Kaspersky® Security System for Linux

Операционные системы на базе ядра Linux широко используются во встраиваемых системах. Их можно найти в бытовой технике, информационно-развлекательных системах автомобилей, беспроводных маршрутизаторах, системах промышленной автоматизации, бортовом ПО космических аппаратов, медицинском оборудовании и даже в смартфонах и планшетах.

На рынке представлены десятки поставщиков, предлагающих специализированные версии Linux для встраиваемых устройств. В то же время существующие модули безопасности, такие как SELinux или AppArmor, обычно используются в системах общего назначения и не всегда приспособлены для встраиваемых решений. Этому способствуют следующие факторы:

- их сложно настраивать;
- они не вполне соответствуют специфическим требованиям и задачам встраиваемых систем;
- они недостаточно гибкие для моделируемых систем.

«Лаборатория Касперского» предлагает метод, средства и набор практик, которые позволяют повторно использовать уже имеющиеся компоненты программного обеспечения для создания безопасных встроенных решений, отвечающих самым различным требованиям.

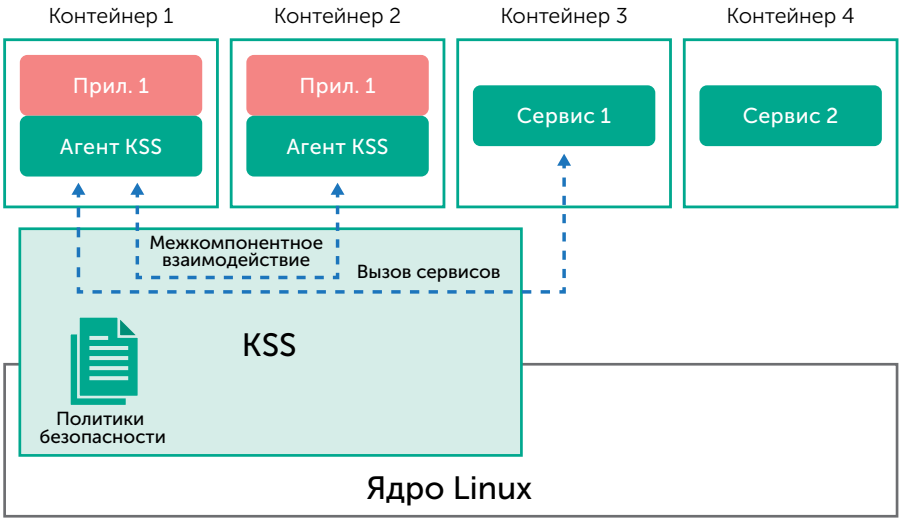
Как правило, встроенные системы имеют заранее известные функции и относительно короткий список свойств безопасности, которые формулируются в терминах, специфичных для области применения, например «любое сообщение приложения X с датчиком Y должно быть запрещено до тех пор, пока сервис Z не будет полностью инициализирован».

Тем не менее, расширения безопасности, такие как SELinux, построены вокруг концепции UNIX, поэтому разработчик должен самостоятельно переформулировать свойства безопасности бизнес-домена в стандартные понятия и средства используемого расширения.

В случае встроенных систем это особенно неприятно, поскольку вызывает два типа проблем:

1. Формулирование целей безопасности часто является нетривиальной задачей, которая приводит к излишне сложным конфигурациям.
2. Иногда разработчики не хотят этим заниматься и строят политики безопасности непосредственно в своих бизнес-приложениях.

Первая проблема затрудняет обзор и сохранение конфигураций безопасности. Однако второй тип проблем намного серьезнее, поскольку нарушает принцип отделения функционала системы от механизмов безопасности. В результате при разработке функциональных возможностей разработчики могут игнорировать или забывать связанные с безопасностью аспекты кода. Несоответствия безопасности и функциональности могут позволить злоумышленникам взять систему под контроль, используя незначительную уязвимость в коде. В этой ситуации специальный компонент для мониторинга безопасности, который реагирует на каждое изменение функциональности, делает всю систему более надежной.



