Безопасность «Интернета вещей»: существующие проблемы и их решение

Гийом Кринон (Guillaume Crinon)
Управляющий по техническому маркетингу в регионе EMEA компании Avnet Silica
guillaume.crinon@avnet.eu

В наши дни «Интернет вещей» является весьма популярной темой: конференции, на которых затрагиваются вопросы безопасности и выступают компании, производящие оборудование или программное обеспечение, проходят чуть ли не еженедельно, новые решения постоянно освещаются в специализированных изданиях. Компания Avnet Silica также считает необходимым принять участие в обсуждении этой важной и интересной темы.
В статье разъясняется, что именно, по мнению специалистов Avnet, скрывается за понятием «безопасность «Интернета вещей», а также перечислены реальные проблемы клиентов компании, которые касаются таких аспектов, как аппаратные средства и встроенное либо серверное программное обеспечение (ПО). Решения, обеспечивающие безопасность «Интернета вещей», представлены в том ключе, как Avnet представляет его развитие в течение ближайших 6–8 лет, т. е., пока наш мир не перейдет полностью на протоколы IPv6 и 6LoWPAN.

Введение

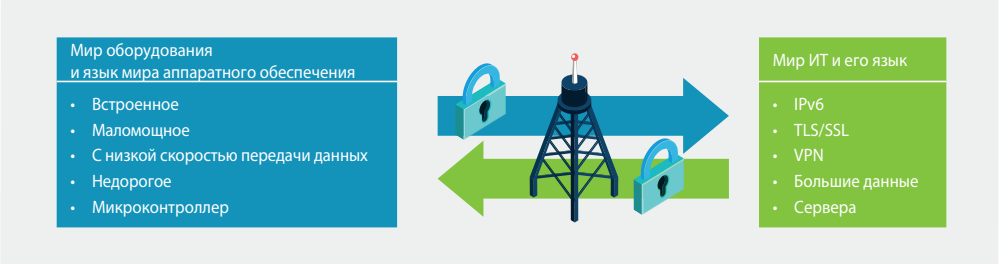
Мы могли бы, подобно многим другим, начать с пространственных объяснений, почему подключенные устройства находятся в зоне риска, как хакеры могут разрушать бизнес-модели, и насколько глубоко каждый должен разбираться в криптографии. Но мы этого делать не станем и пойдем несколько иным путем.

Удивительно это или нет, но главная проблема, с которой сталкиваются наши клиенты, это стоимость персонализации устройств, которые производятся ими с использованием уникальных идентификаторов ID, MAC-адресов, ключей и сертификатов, независимо от того, происходит это непосредственно на производственной линии во время изготовления оборудования или у конечного заказчика во время его установки. Удивительно это или нет, но технические решения для персонализации очень часто предоставляют дополнительный инструментарий, обеспечивающий самый высокий уровень безопасности, причем без каких-либо дополнительных затрат.

В предлагаемой статье мы покажем, как ту архитектуру безопасности Интернета, которую мы строим на протяжении уже более 20 лет, следует использовать для создания архитектуры безопасности «Интернета вещей», а также объясним, как должным образом решить возникающие проблемы безопасности и ресурсного обеспечения не подключенных по протоколу IPv6 сенсоров и устройств с низким собственным энергопотреблением.

На протяжении последних 15 лет предприятия, работающие в сфере информационных технологий (ИТ), успешно модернизировали свои схемы защиты для устройств разных классов, начиная от подключенных проводами настольных компьютеров и заканчивая современными беспроводными ноутбуками и смартфонами. Уровень безопасности при этом постоянно повышался. Подобная эволюция происходит и сейчас: помимо ноутбуков и смартфонов, производителям при помощи закрытых и публичных (общедоступных) сетей приходится подключать огромное количество устройств, машин и механизмов, различных объектов с серверами приложений. Как это происходит, будет показано ниже.

Преодоление разрыва между встраиваемыми и ИТ-приложениями



Какие же проблемы должны быть решены?

