DOI: 10.22184/1992-4178.2019.188.7.60.64

Повышение уровня безопасности граничных узлов Интернета вещей с помощью микросхем ATECC608A компании Microchip

Ю. Асангханва[1], Р. Ий[2], А. Сыров[3]

УДК 004.056.5:621.3.049.774 | ВАК 05.13.19

Интернет вещей (IoT) отражает одну из самых больших технологических волн за последние десятилетия. По прогнозам, к 2020 году количество подключенных устройств достигнет 50 млрд, эта технология может затронуть все, что нас окружает. IoT будет охватывать промышленные, коммерческие, медицинские, автомобильные и другие приложения, которые могут повлиять на жизнь миллиардов людей. Учитывая масштаб вовлечения граждан, организаций и систем, критичным компонентом любой IoT-системы следует рассматривать безопасность. Общепризнано, что любой серьезный коммерческий IoT-проект должен включать средства защиты. Рассмотрим ключевые методы обеспечения безопасности граничных узлов IoT-сети и защищенные аппаратные решения компании Microchip для надежного хранения и управления секретными ключами.

ВВЕДЕНИЕ

Оценивая уязвимость IoT-сети, разработчики сосредоточили внимание на самых фундаментальных элементах – граничных узлах. Иначе известные как «вещи» в Интернете вещей, они представляют собой множество датчиков и актуаторов, которые обеспечивают IoT-сеть данными и исполняют команды, полученные из облака или от пользователя, взаимодействующего с ними через компьютер, сотовый телефон, автомобильную систему, интеллектуальное устройство или другую платформу.

Граничные узлы – это, как правило, небольшие недорогие интеллектуальные устройства, которые отличаются очень ограниченными ресурсами. Зачастую ошибочно полагают, что они малоуязвимы для атак. В то время как серверы, к которым устройства обращаются, и сети, которые их соединяют, оснащены проверенными средствами обеспечения безопасности, граничные узлы обычно не защищены, по крайней мере, пока.

Когда речь заходит о защите таких систем, «шифрование» часто отождествляется с термином «безопасность», хотя это лишь один из элементов безопасности. Для создания безопасной среды прежде всего необходимо обнаружить и идентифицировать элементы, подключенные к вашей сети. Сначала нужно определить, кто именно хочет подключиться к сети, потому что без предварительной аутентификации шифрование и защита транспортного уровня (например, протоколы SSL/TLS) позволяют защитить только тех, кто не должен находиться в вашей сети.

Чтобы лучше понять проблематику обеспечения безопасности узла, рассмотрим аналогичный процесс входа в ваш онлайн-банк. Сначала вы устанавливаете безопасное (то есть зашифрованное и аутентифицированное) соединение между вашим компьютером и веб-сайтом банка (представляет собой https-ссылку). Однако этот защищенный канал связи не идентифицирует вас (не подтверждает вашу личность) – он идентифицирует компьютер, создавая шифрованный канал связи между вашим компьютером и банком. На данном этапе банк не отличает вас от злоумышленника. В этот момент вступает в дело ваш пароль – криптографический ключ, который теоретически известен только вам и банку. Как только вы отправили пароль, банк сравнивает его с паролем, хранящемся у него. Если они совпадают, то для банка это доказательство того, что вы именно тот, за кого себя выдаете. Как видно из примера, безопасность онлайн-банкинга обеспечивается на двух уровнях:

- транспортном, который устанавливает защищенное соединение;
- прикладном, который подтверждает (идентифицирует) личность посредством пароля.

[1] Компания Microchip Technology.

[2] Компания Microchip Technology.

[3] Компания ЭЛТЕХ, alexandr.syrov@eltech.spb.ru.

По аналогии безопасность IoT-узла должна быть многоуровневой, если подходить к построению сети Интернета вещей серьезно.