Применение

Kaspersky Security System, интегрированный с Linux, используется как основа для:

- Встраиваемых промышленных решений (ПЛК, удалённые терминалы, операторские панели)
- Устройств интернета вещей
- Телекоммуникационного оборудования

Большинство встроенных систем имеют схожие требования в отношении их обслуживания и поддержки, такие как регулярное обновление программного обеспечения, удаленная настройка или возможность установки стороннего ПО. Это приводит к созданию с нуля решений, которые копируют уже существующие решения. При этом в ход идут любые доступные средства: от низкоуровневых библиотек до готовых решений, предоставляемых ненадежными разработчиками.

Хотя данный подход, как правило, повышает скорость вывода решения на рынок, он отрицательно сказывается как на качестве конечного продукта, так и на его кибербезопасности. «Лаборатория Касперского» предлагает метод, средства и набор практик, которые позволяют повторно использовать уже имеющиеся компоненты программного обеспечения для создания безопасных встроенных решений, отвечающих самым различным требованиям.

Цели

«Лаборатория Касперского» предлагает метод, средства и набор практик для настройки существующих программных компонентов таким образом, чтобы получить защищённое встраиваемое решение. KSS for Linux:

- предоставляет средства для внедрения политик безопасности, наиболее подходящих для соответствующей области применения;
- заключает приложения в контейнеры Linux;
- обеспечивает каналы взаимодействия между этими контейнерами;
- управляет контейнерами, защищает каналы взаимодействия и обеспечивает выполнение преднастроенных политик безопасности;
- предоставляет набор готовых компонентов, таких как безопасное удалённое управление системой, аудит/логирование, безопасное хранилище;
- может быть расширен до индивидуально настроенных политик безопасности;
- предоставляет средства для безопасного обновления компонентов ядра Linux (криптографических библиотек, сертификатов, ключей и других данных, относящихся к безопасности). Также может поддерживать полное обновление прошивки устройства.

Наш подход – сделать критически важные компоненты защиты как можно компактнее и контролировать все взаимодействия компонентов системы с помощью KSS for Linux.

Интеграция

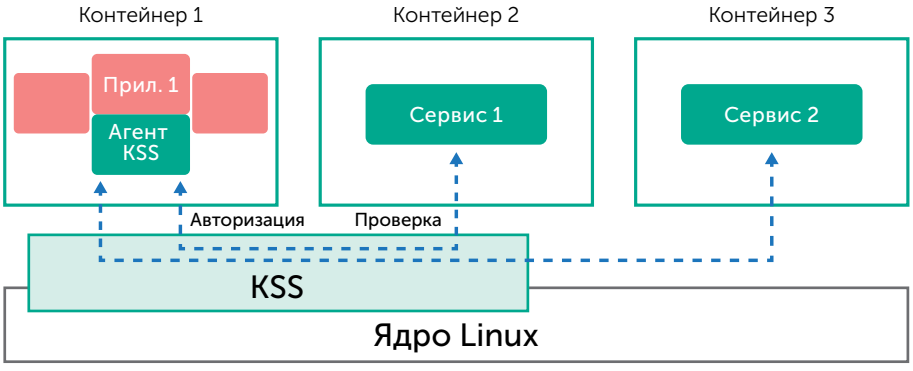
Kaspersky Security System может быть интегрирована с решениями на базе Linux одним из двух способов: неглубокой или более глубокой интеграции. устройству.

Неглубокая интеграция

Простейшая форма интеграции требует минимальных изменений в существующем решении. Поместите приложение в контейнер и используйте компоненты, предоставленные KSS for Linux. Наиболее важные для безопасности функции делегируются выделенным компонентам, таким как:

- безопасный удаленный доступ
- надежные возможности аудита / ведения журнала
- безопасное хранение конфиденциальных данных (конфигурация приложения, ключи, сертификаты, параметры политики и т.д.)

