмуляцией устройств, более гибкий. В этом случае для виртуальной машины средствами менеджера виртуальной машины эмулируется аппаратный интерфейс. Он в точности соответствует интерфейсу реальной аппаратуры, но фактически функциональность реализуется в программном компоненте, который перехватывает обращения к аппаратуре и обрабатывает их. В случае эмуляции есть возможность реализовать множество полезных как с точки зрения функциональности (например, разделение доступа, реализация полностью виртуальных устройств), так и с точки зрения безопасности (анализ и фильтрация данных, шифрование и т.д.) сценариев работы, но обычно платой за это является существенное в сравнении с реальной аппаратурой снижение производительности.

Поставка в форме SDK

Еще одной особенностью KSH является механизм его поставки и развертывания. KSH в первую очередь предназначен для использования во встраиваемых системах, к которым предъявляются повышенные требования информационной безопасности.

Накопленный «Лабораторией Касперского» опыт показывает, что не существует универсальной модели безопасности на все случаи жизни. Напротив, требования безопасности всегда вытекают из модели угроз, которая является уникальной для каждого конкретного случая. С другой стороны, встраиваемые системы, как правило, имеют ограниченные ресурсы памяти и производительности, что также приводит к нецелесообразности использования универсальных дистрибутивов. Учитывая это, «Лаборатория Касперского» поставляет KSH в виде SDK, дающего широкие возможности конфигурирования как состава и свойств функциональных модулей, задействованных в решении, так и требуемых от него (в соответствии с моделью угроз) свойств безопасности. В результате у заказчика появляется возможность получить именно то решение, которое ему необходимо.

Применение
- Интернет вещей
- Автомобильная промышленность
- Здравоохранение
- Промышленная автоматизация
- Кассовые терминалы
- Тонкие клиенты и VDI
- Корпоративные ноутбуки, планшеты и смартфоны

Сценарии использования

Бортовая информационно-развлекательная система (In-Vehicle Infotainment)

Для такого решения в гипервизоре может быть использовано два домена: один безопасный — для критически важного программного обеспечения (управление транспортным средством, функции, требующие сертификации по ISO 26262), а другой общего назначения – для информационно-развлекательного программного обеспечения (развлекательная система, связь с внешним миром, голосовые функции, пользовательский интерфейс). При этом средствами гипервизора исключается влияние домена общего назначения на безопасный домен.

Отдельные виртуальные среды обеспечивают стабильность критически важного программного обеспечения независимо от того, какое действие выполняет пользователь. С помощью технологии эмуляции устройств общие аппаратные средства (например, сетевая карта, модули GSM или Wi-Fi) могут использоваться доменами, что снижает затраты на оборудование. Путем проброса устройства, например, контроллера графики в домен общего назначения, появляется возможность реализации современного графического интерфейса для пользователя без потерь производительности. При использовании нативных сервисов KasperskyOS появляется возможность реализации различных сервисов безопасности для гостевой ОС, таких как Trusted Execution Environment, безопасное обновление ПО и др.

Системы промышленной автоматизации (АСУ ТП)

В этом решении для разделения промышленного программного обеспечения, программного обеспечения связи, баз данных и пользовательских интерфейсов используются два и более доменов.

Мы рекомендуем применять KSH для обеспечения безопасности систем SCADA. Использование решений на базе гипервизора позволяет решить ряд проблем кибербезопасности без изменения или обновления программного обеспечения SCADA. Возможны несколько сценариев обеспечения безопасности с KSH.

