DOI: 10.22184/1992-4178.2019.183.2.92.94

Обеспечение безопасности коммуникаций промышленных встраиваемых систем с облачными сервисами

Кс. Биньяле[1]

УДК 004.738 | ВАК 05.13.15

Внедрение «Индустрии 4.0» позволило автоматизировать работу «умных» фабрик благодаря концепции удаленного производства и управления. Однако наряду со многими преимуществами с точки зрения эффективности бизнеса возникают риски несанкционированного доступа к весьма дорогостоящим ресурсам предприятия. Причем под угрозой оказываются не только ценное оборудование, но и доходы компании от произведенных изделий. Рассмотрим, как обеспечить защиту и предотвратить потенциальные угрозы для безопасности сетей Интернета вещей, используя комплексное решение компании Microchip.

Когда «умная» фабрика подключается к публичному или частному облачному сервису, возникают риски для внутренней безопасности компании. Это происходит, как только предприятие соединяется с сетью, например при обращении во внешний центр данных. Задача состоит в том, чтобы сохранить гибкие преимущества подключенной фабрики, обеспечив сетевую безопасность.

Для начала стоит определить, какое решение будет использовать коммуникационная система предприятия – проводное, беспроводное или комбинированное. Рекомендуется применять сетевую технологию на основе стандартных протоколов, таких как Wi-Fi, Bluetooth или Ethernet, которые наиболее широко распространены в промышленном сегменте. Использование общепринятых подходов к обеспечению безопасности снижает риск взлома сетевого соединения, хотя такой подход иногда идет вразрез с увлечением специализированными решениями для промышленности. Инфраструктура сети должна быть надежной и служить долгие годы. Хотя во многих сетях применяют собственные протоколы, их использование должно быть ограничено внутренними нуждами предприятия.

Одна из проблем состоит в том, что даже у самого квалифицированного специалиста по встраиваемым системам ограниченные познания в области ИТ-безопасности. Инженеры – не эксперты в этой сфере, пробел в знаниях – помеха для создания надежной и безопасной инфраструктуры Интернета вещей (IoT). Как только устанавливается связь фабрики с облаком, инженеры погружаются в мир Amazon Web Services (AWS), Google, Microsoft Azure и других сервисов, а вскоре обнаруживают, что нуждаются в помощи ИТ-специалистов, чтобы справиться с разнообразными угрозами безопасности.

Среди основных целей хакеров – использование одной точки входа в сеть для того, чтобы получить удаленный доступ к большей части систем. Удаленные атаки могут обернуться крупным ущербом для предприятия, как, например, это продемонстрировали массовые DDoS-атаки. Самая слабая точка IoT-сети – это, как правило, оборудование и его пользователь в конечном сетевом узле, поскольку обслуживающие оборудование инженеры недостаточно подготовлены в области ИТ, чтобы самостоятельно справиться с возможной проблемой.

Однако ситуация меняется. Такие компании, как Microchip Technology, в качестве одного из элементов своей миссии рассматривают обучение инженеров по вопросам создания инфраструктуры комплексной безопасности. Кроме того, источником специальных знаний служат крупные облачные компании, такие как AWS, Google и Microsoft. Важный урок для специалистов – не пренебрегать безопасностью и не считать ее дополнительным элементом, создаваемым уже после развертывания IoT-сети. К моменту запуска IoT-сети заботиться о безопасности бывает слишком поздно. Меры защиты продумываются заранее и планомерно реализуются в любом проекте

[1] Компания Microchip, менеджер по маркетингу продуктов для обеспечения безопасности.

Интернета вещей. Изначально безопасность закладывается в аппаратуре, она не может быть добавлена на более поздних этапах разработки, например, в виде дополнительного программного модуля.

ИДЕНТИФИКАЦИЯ

Наиболее важный элемент обеспечения безопасности – идентификация. Системный разработчик должен позаботиться о том, чтобы каждый узел, подключенный к сети, был снабжен уникальным, защищенным и достоверным идентификатором. Важно знать, что пользователи сети являются теми, за кого себя выдают, и им можно доверять. Для этого обычно применяются протокол TLS1.2 и процесс взаимной идентификации сервера и конечного узла IoT-сети, что обеспечивается путем использования источника информации, которому доверяют обе стороны, – центра сертификации.

Однако выданные центром сертификации права доступа (полномочия) должны быть защищены на всех этапах – от запуска проекта, в самом процессе производства, и до момента развертывания системы на «умной» фабрике. Должен быть в безопасности секретный ключ для подтверждения прав доступа конечного узла IoT-сети. Сегодня повсеместно применяется слабо защищенный метод – хранение секретного ключа в незашифрованном виде во флеш-памяти микроконтроллера, где он может подвергнуться манипуляции с помощью программных средств. Каждый может воспользоваться доступом к этой области памяти и получить секретный ключ. Этот несовершенный подход может дать разработчикам ложное чувство безопасности, на этом участке и возникают основные проблемы.