Действия всех этих компонентов могут быть ограничены специфичной для каждого приложения политикой безопасности, настраиваемой и контролируемой средствами KSS for Linux.



В дополнение к функциям, обеспечиваемым неглубокой интеграцией, глубокая интеграция даёт следующие преимущества:

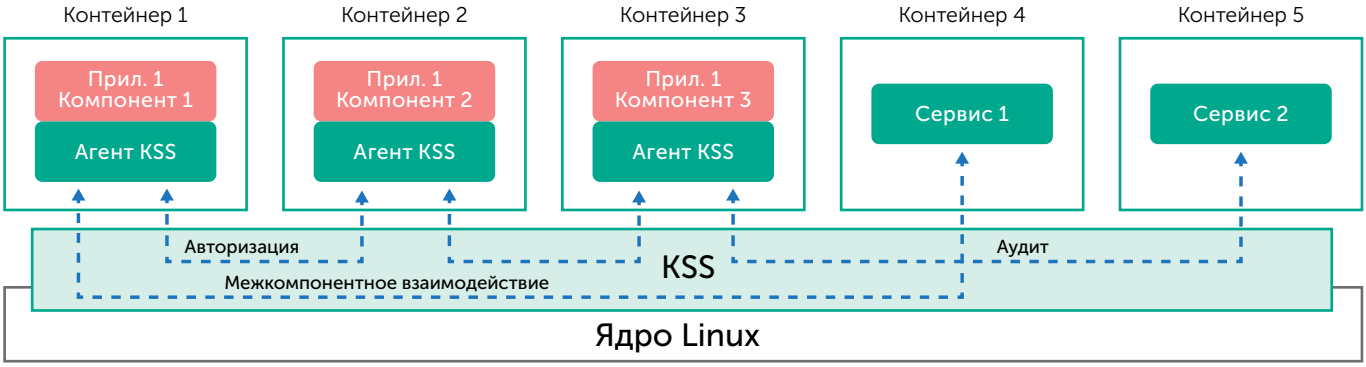
- **тщательный мониторинг и контроль поведения приложений** благодаря наличию доступа к взаимодействиям между их компонентами;
- **понижение привилегий наиболее уязвимых частей приложения**;
- **возможность создания специализированных сервисов**, таких как безопасная служба удалённых обновлений.

Глубокая интеграция

Более глубокая интеграция Kaspersky Security System с решениями на базе Linux предполагает переработку архитектуры существующих приложений таким образом, чтобы сделать их безопасными с помощью KSS.

Например, веб-служба, используемая для безопасного удалённого доступа к промышленному приложению, может быть легко разделена на несколько компонентов, таких как обработчик ввода, запрос на проверку безопасности и механизм обработки запросов. Как наиболее подверженный угрозам и обычно наиболее уязвимый компонент, обработчик ввода работает с минимальными привилегиями. Все запросы от обработчика ввода к движку обработки проверяются и фильтруются в соответствии со строгой политикой. Средство проверки безопасности запросов может либо выступать в роли посредника между обработчиком ввода и механизмом обработки запроса, либо вызываться процессором обработки в качестве средства обработки. Аутентификатор доступа и служба аудита также действуют как службы с явно определёнными интерфейсами.

Декомпозиция может отличаться от описанного выше, сохраняя при этом основную идею – сделать критически важные компоненты защиты как можно компактнее и контролировать все взаимодействия компонентов системы с помощью KSS for Linux.



Особенности

Безопасное удалённое обновление устройств

Некоторые встроенные системы могут требовать особого внимания к вопросам, которые редко возникают в случае чистых ИТ-приложений, таким как непрерывное функционирование или соответствие требованиям функциональной безопасности. Для процедуры удалённого обновления устройства или прикладного программного обеспечения эти аспекты следует рассматривать вместе с требованиями целостности и аутентичности предоставляемых удалённо обновлений. Возможным решением является реализация специальной службы удалённых обновлений, которая наследует все необходимые механизмы безопасности и при этом соответствует внешним требованиям. Решение такого рода требует гибко настраиваемых политик безопасности и надлежащей изоляции этой службы. И то, и другое предоставляется KSS for Linux.