Для IoT-узлов TLS также используется для создания защищенного соединения, например с облаком. Но чтобы быть по-настоящему безопасным, IoT-узел должен получить защиту на уровне приложений. Это означает, что следует идентифицировать сам узел, а не только канал связи. Наряду с идентификацией канала необходимо обеспечить шифрование и целостность данных на уровне приложений для защиты передаваемых данных.

Кроме того, IoT-устройства привносят новую парадигму в сетевое взаимодействие, поскольку они очень компактны и просты, практически не взаимодействуют с человеком. Поэтому в связи с безопасностью IoT-инфраструктуры возникает немало вопросов: «Откуда вы знаете, что IoT-устройство, подключенное к вашей сети, заслуживает доверия?», «Откуда вы знаете, что это IoT-устройство, а не вредоносное оборудование, притворяющееся узлом IoT?» В то же время многие задаются такими вопросами, как: «В чем проблема, если кто-то знает, на какую температуру настроен мой термостат?», «Кому интересно, что мои фары включены?», «Кого волнует, сколько шагов зарегистрировал мой шагомер?»

Если задуматься не только о том, какие данные находятся в устройстве, но и о том, к чему это устройство имеет доступ в сети, проблема становится более существенной. Известен ряд громких нарушений, связанных с несанкционированным доступом к данным путем подмены идентификаторов незащищенных сетевых узлов, когда злоумышленникам удалось проникнуть в сети компаний, притворившись IoT-узлом. Оказавшись внутри сети, где защита намного слабее, они в конечном итоге смогли получить доступ к пользовательской базе данных и нанести ущерб промышленным процессам. Если учесть, что все это в дополнение к доступу к облачным сервисам и потенциальной возможности доступа и управления работой самих узлов, то подтверждение подлинности узла (аутентификация) становится критически важным фактором.

Хотя технологии интернет-безопасности, такие как SSL/TLS, могут хорошо защищать коммуникационные каналы между неповрежденным граничным узлом и сервером, они не являются непреодолимыми. И это не защищает от атак, которые не затрагивают входящую сеть. Очевидно, что SSL/TLS не помогает, если злоумышленник получает контроль над граничным узлом.

Строгие меры безопасности предусматривают три основных элемента (в англоязычной литературе обозначаются аббревиатурой CIA (Confidentiality, Integrity, Authenticity):

- конфиденциальность – данные, хранящиеся или передаваемые в сообщении, должны быть видны только уполномоченным лицам;
- целостность – отправленное сообщение не должно меняться по пути к месту назначения;
- подлинность – нужно быть уверенным, что отправитель сообщения – тот, за кого себя выдает.

Перечисленные элементы основаны на различных технологиях, но самая распространенная – использование секретных или частных ключей, которые служат частью уникального проверяемого идентификационного признака. То, как эти ключи управляются – их хранение и связь, – определяет безопасность системы.

Задача состоит в том, чтобы обеспечить безопасность граничных узлов, оставаясь в узких пределах доступных ресурсов – с точки зрения вычислительной мощности, памяти и энергопитания, а также в рамках бюджета. Цель данной статьи – определить важнейшие стратегии безопасности для граничных узлов, проиллюстрировать роль ключей в любом защищенном решении и описать успешные методы управления ключами.

ПРЕИМУЩЕСТВА КАСКАДНОЙ ИДЕНТИФИКАЦИИ

Как только установлено, что узел или устройство проверено, то есть является доверенным, можно реализовать множество других преимуществ. К ним относятся безопасные коммуникации, контроль экосистемы и безопасное хранение (рис. 1). Когда вы смогли убедиться, что IoT-устройство является тем, за кого выдает себя, можно воспользоваться преимуществами, доступными только в доверительной и безопасной среде.

УЯЗВИМОСТИ ГРАНИЧНОГО УЗЛА: ЧТО МОЖЕТ ПОЙТИ НЕ ТАК?

Прежде чем обсуждать конкретные решения, следует понять, что представляют собой уязвимости, чтобы мы могли обеспечить эффективную защиту. У проблемы два аспекта: определение способов, которыми злоумышленник может нарушить безопасность узла, и понимание последствий таких действий.