Сложность персонализации подключенных устройств

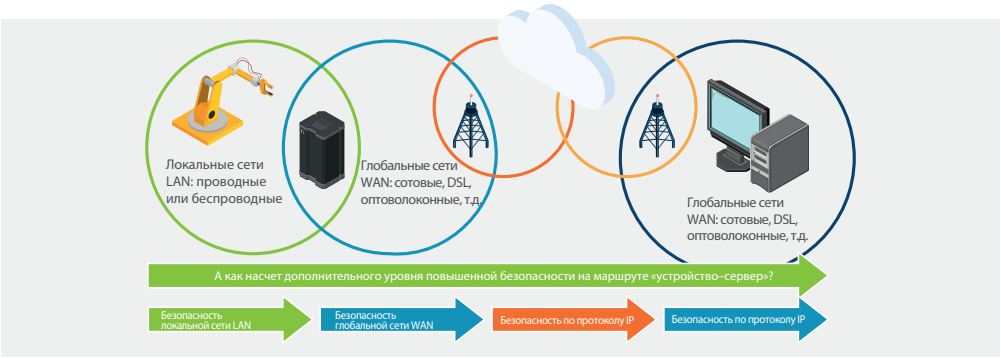
Независимо от области применения и используемой схемы защиты, всегда наступает такой момент, когда устройству, подключаемому к другому устройству или удаленному серверу, необходим кто-то, кто внесет в память устройства уникальные идентификаторы либо ключи доступа. Это и называется персонализацией устройства. И она несет за собой определенные сложности, которые всегда приходится решать либо производителю оборудования, либо уже его конечному потребителю.

Для пояснения приведем простой наглядный пример, а именно — подключение Wi-Fi-принтера в домашнюю сеть. В какой-то момент для того, чтобы пользователи сети могли использовать один и тот же ключ доступа, вам нужно будет вручную подсоединить принтер к Wi-Fi-роутеру. Неважно, будете вы это делать с помощью беспроводной связи или через USB-кабель, но в принтер нужно будет ввести ключ. В этом случае задачу персонализации решаете вы, как конечный пользователь, а не производитель принтера.

То же самое происходит и в бизнесе, только в больших масштабах. Для примера возьмем систему сигнализации, входящую в комплекс автоматизации здания. Она состоит из центрального сервера и нескольких периферийных устройств, соединенных локально с помощью радиочастотной связи, и могла быть приобретена как в комплекте, так и в виде ее отдельных частей. И тогда либо производителю, либо продавцу, либо организации–конечному пользователю самостоятельно нужно будет связать все эти периферийные устройства с центральным сервером, который, в свою очередь, зарегистрировать на сервере удаленной мониторинговой службы (например, охранной компании).

Во всех этих случаях кто-то должен взять на себя расходы по решению задачи персонализации и процессу подключения, будь то производитель устройства, поставщик услуг или конечный пользователь с собственным опытом подключения уже готового к использованию оборудования.

Сложность этих процессов часто делает их слабым звеном в безопасности сетей. Как часто вы обновляете свой ключ доступа к домашней Wi-Fi-сети? Возможно, никогда, так как это слишком хлопотно. Как часто AES-ключ (Advanced Encryption Standard — усовершенствованный стандарт шифрования) обновляется в ваших многочисленных системах? Скорее всего, не слишком часто, а то и никогда, и по тем же причинам.



Работа сетей и их безопасность: важность комплексного решения

Канальная и сетевая безопасность в настоящее время обеспечивается различными коммуникационными и сетевыми технологиями на различных уровнях, наборами протоколов, такими как IPsec для IP, WPA 802.11, 802.15.4, Bluetooth, и т. д. Однако они не должны рассматриваться, как средство для обеспечения комплексной конечной безопасности соединений. Действительно, иметь защищенное посредством WPA соединение Wi-Fi в локальном маршрутизаторе, безусловно, недостаточно для того, чтобы обеспечить в частном порядке соединение HTTP на отдаленном сервере, поскольку ключи большинства локальных сетей вряд ли когда-либо обновляются по причинам, перечисленным выше.

Ниже показан пример достаточно обычной ситуации, когда данные с сенсора или исполнительного механизма, прежде чем достигнут нужного сервера, транслируются через много сетей разного типа, принадлежащих большому количеству поставщиков услуг.

