Решения для защиты интернета вещей от «Лаборатории Касперского» и Advantech

KasperskyOS®

www.kaspersky.ru
os.kaspersky.ru

ADVANTECH
Enabling an Intelligent Planet

www.advantech.ru

«В современном высокотехнологичном мире, когда конкурентоспособность практически любого бизнеса зависит от эффективности применяемых IT-решений, защищенность и надежность устройств играют ключевую роль. Особенно это важно для такого класса устройств, как гейтвеи, поскольку они всегда находятся на границе между разными информационными средами. Функции безопасности, определяющие степень доверия к таким устройствам, – один из ключевых параметров при выборе гейтвея. И я хорошо понимаю заказчиков, которые включают пункты по информационной безопасности в ТЗ на свои информационные системы.»

Андрей Духвалов,
Руководитель управления перспективных технологий, «Лаборатория Касперского»

В настоящее время на рынке представлено множество программно-аппаратных комплексов, которые могут использоваться в качестве шлюзов для сбора, обработки и передачи данных. Эти устройства могут выступать как конвертеры сред и протоколов, иметь разнообразные формы и размеры и, самое главное, обладать разными характеристиками. Если идет речь о выборе такого устройства, следует учитывать не только ваши задачи и среду, но и уровень его безопасности.

Задача

Перед специалистами «Лаборатории Касперского» была поставлена задача найти универсальную аппаратную платформу, которую можно адаптировать к выполнению широкого ряда задач и условий, а затем на базе этой платформы построить защитное решение для IoT-гейтвея.

При выборе аппаратной платформы использовались следующие критерии:

- Платформа должна быть широко распространенной и доступной;
- Должна поддерживать операционные системы Linux и иметь хороший пакет поддержки платформы (BSP);
- Характеристики устройства должны поддерживать реализацию всех функций безопасности без ущерба для производительности, чтобы обеспечить защиту самого устройства и контроль других устройств, подключенных к нему.

Решение

После анализа всех вариантов нами была выбрана аппаратная платформа Compact Box Computer UBC-200 производителя Advantech на основе процессора ARM. Из всех продуктов, доступных на рынке, она наиболее полно отвечает всем предъявленным требованиям. Кроме функций, необходимых для реализации решения «Лаборатории Касперского», платформа UBC-200 достаточно универсальна, благодаря чему может использоваться в различных вертикалях интернета вещей – от промышленности и автоматизации умных городов до сельского хозяйства.

В качестве дальнейших шагов в «Лаборатории Касперского» разрабатывается продукт Kaspersky IoT Secure Gateway на базе платы RSB-4411 и устройства UTX-3117 с архитектурой x86.

Основные преимущества использования одноплатного компьютера Advantech Compact Box Computer UBC-200 в качестве аппаратной платформы:

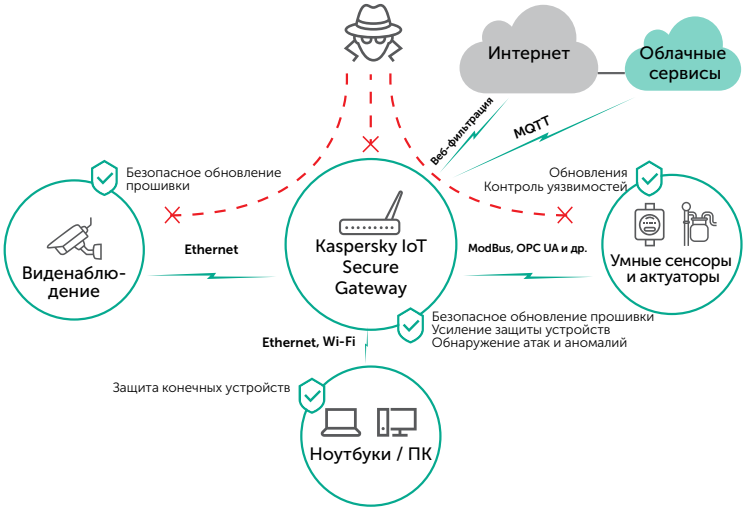
- **Высокая производительность**
  Четырехъядерный процессор i.MX6 на основе ARM Cortex-A9 с оперативной памятью DDR3 до 2 Гб
- **Высокая пропускная способность сети**
  Gigabit Ethernet и возможность использовать модули беспроводной связи
- **Поддержка ПО**
  Функциональный Linux BSP
- **Компактность, климатическая устойчивость**
  Размеры: 111 x 77 x 30 мм; вес: 312 г. Рабочий диапазон температур: 0~60 °C; рабочая относительная влажность: до 95%.

- **Питание и энергопотребление**
  UBC-200 требуется источник постоянного тока 9~24 В.
  Потребляемая мощность при максимальной нагрузке – всего 3,16 Вт.
- **Безопасность**
  UBC-200 позволяет реализовать передовые технологии безопасности, разработанные «Лабораторией Касперского» специально для защиты IoT-устройств, что повышает уровень защищенности как устройства, так и всей сети.