1. Контроль периферии	KSH обеспечивает полную изоляцию гостевых операционных систем, что даёт возможность предоставлять или не предоставлять доступ к периферийным устройствам. Использование KSH позволяет обеспечить выполнение таких сценариев, как деактивация неиспользуемых устройств, контроль доступа в соответствии с заданными политиками безопасности, авторизация доступа к устройствам и др.
2. Безопасное обновление	Возможность обновления ПО – важное требование для современных решений. Однако реализация безопасной процедуры обновления ПО является чрезвычайно сложной задачей. По статистике, часть вирусного ПО попадает в систему именно во время ее обновления. Известно множество примеров, когда злоумышленники использовали функции обновления программного обеспечения для проведения кибератак. Средствами KSH можно обеспечить сохранность системы и её поддержку в актуальном состоянии. Для контроля процесса обновления используется независимый механизм, который верифицирует целостность и аутентичность обновления. При этом поведение системы находится под постоянным контролем, поэтому даже если обновление получено из доверенного источника, но содержит вредоносные компоненты, попытка атаки будет немедленно обнаружена и заблокирована.
3. Доверенная аутентификация	Гостевые ОС сложны и часто содержат уязвимости, поэтому их системы аутентификации нельзя считать надёжными. Так как KSH работает в доверенном окружении KasperskyOS, есть возможность обеспечить дополнительные надёжные механизмы аутентификации пользователей таким образом, чтобы при попытке аутентификации в гостевой системе пользователь не мог обойти защиту на уровне KSH.
4. Безопасная загрузка	KSH поддерживает механизм безопасной загрузки гостевой ОС, который включает набор процедур верификации, основанных на механизмах аппаратной защиты. Безопасная загрузка обеспечивает целостность и аутентичность образа ОС (ядра ОС и файловых систем) и его загрузчиков, а также гарантирует, что в случае повреждения или модификации гостевая ОС не будет загружена.

5. Безопасный аудит	Один из существенных аспектов информационной безопасности связан с аудитом. Порча или подмена записей в журнале событий аудита безопасности является распространенной практикой, применяемой с целью сокрытия неправомерных действий, совершенных операторами систем, и вредоносных действий, произведенных в ходе кибератак. Использование KSH позволяет обеспечить надежную защиту записей журнала событий гостевой ОС. С помощью SecDev реализуется независимый канал для сбора данных аудита гостевой операционной системы и передачи их в KasperskyOS. Получив эти данные, KasperskyOS сохраняет их таким образом, что никаким средствами гостевой ОС невозможно произвести их модификацию.
6. Защита распределённых систем	Распределённые системы SCADA могут быть весьма сложными, иметь неоднородную структуру и, в частности, содержать большое количество устаревших компонентов, использующих старые и уязвимые протоколы информационного обмена. Исправить такую ситуацию очень тяжело, поскольку модернизация подобных систем является сложной, затратной, а часто просто нерешаемой задачей. Однако с использованием гипервизора эта задача может быть решена. Средствами KSH можно организовать прозрачный доверенный сетевой канал для информационного обмена в рамках распределённой SCADA без каких-либо модификаций имеющегося программного обеспечения. KSH создаёт эмулируемое сетевое устройство, ответная часть которого, работающая на уровне KasperskyOS, осуществляет шифрование данных с использованием самых современных алгоритмов и подходов. В результате организуется защищённая сеть, в которой невозможно перехватить или подменить какие-либо данные.
7. Дополнительная доверенная гостевая ОС	В силу того, что полнофункциональные операционные системы имеют множество проблем, связанных с безопасностью, использование средств защиты, работающих в контексте таких операционных систем, нельзя считать надёжным. Например, наличие в ядре операционной системы уязвимости, допускающей выполнение произвольного кода в привилегированном режиме процессора (а такие уязвимости находятся достаточно часто), позволяет злоумышленникам преодолеть любые программные средства защиты. Стоит отметить, что эти средства защиты, а также критичные с точки зрения безопасности сервисы – криптографические протоколы, DPI (глубокая проверка пакетов), средства администрирования и т.д. – могут быть настолько сложными, что их адаптация для KasperskyOS будет нецелесообразна. Избежать доработок позволяет использование отдельной изолированной гостевой системы, в которую можно перенести сервисы безопасности без каких-либо модификаций. В результате общая безопасность решения существенно возрастает, поскольку полнофункциональная ОС не может неконтролируемым образом влиять на работу сервисов в изолированной гостевой ОС.
8. Доступ на основе ролей и полномочий	Многие операционные системы общего назначения реализуют свои сервисы безопасности на основе ролевого доступа, которые не могут считаться надёжными, поскольку сами ОС не являются доверенными. Однако безопасность подобных решений можно существенно повысить путём вынесения точки принятия решений безопасности за пределы виртуальной машины, что может быть сделано с использованием KSH. Стоит отметить, что Kaspersky Security System и KasperskyOS поддерживают стандартные модели ролевого доступа.
9. Авторизация действий гостевой ОС	KSH позволяет контролировать поведение приложений гостевой ОС. При соблюдении ряда условий можно рассматривать гостевую ОС как достаточно доверенную для работы SCADA, что, тем не менее, не исключает ошибок оператора, а также ошибок в ПО самой SCADA или в загружаемых в SCADA сценариях работы. Безопасность такого решения может быть усилена за счет добавления дополнительных механизмов авторизации, реализованных с использованием KSH на базе стандартных политик безопасности KasperskyOS. В этом случае для выполнения действий, описанных в конфигурации безопасности решения, Kaspersky Security System вычисляет вердикт и таким образом авторизует или не авторизует проводимую операцию. Если для выполнения операции требуется подтвердить полномочия оператора независимым образом, потребовав его дополнительную аутентификацию, это также может быть сделано.
10. Безопасная среда исполнения (TEE)	Средствами KSH также можно обеспечить безопасную среду исполнения (TEE – Trusted Execution Environment) для гостевых ОС: часть функций (криптография, хранение критически важной информации, функции администрирования и т.д.) может быть вынесена за рамки гостевой ОС в реализованное средствами KasperskyOS безопасное окружение. Таким образом исключается нежелательное влияние гостевой ОС на TEE.