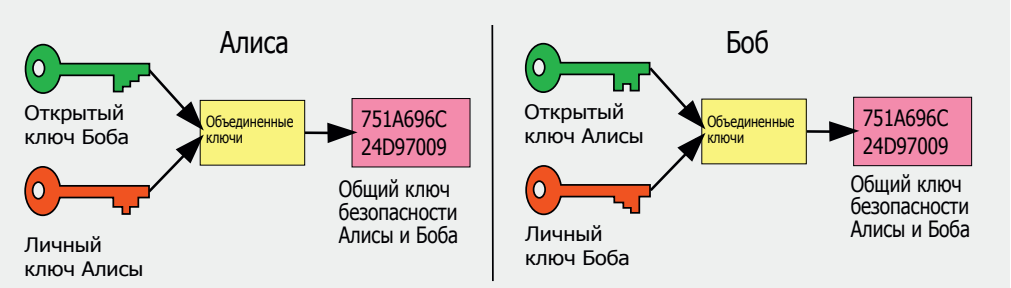
На каждом звене передачи безопасность этого конкретного участка обеспечивается протоколами, а что происходит до или после него — неизвестно, это «тайна за семью печатями». Вследствие этого данные расшифровываются и снова зашифровываются шлюзами безопасности на каждом участке. Как известно, уровень безопасности всей системы определяется уровнем безопасности самого слабого звена. Поэтому ситуация с комплексной безопасностью находится в зависимости от безопасности, обеспеченной несколькими провайдерами и производителями шлюзов, и остается полностью на их совести, что и является слабым звеном всей системы безопасности.

В случае, если данные передаются по межсетевому протоколу IP непрерывно, есть возможность их так называемого «туннелирования» на пути от устройства к серверу. Однако это единственное исключение в данной схеме, которое приблизительно соответствует понятию комплексной конечной безопасности.

Дополнительный уровень комплексной безопасности на маршруте «устройство–сервер» решает следующие задачи:

- аутентификация устройства на сервере;
- аутентификация сервера на устройстве;
- создание ключа безопасности сеанса связи;
- целостность данных;
- конфиденциальность данных, если требуется.

Магия Диффи-Хелмана



Решения

SSL (уровень защищенных сокетов)

Прошло уже более 20 лет с тех пор, как компания Netscape представила в 1995 г. первую публичную версию SSL (получившую номер 2.0, так как версию 1.0 не выпустили из-за присущих ей недостатков).

Идея была проста: найти способ, как дать интернет-пользователям возможность безопасно, конфиденциально и непрерывно соединяться с удаленными серверами для работы с почтой, интернет-банкингом, сервисами электронной коммерции вне зависимости от того, кто является производителем самого компьютера («железа») и установленной на нем операционной системы («софта»).

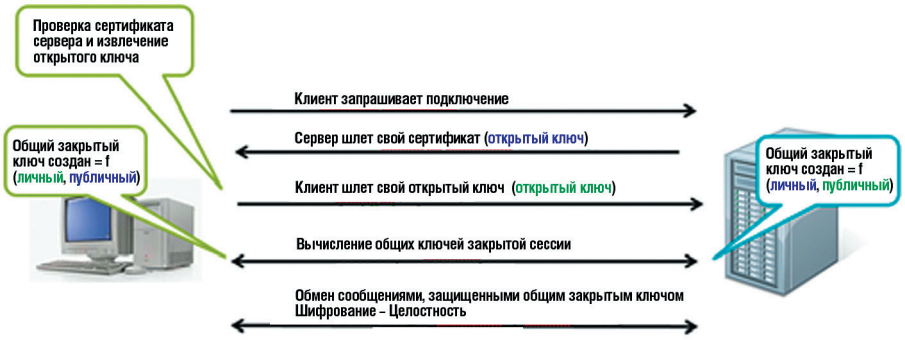
«Безопасно, конфиденциально и непрерывно» означало, что клиент имеет возможность проверить подлинность сервера, не раскрывая пароли и конфиденциальную информацию третьим лицам, включая интернет-провайдеров и телеком-операторов. Также это должно было оставить без работы любителей «подслушивать» и хакеров. Самым простым решением данной проблемы было использовать один и тот же уникальный ключ безопасности на обеих сторонах коммуникационного канала.