Результат

Используя Advantech Compact Box Computer UBC-200, специалисты «Лаборатории Касперского» смогли внедрить ряд модулей и технологий безопасности:

- **Kaspersky OS**
  При необходимости в качестве программной основы может использоваться KasperskyOS. KasperskyOS – это безопасная операционная система для встраиваемых подключенных устройств со специфическими требованиями к информационной безопасности. KasperskyOS создает среду, в которой уязвимости и ошибки кода больше не представляют угрозы.
- **Kaspersky Security System**
  В зависимости от бизнес-требований, Kaspersky Security System (KSS) – часть KasperskyOS – может использоваться в ОС на базе Linux. KSS обеспечивает выполнение политик безопасности при взаимодействии компонентов ПО.
- **Безопасная загрузка (Secure Boot)**
  Безопасная загрузка позволяет с помощью криптографических методов подтверждать аутентичность и целостность образа прошивки до его загрузки устройством.
- **Безопасное обновление (Secure Update)**
  Безопасное обновление обеспечивает целостность и аутентичность обновлений прошивки при помощи криптографических методов и позволяет обновлять прошивку только из корректно подписанных и зашифрованных образов, полученных из доверенных источников.



О «Лаборатории Касперского»
«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами. Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 270 тысяч корпоративных клиентов во всем мире.

Об Advantech
Компания Advantech, основанная в 1983 г., является ведущим поставщиком надежных инновационных продуктов и решений для встраиваемых систем и промышленной автоматизации. Advantech предлагает комплексную системную интеграцию, оборудование, программное обеспечение, разработку по индивидуальным проектам и глобальную логистическую поддержку, располагая передовыми решениями электронной коммерции для работы с клиентами и организации внутренних процессов. В тесном сотрудничестве с нашими партнерами мы предлагаем законченные решения для широкого спектра применений в различных отраслях. Компания Advantech постоянно является новатором в разработке и производстве качественных вычислительных платформ высокой производительности, и наша миссия состоит в раскрытии практического потенциала этих инноваций в надежных продуктах и услугах. Выбирая Advantech, можно быть уверенным в отсутствии барьеров перед применениями и возможностями наших продуктов.

- **Безопасный аудит (Secure Audit)**
  Безопасный аудит – это функция KasperskyOS, которая распознает, записывает и хранит журналы аудита и гарантирует, что записи в них не будут подменены.
- **Контроль приложений Linux (Linux Application Control)**
  Контроль приложений Linux позволяет создавать белые и черные списки исполняемых объектов в системе и блокировать исполнение неразрешенных файлов, а также получать из Kaspersky Security Network информацию о репутации приложения и рекомендации по его безопасности. Эта технология помогает предотвратить заражение IoT-устройств такими вредоносными программами, как Mirai и Bashlite.
- **Веб-фильтр/Родительский контроль (Web-filter/Parental control)**
  В зависимости от предназначения устройства, в его прошивку могут быть добавлены технологии веб-фильтрации (устройства для организаций, индустриальные устройства) или родительского контроля (устройства для домашних пользователей, например для умного дома).
- **Защита на базе машинного обучения (Machine Learning-based protection)**
  Чтобы обеспечить надежную защиту устройств и сетей, подключенных к гейтвею, в Kaspersky IoT Secure Gateway используются технологии машинного обучения (Machine Learning, ML) для идентификации и категоризации всех устройств в сети с помощью активного и пассивного анализа их поведения, составления профиля каждого устройства и детектирования аномальной или непредусмотренной активности.
- **Обнаружение активов на базе ML (ML asset discovery)**
  Технология обнаружения активов с использованием ML позволяет автоматически обнаруживать, категоризировать и систематизировать все активы в защищенной сети. Используя специальную технологию распознавания по идентификационным меткам (fingerprints), наше решение определяет тип устройства, его производителя, модель и даже версию прошивки, анализируя при этом лишь определенные элементы (метаданные) сетевого трафика.
- **Анализ поведения устройств на базе ML (ML device behavior analysis)**
  Когда активы в сети обнаружены и категоризированы, для них создаются особые профили. Профиль описывает нормальное поведение устройства с данной прошивкой в данной пользовательской сети.
- **Выявление аномалий на базе ML (ML Anomaly Detection)**
  Использование технологий на базе ML для обнаружения активов и создания профилей устройств позволяет выявить любую аномалию в устройствах интернета вещей, в том числе индустриального. Технология детектирования аномалий на базе ML позволяет обнаружить активность вредоносного ПО и ботнетов, участие устройств в DDoS-атаках, эксплуатацию прошивки, майнинг, перехват управления устройством хакерами и т.д.

KasperskyOS®

Подробнее на
os.kaspersky.ru

www.kaspersky.ru