Безопасное удалённое изменение настроек устройства

Необходимость удалённого обслуживания и изменения настроек встраиваемых решений может подтолкнуть разработчика к выдаче повышенных привилегий процессам, которые отвечают за соответствующие изменения настроек системы. При самом худшем сценарии функционал изменения настроек встраивается в само приложение. Результатом такой архитектуры может стать компрометация всего приложения и даже системы ввиду неправильного использования функционала изменения настроек или эксплуатации уязвимостей в коде, который исполняется с повышенными привилегиями.

Есть архитектурное решение данной проблемы, реализация которого не требует значительных усилий. Можно внедрить удалённое изменение настроек, используя специальный изолированный агент в системной среде. Любая ре-

Технические требования

- Ядро Linux версии 2.6.30 и выше (рекомендуется 3.8 и выше)
- Архитектура: Intel x86, ARM, PowerPC

Патенты

Технологии, составляющие основу KasperskyOS и Kaspersky Security System, основаны на ряде патентов:

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.

гулировка прав для любых процессов в такой среде определяется принципом наименьших привилегий. Применение чётко определённой политики по изменению настроек осуществляется механизмами, которые не зависят от самого настраиваемого процесса, и эта политика основывается на принципе отказа по умолчанию. KSS for Linux предлагает именно такое архитектурное решение.

Разделение задач

Иногда необходимо, чтобы приложения, работающие в различных предустановленных режимах, не взаимодействовали друг с другом. Например, алгоритмы диагностики с физически подключённым измерительным прибором не должны иметь доступ к удалённым запросам к диагностируемому оборудованию. Диагностическая информация не должна быть доступна контрагенту, подключённому удалённо. Этот запрет взаимодействий может быть достигнут путём применения политик безопасности. Движок, осуществляющий контроль взаимодействий, может блокировать исполнение приложения в определённом режиме в случае невыполнения условий, описанных в политиках безопасности. Обычно такие политики зависят от конкретной системы. Поддержка гибких политик безопасности и настроек, предлагаемая KSS for Linux, в этом отношении очень полезна.

Безопасная среда для недоверенных компонентов

Несмотря на то, что поставщики встраиваемых систем непрерывно повышают качество кода и надёжность новых программных решений, устаревшие приложения всё ещё широко используются в промышленной автоматизации, транспорте, энергоснабжении и других критических областях. Важные компоненты, которые не могут быть заменены в ближайшем будущем и которые угрожают безопасности всей системы ввиду своей ненадёжности, должны быть изолированы и использоваться только в сочетании с дополнительными мерами, усиливающими их безопасность.

В частности, эти меры могут включать аутентификацию пользователей и запросов, шифрование внешних соединений, фильтрацию запросов, проверку цифровых подписей для скачанных двоичных файлов и другие механизмы. Kaspersky Security System помогает правильно интегрировать сервисы безопасности с устаревшими компонентами, выступая в роли монитора обращений для их взаимодействий.

Сценарии использования, описанные выше, связаны друг с другом. Их общая идея состоит в правильной изоляции компонентов и контроле коммуникаций между ними посредством определённого механизма. Их можно с успехом комбинировать между собой для достижения более сложных целей. KSS for Linux позволяет контролировать как внутренние, так и внешние коммуникации, что особенно важно, когда речь идёт о взаимодействии компонентов различной степени конфиденциальности и надёжности.

Преимущества

- **Высокий уровень безопасности**
  (Изоляция контейнеров Linux и контроль взаимодействий между ними.)
- **Не требует значительных изменений**
  (Необходима только переработка архитектуры.)
- **Работает со всеми версиями Linux** с поддержкой контейнеризации

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