Однако возникла новая проблема: как передать этот уникальный ключ безопасности, не раскрывая его? Возможным решением могло стать использование дополнительного канала. В конце концов, банки шлют нам ПИН-коды карт в отдельном письме, а некоторые сайты используют нашу электронную почту, чтобы послать нам временный пароль в процессе регистрации на новом сервисе или для обновления старого пароля.

Тем не менее, это еще не был молниеносный процесс и, конечно, это было непрактично для обновления ключей сеанса на постоянной основе, причем бесшовным (не прерывающим сеанс, незаметным) и открытым для пользователя способом.

Настоящий прорыв произошел благодаря применению ассиметричной криптографии.

Эта технология включила в себя фундаментальные труды основателей ассиметричной криптографии Клиффорда Кокса (Clifford Cocks), Уитфилда Диффи (Whitfield Diffie), Мартина Хелмана (Martin Hellman), Рона Ривеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman), которые они опубликовали



еще за 20 лет до этого, в промежутке между 1973 и 1977 гг. Они разработали методы для вычисления уникального ключа безопасности, который могут совместно через открытый канал связи, не раскрывая при этом никакой секретной информации, использовать два связанные объекта. Невероятно! Так что, если вы увидите аббревиатуру RSA (Rivest, Shamir, Adleman) или DH (Diffie-Hellman), вспомните этих математиков. Поскольку Кокс работал на британскую разведку, до недавнего времени его работы и само имя ученого были засекречены, но, тем не менее, он также заслужил наше признание.

Ассиметричная криптография RSA, ECC (RSA — аббревиатура от фамилий Rivest, Shamir, Adleman; ECC — Elliptic Curve Cryptography, эллиптическая криптография) — это мощный инструмент, но он требует намного больше вычислительной мощности для зашифровки и расшифровки данных по сравнению с симметричными алгоритмами DES, AES (DES — Data Encryption Standard, стандарт шифрования данных; AES — Advanced Encryption Standard, также известный, как алгоритм Рэндала (Rijndael), симметричный алгоритм блочного шифрования). Поэтому его использование оказалась не очень эффективно для передачи каждого зашифрованного пакета данных по Интернету и, как следствие, применение ассиметричной криптографии ограничили обменом и вычислением ключей симметричных сеансов, которые и используются для шифрования и дешифрования потоков данных в Интернете.

Возвращаясь в 1995 г., отметим, что у пользователей все же была возможность безопасно проверять подлинность сервера и вычислять общий ключ защищенного сеанса, используемого для обмена данными.

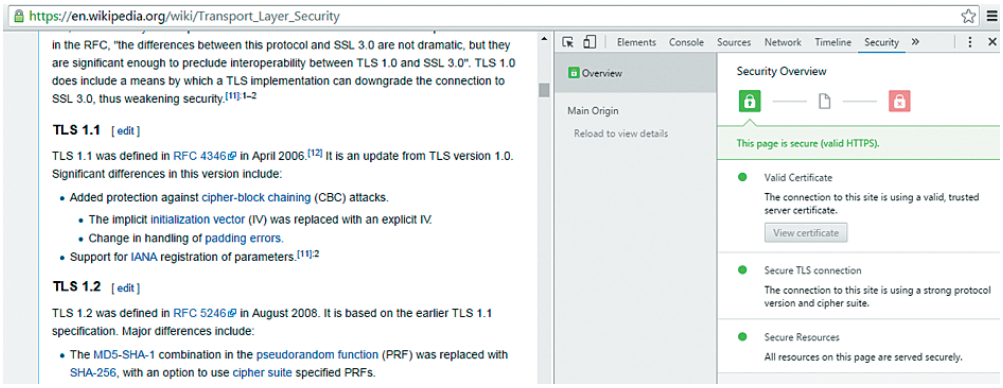
Как показано на рисунке, серверы не посылают свои открытые ключи в чистом виде, они посылают сертификаты, которые содержат в себе их открытые ключи.

Почему же нельзя послать открытый ключ напрямую?