11. Контроль ресурсов	KSH позволяет обеспечить контроль доступа гостевых ОС к ресурсам (память, периферийные устройства).
12. Мониторинг состояния	Средствами KSH можно обеспечить независимый мониторинг состояния гостевой ОС: сбор статистики по использованию памяти и процессора, детектирование зависаний и нехватки ресурсов, подсчет и анализ сетевого трафика и др.

Технические требования

Платформы
Intel x86 или x64 с поддержкой технологий VT-x и (опционально) VT-d. Поддержка VT-d настоятельно рекомендуется. 64-битные гостевые системы могут работать только на x64 CPU. В настоящее время ведутся работы по поддержке архитектуры ARM (v7, v8).

Объём оперативной памяти
Объём оперативной памяти, необходимый для работы KSH, зависит от его конфигурации, количества и типа виртуализированных устройств и многих других параметров. Рекомендуемый объём оперативной памяти для KSH составляет 32 Мб для каждого экземпляра Менеджера виртуальной машины и дополнительно 32 Кб за каждый Мб гостевой оперативной памяти на каждой виртуальной машине. При расчёте требований к объему оперативной памяти для решения в целом необходимо также учитывать потребности KasperskyOS.

Дисковое пространство
KSH требует 8 Мб дискового пространства для каждой виртуальной машины. При расчёте требований к решению в целом также следует учитывать требования KasperskyOS, размеры образов гостевых ОС и размеры файловых систем гостевых ОС.

Гостевые операционные системы
В качестве гостевых ОС могут использоваться немодифицированные дистрибутивы на базе ядра Linux, такие как Ubuntu, Fedora и CentOS, а также Windows (XP, Windows7, Windows8, Windows 10) и KasperskyOS.