Типы атак

Можно выделить четыре способа попадания в граничный узел:

- через сеть;
- через внешние порты;
- посредством бесконтактных атак (Proximity Attack), которые также называют атаками «по боковым каналам»;
- путем физического проникновения в устройство.

Сетевая атака

Сеть – наиболее защищенный порт, однако ее безопасность всего лишь локальная. Незащищенные узлы не могут выжить, надеясь остаться вне поля зрения. Такие

Рис. 1. Многочисленные преимущества становятся доступными для узла, подлинность которого проверена

веб-инструменты, как Shodan, могут сканировать сеть, идентифицируя каждый незащищенный узел. Хотя TLS-защита играет важную роль, могут оставаться тонкие уязвимости из-за ошибок в реализации TLS для граничного узла, плохого использования случайных чисел в крипто-алгоритмах, необнаруженного вредоносного ПО, агрессивных протокольных атак с установленных экспертных узлов и даже из-за слабых мест самих протоколов, как было видно на примере недавно выявленной атакой FREAK.

Даже в идеально защищенной сети злоумышленник может взломать плохо защищенный граничный узел, подделав обновление прошивки и заменив легальное ПО кодом, написанным злоумышленником.

Атака на порты

Сетевой порт (проводной или беспроводной) может быть единственным подключением, доступным на небольшом граничном узле, не использующем ПО. Сложные граничные узлы, однако, могут быть оснащены, например, модульными портами для подключения различных датчиков, USB- или другими (даже беспроводными) портами для подключения периферийных устройств, расходных материалов (например, чернильных картриджей) или для тестирования и отладки оборудования. Каждый порт предоставляет возможность доступа к граничному узлу. Атака может проходить через неиспользуемый порт, можно также удалить и заменить периферийное устройство другим оборудованием, предназначенным для атаки. В отличие от сетевого порта для защиты этих портов не существует установленного стандарта.

Бесконтактная атака

Возможны также сложные атаки без установления соединения с граничным узлом. Подключившись к линии питания или измеряя уровень излучаемых помех либо вибрации на незащищенном устройстве, можно извлечь информацию о ключах. Используя недокументированное поведение или неполадки, например искусственно вызвав скачок напряжения, можно перевести устройство в незарегистрированное незащищенное состояние.

Физическая атака

Злоумышленник может физически разобрать граничный узел, пытаясь исследовать внутренние цепи (с питанием или без питания), или даже удалить и отключить ИС для изучения содержимого встроенной памяти.

Комплексная безопасность должна защищать от всех этих способов атак.

Последствия атак

Конечно, мы защищаем только те объекты, которые, по нашему мнению, представляют ценность. Может казаться, что простой сенсорный узел имеет ограниченную ценность для злоумышленника, но последствия успешной атаки могут подвергнуть риску сеть целиком и все, что подключено к ней.

Взломав граничный узел, даже используя слабые места в системе обеспечения безопасности сети, злоумышленник может получить доступ ко всем секретным данным, которые должна защищать эта система, в частности, к ключам, необходимым для реализации мер безопасности. После изъятия ключей можно обойти все другие средства защиты, включая шифрование и аутентификацию сообщений.

Как только злоумышленник получает контроль над граничным узлом, он может изменить поведение узла в сети, не оповещая сеть о том, что что-то не так. Что касается других серверов, то граничный узел для них все еще остается доверенным объектом, поэтому секретная

информация может вполне добровольно распространяться без опасения, что она попадет в чужие руки.

Утрата секретов может подорвать уверенность клиентов в том, что их финансовые, медицинские, личные и другие данные являются конфиденциальными и защищенными. Это также может нарушить нормативно-правовое регулирование, которое, например в США, связано с вопросами торговли (FTC), медицинской деятельностью (HIPAA/FDA) или финансовыми операциями (SEC/FDIC). Атаки на некоторые сети, такие как системы управления воздушным или дорожным движением, электрические сети, самолеты и автомобили, могут также повлиять на общественную безопасность, а промышленная деятельность может стать ненадежной, если не просто небезопасной.