Дело в том, что клиент должен иметь возможность отличать настоящий сайт от поддельного. Как, например, отличить "www.mybank.com" от "www.my-bank.com", если последний хочет выдать себя за подлинный банк, чтобы похитить ваши конфиденциальные данные?

Оба сайта имеют открытый ключ, но клиенту нужно проверить и убедиться, какой из этих сайтов действительно является подлинным.

Для того, чтобы осуществлять такие проверки, созданы Центры сертификации (Certificate Authorities, CA). Это независимые корпорации, которые выпускают цифровые сертификаты,



удостоверяющие принадлежность открытого ключа той организации, чье имя указано в сертификате.

Давайте предположим, что "www.mybank.com" хочет выпустить открытый ключ. Сначала Mybank посылает ключ в центр сертификации вместе с сопроводительными документами и доказательством их идентичности. Центр сертификации проверит, является ли "www.mybank.com" собственником ключа, и после этой процедуры выпустит цифровой сертификат (в соответствии со стандартом X.509). В нем будет содержаться, помимо открытого ключа "www.mybank.com", имени компании-владельца, сроков действия и другой сопутствующей информации, закрытый ключ самого центра сертификации.

Затем этот сертификат будет выслан обратно в "www.mybank.com", и он будет отправляться клиентам, запрашивающим соединения.

После получения клиент проверит подпись сертификата, используя открытый ключ центра сертификации, который, как правило, уже установлен в браузер. Таким образом, он убедится, что открытый ключ, содержащийся в сертификате, действительно принадлежит сайту "www.mybank.com", к которому и надо подключиться.

Несмотря на большое количество предложений по улучшению системы, именно эта архитектура на текущий момент позволяет обеспечивать безопасность интернет-соединений.

Ниже приведен снимок экрана компьютера, иллюстрирующий процесс запроса.

TLS (безопасность транспортного уровня)

После обнаружения некоторых недостатков и уязвимых мест в SSL2.0 и SSL3.0, протокол SSL был заменен протоколом TLS1.x, основанном на улучшенных алгоритмах цифровой подписи, аутентификации и шифрования. Но в рамках данной статьи мы не будем на них останавливаться.

Также протокол RSA часто заменяют протоколом ECC, так как он создает ключи намного меньшей длины и не требует сложных вычислений, обеспечивая при этом более высокий уровень безопасности.

Встроенные сенсоры и IPv6

С учетом того, что прогнозируемое число устройств, которые будут подключены к интернету, постоянно растет, размер адресного пространства уже изменился с 32 бит в IPv4 (4,3 млрд уникальных адресов) до 128 бит в IPv6 (3,4x1038 уникальных адресов!). И даже несмотря на это миллиарды уже установленных сенсоров и устройств все еще не являются IP-совместимыми.

С одной стороны, большинство этих устройств могут передавать данные, используя беспроводные технологии, и работать от аккумуляторов в течение 5–15 лет, в зависимости от сферы использования.

А с другой стороны, IP-совместимые беспроводные технологии, такие как 802.11 и 3G/4G, которые используются уже не один год, сильно снижают срок службы аккумуляторов этих устройств.

Вместе с тем, беспроводные технологии, которые рационально используют аккумуляторы за счет уменьшения полезных нагрузок, увеличения времени «спящего режима», асинхронного режима и

ассиметричного соединения, очень часто подключаются к шлюзам таких LAN-протоколов, как Bluetooth, ZigBee, WmBUS, Z-Wave, Enocean, KNX, ioHomeControl, 802.15.4, а также без использования шлюзов с LPWAN (Low Power Wide Area Network, энергоэффективная сеть дальнего радиуса действия) на основе таких технологий, как Sigfox, LoRaWAN, NB-IoT и еще нескольких.

Несмотря на недавние внедрения протокола 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks — энергоэффективные беспроводные персональные сети под стандарт IPv6) в такие стандарты, как Thread и Bluetooth 4.2, ожидается, что огромное количество датчиков и устройств, которые будут внедрены под лозунгом «Интернета вещей», не будут на самом деле IP-совместимыми. Причем, это будет, как минимум, до 2025 г., хотя бы

по соображениям обратной совместимости с существующими продуктами. Это означает, что все эти миллиарды устройств, от интеллектуальных счетчиков до индустриальных сенсоров, не смогут использовать стандарт IP для установления TLS-сеанса с сервером, к которому они подключаются.

