Защита интернета вещей с помощью аппаратных элементов безопасности

Ксавье Бигналет (Xavier Bignalet), менеджер по маркетингу продукции, Microchip Technology

Интернет вещей (IoT) значительно расширил область потенциальных угроз для всего рынка. Каждое IoT-устройство представляет собой уязвимую конечную точку, а рост числа успешных атак на программные средства защиты доказал, что такой подход совершенно несостоятелен, особенно в случае использования небольших микроконтроллеров.

Накопленный отраслевыми компаниями опыт показывает, что для сокращения уязвимости необходимо усилить модель аутентификации подключаемого устройства с помощью элемента безопасности, настроенного на хранение закрытых ключей и обработки криптоалгоритмов. К сожалению, из-за логистических ограничений в цепочке поставок такой подход оказалось трудно использовать применительно к большинству проектов малого и среднего масштабов. Возник закономерный вопрос: как реализовать кастомизированный производственный процесс, предложив массовому рынку уникальный действующий ключ для каждого устройства по доступной стоимости?

К настоящему времени появилась возможность благодаря подходящей платформе предоставить приложениям интернета вещей аппаратную защиту с помощью предварительно подготовленных элементов безопасности; при этом минимальный объем заказа составляет всего 10 предварительно подготовленных устройств. Таким образом, если изготовленные на производстве элементы безопасности предварительно настроить и зарегистрировать для использования с IoT-устройствами, доступ к хранилищу аппаратных ключей безопасности может осуществляться с помощью типового сертификата при меньшей стоимости из расчета на одно изделие и значительно проще, чем с привлечением сторонних компаний для конфигурации устройств, поставщиков сервисов инфраструктуры открытых ключей (PKI) и центров сертификации. Даже такое базовое приложение интернета вещей как шлюз, кондиционер или камеру наблюдения теперь можно защитить на аппаратном уровне с помощью предварительно сгенерированных типовых сертификатов, которые изолированы внутри элемента безопасности для автономной облачной аутентификации.

Преимущества элементов безопасности

Не существует универсального подхода, обеспечивающего безопасность интернета вещей, – каждой реализации требуется собственная многоуровневая стратегия. Однако согласно принципу Керкгоффса, при оценке надежности шифрования предполагается, что злоумышленник знает об используемой системе шифрования все кроме ключей. Ключ играет решающую роль, позволяя клиенту и хосту установить подлинность «доверенной идентичности» устройства, прежде чем оно получит возможность установить связь, обмениваться данными или совершать транзакции. Необходимо, чтобы ключ был защищен от физических атак и удаленного извлечения. Оптимальное решение состоит в изоляции стандартных криптографических ключей в элементе безопасности и обеспечении изолированной защищенной границы, чтобы они не были открыты. Для реализации такой защиты разработчику требуются соответствующие знания и опыт, а также дополнительное время на проектирование IoT-решения. Как бы то ни было, такой подход является фундаментальным в сфере обеспечения безопасности.

Прежде всего, каждому IoT-устройству должен быть предоставлен элемент безопасности, который работает совместно с микроконтроллером устройства [1]. Затем этот элемент необходимо правильно настроить для выбранных сценариев использования, оснастить регистрационными данными и другими криптографическими средствами, которые применяются для конкретной модели аутентификации. Далее устройству предоставляются соответствующие ключи для каждого из соответствующих сценариев использования; при этом исключается возможность раскрытия этих ключей на любом этапе производства. Такая технологическая операция часто недоступна для большинства малых или средних проектов.

Производители устройств для интернета вещей, как правило, возлагают на себя бремя такого аппаратного механизма аутентификации только в случае крупных заказов, но теперь полупроводниковая промышленность получила возможность реализовать этот механизм для массового внедрения. Благодаря новой платформе доверия (Trust Platform) компании Microchip для ее семейства устройств CryptoAuthentication появилось несколько способов развертывания безопасного хранилища ключей для аутентификации в любом объеме. Например, некоторые производители предпочитают вариант изготовления IoT-изделий с предварительно зарегистрированными элементами безопасности. В этом случае закрытый ключ элемента безопасности и типовые сертификаты генерируются на этапе изготовления на защищенном оборудовании Microchip и остаются нераскрытыми на протяжении всего защищенного процесса регистрации. Они надежно заперты внутри элемента безопасности при отгрузке и далее при подключении к автоматизированному IP-облаку или сети LoRaWAN.

Производителям может потребоваться не только аутентификация некоторых или всех выпускаемых устройств при подключении к сети. Например, некоторые заказчики желают работать с собственной цепочкой сертификатов, воспользовавшись также предварительно сконфигурированными сценариями, чтобы сократить время и сложность кастомизированного решения. Примеры этих сценариев варьируются, начиная с таких базовых мер безопасности как аутентификация на основе сертификатов TLS (Transport Layer Security) и заканчивая проверкой подлинности в сетях LoRaWAN, обеспечение безопасной загрузки, обновлений по беспроводной сети (OTA), защиты IP и данных пользователя, а также ротации ключей. Другим же заказчикам помимо использования основных сценариев требуется возможность собственной настройки параметров.

В отрасли увеличивается спрос на самое широкое внедрение аппаратной безопасности рассматриваемого типа и обеспечение аутентификации IoT-устройств в любой открытой или частной облачной инфраструктуре. Например, компания Microchip Technology недавно воспользовалась функциями веб-сервиса Amazon (Amazon Web Services, AWS), чтобы упростить подключение к сервисам AWS IoT любых изделий, созданных с использованием платформы доверия. Продукция Microchip обеспечивает предварительно сконфигурированную или полностью

настраиваемую аппаратную безопасность для IoT-устройств с использованием защищенного элемента безопасности ATECC608A.
Эта последняя разработка в области аппаратной безопасности позволяет компаниям, работающим над проектами любого размера, легко и экономично внедрять элементы безопасности в свои IoT-устройства. Трудности, традиционно связанные с настройкой и предоставлением безопасных элементов, устранены, создана безопасная цепочка поставок для заказов любого объема. Кроме того, появилась возможность распространить передовой отраслевой опыт на аутентификацию любых подключаемых устройств во всех приложениях интернета вещей.

Ссылки

1. Antony Passemard. Securing cloud-connected devices with Cloud IoT and Microchip//https://cloud.google.com/blog/products/gcp/securing-cloud-connected-devices-with-cloud-iot-and-microchip.

MCA837ru