ЭЛЕМЕНТ ЗАЩИТЫ

Защищенное решение состоит в том, что ключ и другие критичные данные должны быть не только удалены из микроконтроллера, но и изолированы от микроконтроллера и от любого воздействия ПО. На передний план выходит понятие элемента защиты, задача которого – обеспечить зону безопасности для хранения и защиты ключа, где никто не может получить к нему доступ. Для подтверждения прав доступа можно обеспечить связь по схеме «вопрос-ответ» между микроконтроллером и элементом защиты с помощью команд библиотеки CryptoAuthLib. Секретный ключ не покидает элемента защиты ни на каком этапе разработки продукта и его жизненного цикла. Таким образом можно организовать непрерывную доверительную цепочку.

В качестве элементов защиты выступают специализированные микросхемы семейства CryptoAuthentication компании Microchip, которые можно представить в виде сейфов для хранения секретов предприятия. В данном случае они содержат секретные ключи, используемые для IoT-идентификации.

ПОРЯДОК СОЗДАНИЯ КЛЮЧЕЙ

Еще один важный аспект – контроль получения пользователем секретных ключей и других регистрационных данных с помощью устройства семейства CryptoAuthentication. Для этого компания Microchip предлагает платформу, на базе которой пользователь может создать и надежно запрограммировать свои секретные данные в процессе производства микросхем без доступа посторонних лиц, включая сотрудников Microchip. После того как информация сформирована, Microchip изготавливает элемент защиты на своем производственном участке и высылает конечным пользователям сразу же, как только изделие покидает защищенные и сертифицированные в соответствии с общепринятыми критериям обеспечения безопасности помещения.

Когда пользователи входят в учетные записи в облачном сервисе AWS IoT, они получают сертификаты пользователя, созданные в их интересах компанией Microchip с помощью AWS-функции «использовать свой собственный сертификат» (Use Your Own Certificate). Затем с помощью AWS IoT-функции, получившей название «регистрация точно вовремя» (just-in-time registration – JITR), они выполняют групповую загрузку сертификатов уровня устройства, которые предоставляются элементами защиты для учетных записей AWS IoT. Теперь сертификат уровня пользователя сможет проверить сертификат уровня устройства, завершив цепочку сертификатов. Эта функция делает возможной полное масштабирование Интернета вещей в рамках предприятия с учетом обеспечения безопасности. Используя JITR-процесс, можно обработать многие тысячи сертификатов параллельно и без вмешательства пользователя. Вместо того чтобы вручную загружать сертификаты от подключенных устройств в облачную учетную запись и открывать их посторонним, пользователи могут организовать автоматическую регистрацию сертификатов нового устройства как часть процесса установления связи между устройством и AWS IoT-платформой, причем без ущерба для безопасности.

НАЧАЛО РАБОТЫ С ОБНОВЛЕННЫМ КОМПЛЕКТОМ AT88CKECC-AWS-XSTK-B

В комплект разработчика для создания безопасной IoT-сети Zero Touch от Microchip (см. рисунок) входит сопроцессор шифрования ATECC508A-MAHAW семейства CryptoAuthentication, который предварительно

Комплект разработчика AT88CKECC-AWS-XSTK-B семейства Zero Touch

сконфигурирован для идентификации пользовательской учетной записи в облачном сервисе AWS IoT. Первый этап работы с комплектом – определение цепочки сертификатов с помощью обновленных Python-скриптов и изучение процесса создания ключей компании Microchip. Комплект ознакомит разработчика с принципами производственного процесса компании. Изделие Microchip защищено от взлома, в том числе от воздействия внешних атак. Оно оснащено высококачественным генератором псевдослучайных чисел, соответствующим стандарту FIPS (Federal Information Processing Standard), и малопотребляющим криптографическим ускорителем, совместимым с широчайшим спектром IoT-устройств и различными вариантами реализации технологического маршрута.

В дополнение к Python-скриптам комплект содержит CloudFormation-скрипт для ускорения установки учетной записи в AWS, что повышает доступность работы с облачным сервисом для разработчиков встраиваемых систем. Используя CloudFormation-скрипт, инженер может в течение нескольких минут описать интерфейс пользователя в среде AWS.

ЗАКЛЮЧЕНИЕ

Комбинация JITR-регистрации от AWS IoT с сопроцессором шифрования ATECC508A-MAHAW семейства CryptoAuthentication и процессом создания секретных ключей компании Microchip – лучшее в своем классе решение для защиты IoT-сетей. Это по-настоящему комплексное решение обеспечивает возможность дальнейшего эффективного и безопасного развития «Индустрии 4.0». ●