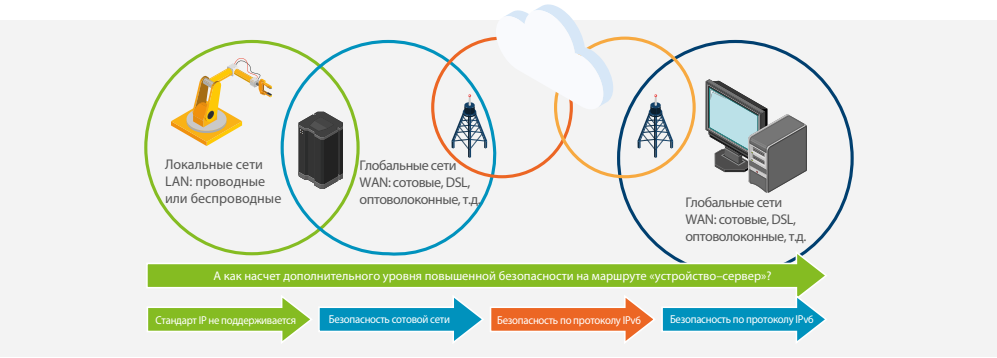
Комплексная безопасность за пределами мира протокола IPv6

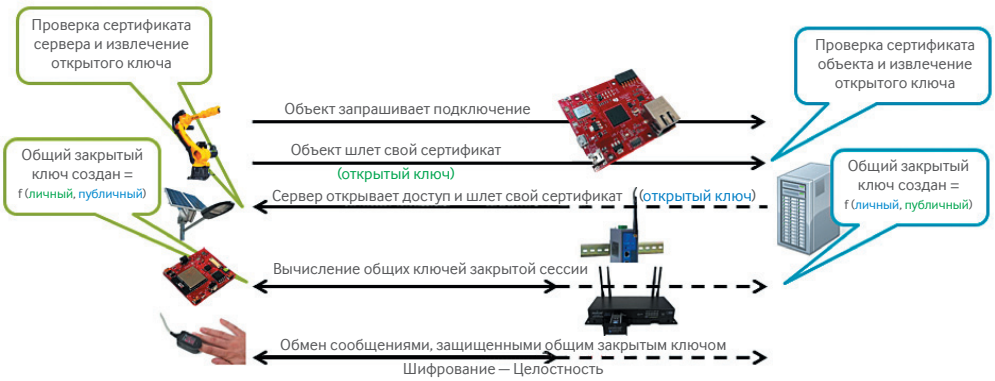
Неужели наш рассказ на этом и закончится? Конечно, нет! Мы ищем способ внедрения дополнительного уровня комплексной безопасности, обозначенного на рисунке зеленым цветом, чтобы он устанавливался поверх систем безопасности остальных участков соединения.

Если у нас есть хотя бы один участок, где не поддерживается стандарт IP, пусть маломощный, с низкой скоростью передачи данных, то он будет являться препятствием для передачи данных по всему пути (мы не забываем, что если IP поддерживается на всем маршруте, как показано выше, то никакой проблемы нет).

Мы предлагаем простое решение: если существующий сигнал IP TLS не может преодолеть это препятствие из-за большого объема данных, мы создаем адаптированный вариант TLS, который включает в себя:

- использование криптографических алгоритмов с более короткими ключами (ECC), а не алгоритмов с длинными ключами (RSA);
- сертификаты меньшего размера;
- увеличенный срок действия ключа сеанса;
- возможность сенсора проверять сертификат сервера офлайн, если требуется;
- безопасный и простой способ персонализировать и хранить сертификаты вместе с ключами сеанса непосредственно на устройстве или сенсоре;
- услуги центра сертификации по выпуску и проверке заказанных сертификатов.