Эмулируемые устройства
- SATA контроллер
- IDE контроллер
- VGA контроллер
- NE2000 сетевой контроллер
- RTL8139 сетевой контроллер
- Программируемый контроллер прерываний (PIC)
- Расширенный программируемый контроллер прерываний (APIC)
- Шина PCI
- Часы реального времени
- Программируемый интервальный таймер (PIT)
- Контроллер UART 16550A
- PS/2 с поддержкой клавиатуры и мыши

Протестированные пробрасываемые устройства
- EHCI, xHCI USB контроллеры
- SATA контроллер
- PCI Ethernet контроллеры
- Radeon/nVIDIA видеокарты
- IDE контроллер

Мобильные устройства

Гипервизорное решение может содержать отдельные домены или профили для разделения (1) корпоративных данных и критически важных приложений (например, пакета системы обеспечения доступа к интернету, VPN, служб безопасности, хранилища для сертификатов и кредитных карт) и (2) персональных данных.

Безопасное хранилище для сертификатов и ключей

В этом решении службы хранения и шифрования сертификатов хранятся в отдельном доверенном домене. Приложения гостевой ОС запускаются в другом домене и получают доступ к службам шифрования через каналы связи Kaspersky Secure Hypervisor (через устройство SecDev). Доверенные компоненты могут предоставлять дополнительные привилегированные права доступа для приложений гостевой ОС (например, доступ к административным службам) после прохождения ими авторизации. Даже если приложения гостевой ОС подверглись атаке, они не смогут получить доступ к ключам или повысить уровень своих привилегий из-за действующих политик безопасности и разделения доменов, которые гарантированы KasperskyOS.

Мониторинг и фильтрация сетевого трафика

При необходимости для всех сетевых взаимодействий между приложениями гостевой ОС и внешним миром средствами KSH реализуется возможность мониторинга и анализа передаваемых данных – прозрачно и незаметно для приложений гостевой ОС. Также может осуществляться фильтрация, перенаправление или модификация сетевых пакетов в соответствии с задачами безопасности, реализуемыми решением. Поскольку данные средства безопасности реализуются независимо на уровне KasperskyOS, гостевые сервисы ни при каких обстоятельствах не смогут их обойти.

Защита данных гостевой ОС

Kaspersky Secure Hypervisor позволяет защитить данные гостевой ОС от модификаций и неавторизованного доступа посредством механизма защиты памяти. К защищаемым данным в общем случае могут относиться бинарный код ядра ОС или его загружаемых модулей, код сервисов безопасности, страницы памяти, в которых хранятся настройки гостевой ОС, и другие критически важные данные. Защита памяти достигается за счёт установки соответствующих прав доступа (чтение/запись/исполнение) на физические страницы ОЗУ, с которыми работает гостевая ОС. При загрузке гостевая ОС может считаться доверенной, что обеспечивается средствами доверенной загрузки. На этом этапе гостевая ОС передает гипервизору информацию о конфигурации физических страниц своей памяти, требующих защиты. Затем с определённого момента (например, когда у виртуальной машины появляется внешний канал передачи данных) гостевая ОС рассматривается как недоверенная. При этом выполнение заданных на этапе загрузки свойств безопасности гарантируется гипервизором на протяжении всей работы системы. Решение о возможности/невозможности доступа в этом случае принимается KSS, что позволяет задавать чрезвычайно гибкие политики доступа к защищаемой памяти.

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 решение. Kaspersky Secure Hypervisor – это проприетарное решение, полностью поддерживаемое «Лабораторией Касперского». Процесс разработки основан на лучших отраслевых практиках с применением систематического тестирования и верификации.

Надёжная изоляция и контролируемые взаимодействия. Для изоляции виртуальных машин используются стандартные механизмы KasperskyOS, включая MMU и ASLR. Дополнительно для изоляции компонентов при доступе к аппаратуре с использованием DMA применяется технология VT-d, в частности механизм IOMMU. При этом каждая виртуальная машина помещается в отдельный изолированный домен.

Все взаимодействия между доменами, а также между доменом и микроядром KasperskyOS контролируются KSS в соответствии с заданными политиками безопасности. Если злоумышленник предпримет попытку атаки на виртуальную машину, его действия будут обнаружены и заблокированы.