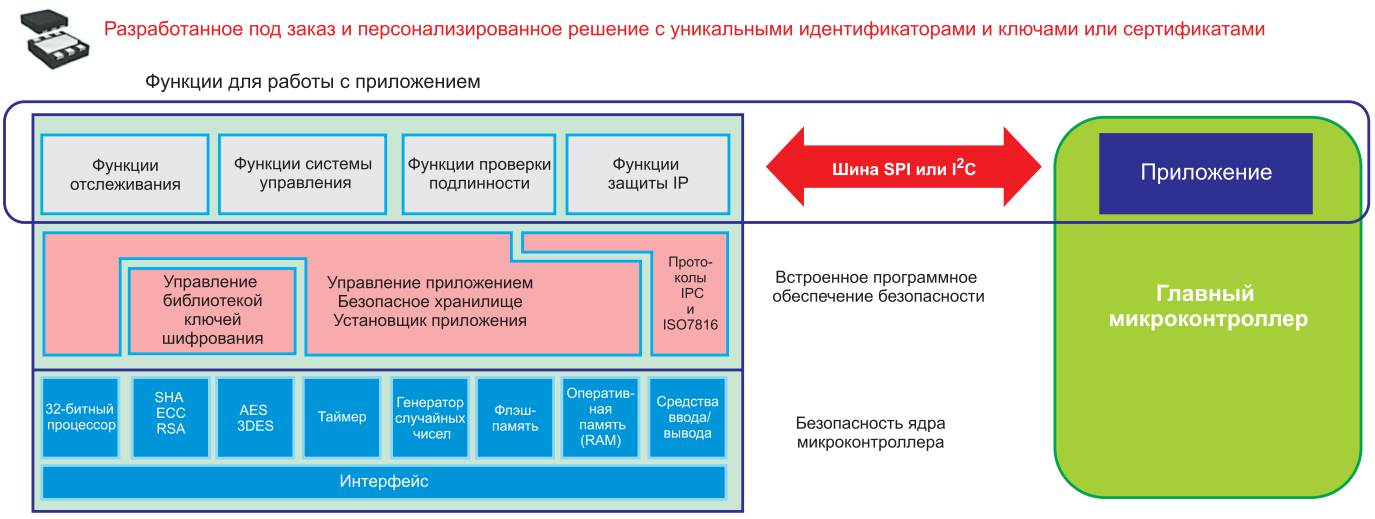
Такой вариант TLS должен выполнять такие же функции, как и исходный:

- взаимная аутентификация;
- простое и автоматизированное выделение ресурсов сенсору или устройству в удаленном приложении;
- механизмы отзыва сенсора или устройства из удаленного приложения;
- обеспечение создания AES ключа сеанса и безопасного обмена с соблюдением при этом целостности и шифрования сообщения.

Хотя многие микропроцессоры могут похвастаться энергоэффективной криптографической начинкой, они не решают реальные проблемы: кто-то должен персонализировать их в какой-то момент, и это создает определенные неудобства. Они не защищены, и закрытые ключи могут быть считаны из их памяти или вычислены по динамическому изменению тока питания или даже по электромагнитному излучению.

Вот почему чипы карт Visa и SIM-карт не используют микроконтроллеры со стандартным ядром типа Cortex-M. И вот почему такие элементы безопасности необходимы.

Эти элементы представляют собой миниатюрные компоненты, соединяющие периферийные устройства с принимающими микроконтроллерами или микропроцессорами, и отвечают за персонализированные сертификаты; безопасное размещение закрытых клю-



чей; управление криптографическими элементами.
Если говорить кратко, все это является частью общего решения по обеспечению безопасной персонализации.
Некоторые итоги в части персонализации подсоединенного устройства
Наша исходная задача состояла в том, чтобы снизить стоимость и уменьшить сложность персонализации и обеспечения ресурсами устройств, сенсоров, машин и механизмов, которые подсоединены к локальным или удаленным серверам. С помощью изменения технологий, упомянутых выше, мы теперь обладаем полным набором решений:

- TLS или им подобные стеки и API (Application Programming Interface — интерфейс программирования приложений), осуществляющие взаимную аутентификацию, распределение и обновление ключей сеанса;
- элементы безопасности, способные принимать сертификаты и управлять исходными функциями TLS;
- обеспечение безопасности в процессе персонализации — элементы защиты перед производством устройства, что исключает необходимость персонализации самого устройства;
- Услуги центра сертификации по выпуску и проверке заказанных сертификатов в течение всего 15-летнего срока службы подсоединенного устройства.

Шлюз

Как правило, шлюз является мостиком, соединяющим локальную сеть LAN и сервер приложения с помощью интернета (сеть IP). Поэтому необходимо провести безопасную идентификацию, как локального сервера, так и удаленного.
С тех пор, как соединение шлюза и сервера осуществляется по IP-протоколу, это может быть сделано с помощью протокола TLS через любое IP-соединение, будь то Wi-Fi, Ethernet или сотовая сеть 3G/4G.
Для такого случая мы рекомендуем использовать элемент безопасности, персонализированный компанией Avnet Silica, как дополнительный чип к главному процессору, работающий под нашей операционной системой UbiquiOS и расположенный в шлюзе. Он обеспечивает бесперебойное TLS-соединение с сервером, который управляется нашими API и выполняет задачу обеспечения шлюза ресурсами по протоколу HTTPS или MQTTS.

IP или 6LoWPAN сенсор

Как было показано выше, сенсоры зачастую работают на аккумуляторах и должны оперировать небольшими по объему данными. Протокол 6LoWPAN является энергоэффективной версией протокола IPv6 и обычно используется в сетевом протоколе Thread™. Это позволяет напрямую соединить сенсор и сервер с помощью протокола TLS.
Для этого варианта мы рекомендуем использовать другой элемент безопасности, персонализированный компанией Avnet Silica, как дополнительный чип к микроконтроллеру сенсора, также работающий под управлением нашей операционной системы UbiquiOS. Он управляет бесперебойным TLS-соединением, обеспеченным шлюзом, с сервером, который управляется нашими API и выполняет задачу безопасного обеспечения сенсора ресурсами по протоколу HTTPS или MQTTS.

Сенсор, не поддерживающий IP

Если сенсор не поддерживает ни IP, ни 6LoWPAN протоколы, то тогда необходимо установить адаптированный под технологию локальной сети вариант TLS непосредственно между сенсором и сервером.
В данном случае мы рекомендуем использовать такой же элемент безопасности, персонализированный компанией Avnet Silica, как дополнительный чип к микроконтроллеру сенсора, работающий под управлением нашей операционной системы UbiquiOS. Отличие в том, что он управляет бесперебойным адаптированным нашей компанией вариантом TLS-соединения, обеспеченным шлюзом, с сервером, который управляется нашими API и выполняет задачу обеспечения сенсора ресурсами с оптимальным балансом между безопасностью и энергопотреблением, в соответствии с механизмами, используемыми в протоколах HTTPS или MQTTS.

Заключение

Компания Avnet Silica и ее партнеры для реализации проектов, касающихся «Интернета вещей», предлагают воспользоваться нашими экспертными знаниями в вопросах персонализации и схем безопасности.
Наша компания является представителем таких широко известных производителей элементов безопасности, как Infineon, STM, Morpho/Trusted Objects, NXP, Maxim и Microchip/Atmel.
В мае 2016 г. мы открыли новый центр персонализации, интегрированный с нашим европейским складом, который расположен в г. Пойнг, неподалеку от Мюнхена.
В настоящее время компания Avnet Silica находится в процессе разработки своих собственных стеков и API. Это позволит управлять адаптированными вариантами TLS и схемами обеспечения ресурсами, работающими на разных протоколах, совместно с технологией UbiquiOS и сервисными службами компании Avnet.
Наша компания вместе с надежным партнером также предлагает услуги сертификационного органа для клиентов, которые не хотят вкладывать собственные средства в создание полной инфраструктуры открытых ключей.
Первая версия этого решения демонстрировалась на выставке «Электроника 2016» (7–10 ноября, г. Мюнхен, Германия).
обновленное решение будет демонстрировалось на выставке “Embedded world 2017” (14-16 марта, г. Нюрнберг, Германия).
Актуальная страница решений на сайте “Avnet-Silica”