Гибкий контроль доступа. Kaspersky Security System поддерживает широкий набор формальных моделей безопасности (мандатные и ролевые модели; модели на базе объектных ссылок; использующие конечные автоматы; основанные на различных диалектах темпоральных логик и др.). При необходимости легко могут быть добавлены новые модели. В результате появляется возможность задавать чрезвычайно точные и подробные политики безопасности, специфичные для каждого решения в зависимости от области его применения и разработанной для него модели угроз.

Статическая конфигурация для ресурсов гостевых ОС. Kaspersky Secure Hypervisor ограничивает использование ресурсов (таких, как память или доступ к физическим устройствам) гостевыми ОС. Это позволяет защитить рабочее окружение от возможной нехватки ресурсов в результате их чрезмерного использования гостевыми ОС и исключить доступ последних к потенциально опасным внешним устройствам. При этом конфигурация гипервизора не может быть изменена в процессе работы, что гарантирует невозможность проведения соответствующих атак.

Возможность интеграции с системой безопасной загрузки. Kaspersky Secure Hypervisor включает функции, гарантирующие целостность самого гипервизора и гостевых ОС.

Минимальный размер доверенной вычислительной базы. Доверенная вычислительная база – это набор всех компонентов (аппаратное обеспечение, прошивка и программное обеспечение), критичных для общей безопасности всего решения в целом.

Микроядерная архитектура KasperskyOS в совокупности с Kaspersky Security System позволяет ограничить размер доверенной вычислительной базы решения, исключив из неё функциональные компоненты, к которым не предъявляются требования информационной безопасности. Минимальный состав доверенной вычислительной базы для решений с использованием KasperskyOS включает код микроядра KasperskyOS и часть кода Kaspersky Security System, отвечающую за реализацию используемых в решении моделей безопасности. Стоит отметить, что программный код, отвечающий за привязку конкретного решения к имеющимся моделям безопасности, является генерируемым. Описание, на базе которого генерируется этот код, задаётся на специально разработанном языке высокого уровня, что позволяет проводить формальную верификацию генерируемого кода.

При использовании KSH в большинстве практически значимых сценариев код менеджера виртуальной машины может рассматриваться как недоверенный, и тогда размер доверенной вычислительной базы увеличивается лишь за счёт модуля микроядра KSH, размер которого в настоящее время составляет всего 8000 строк кода. В тех же случаях, когда менеджер виртуальной машины сам выполняет те или иные функции безопасности, например, обеспечивает защиту страниц гостевой памяти или контроль использования периферийных устройств, следует принимать в расчёт кодовую базу самого менеджера виртуальной машины, составляющую 13000 строк кода, а также код, используемый для эмуляции устройств. Объём последнего варьируется в зависимости от набора эмулируемой периферии, и в худшем случае составляет 27000 строк кода. Таким образом, KSH является достаточно компактным решением. Малый размер кодовой базы KSH позволяет добиться гарантированно высокого качества кода и даёт возможность его тщательного исследования в процессе проведения сертификационных процедур.

Эффективная разработка и повторное использование кода. Системы общего назначения и приложения для этих систем могут использоваться KSH без снижения уровня защищённости решения в целом, благодаря разделению функциональности решения на логические блоки (домены) и помещению системы с приложениями в отдельный домен с определённым уровнем доверия.

Контроль на низком уровне. Приложения и целые операционные системы контролируются на уровне гипервизора, что делает невозможным обход или взлом защиты с их стороны. Использование недокументированных возможностей (закладок) оборудования также невозможно, если только гостевой системе гипервизором не предоставлен прямой доступ к этому оборудованию. Доступ к прочим ресурсам при этом ограничивается с помощью аппаратных средств VT-d. Это позволяет свести потенциальные риски использования недоверенных устройств к ущербу только для тех виртуальных машин, которым явно разрешена работа с ними.

KasperskyOS®

Подробнее на os.kaspersky.ru

www.kaspersky.ru