НАДЕЖНЫЙ СПОСОБ ЗАЩИТЫ ГРАНИЧНОГО УЗЛА

Мы рассмотрели некоторые из множества способов, которыми можно взломать граничные узлы. Помешать этим атакам может ряд мер, связанных с хранением ключей. Хотя 100%-ных гарантий безопасности не бывает, эти меры обеспечивают наилучшую возможную защиту и гарантируют, что злоумышленник не сможет определить критические системные ключи. Каждый из этих подходов поддерживает важные элементы CIA:

- подлинность – подтверждайте личность любого посетителя, заходящего в сеть;
- подлинность – идентифицируйте любые дополнительные устройства, которые пытаются подключиться к узлу;
- конфиденциальность – шифруйте сообщения;
- целостность – добавляйте код идентификации сообщений (MAC) ко всем сообщениям, чтобы подтвердить, что никто не изменил сообщение по маршруту.

Кроме того, могут быть приняты меры защиты от бесконтактных атак (атак «по боковым каналам»), которые носят практический характер и могут быть реализованы во всей системе или только в основной подсистеме.

- Храните ключи в защищенном оборудовании, чтобы не было электрического доступа к ключу.
- Экранируйте систему, чтобы предотвратить утечку ключевой информации путем детектирования электромагнитного излучения.
- Добавьте специальные схемы для того, чтобы предотвратить попытки контроля над питанием или другими сигналами. Это могут быть фиктивные счетчики или схемы со встроенными элементами генерирования случайных сигналов для шифрования полезной информации.
- Зашифруйте ключ в хранилище. Даже если ключ недоступен с электрической точки зрения, злоумышленник может попытаться физически вскрыть устройство, чтобы прочитать встроенную флеш-память и извлечь ключ. Шифрование нейтрализует эту атаку.
- По возможности откажитесь от внешних портов. Например, может показаться полезным наличие порта отладки, но если есть вероятность того, что он не будет использоваться, то ваша система будет более защищенной без него.

Также крайне важно защищать ключи в течение всего производственного процесса. Необходима хорошо продуманная система, которая сохраняет ключи в секрете от момента их генерации до помещения в устройство хранения ключей. Проверенная методология – использование аппаратных модулей безопасности (HSM), которые хранят ключи в зашифрованном виде и в защищенном оборудовании.

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ КЛЮЧЕЙ

Компания Microchip предлагает ряд криптографических решений в виде специальных устройств – криптоэлементов. Поскольку эти устройства функционируют как аппаратные криптоускорители, основное внимание часто уделяется их использованию для разгрузки хост-процессора от выполнения сложных математических операций. Есть другой, более важный, аспект их применения: в криптографических операциях используются ключи, поэтому они должны храниться в хорошо защищенных устройствах, гарантирующих, что ключи не будут видны так, как если бы вы попытались выполнить те же вычисления в ПО или в незащищенном оборудовании.

Новейший криптоэлемент Microchip ATECC608A CryptoAuthentication представляет собой микросхему на основе схем с коррекцией ошибок, которая соответствует соглашению о ключах ECDH4, оснащена встроенными функциями асимметричной аутентификации на основе ECDSA5 и защищенным аппаратным хранилищем секретных ключей – самым надежным из существующих (рис. 2).

ATECC608A идеально подходит для обеспечения безопасности граничных IoT-узлов, поскольку оснащена как ECDSA-, так и ECDH-алгоритмами. Добавление компактной микросхемы ATECC608A в любую систему с микроконтроллером, в том числе в IoT-узлы, позволяет легко и эффективно обеспечить конфиденциальность, целостность и аутентификацию в этой системе.

Интегрировать ATECC608A в систему вместе с любым микроконтроллером можно при очень небольших затратах. Однопроводные или I^2C-интерфейсы сводят к минимуму количество выводов, опционально можно выбрать корпус, габариты которого составляют всего 2×3 мм. Ток потребления в режиме сна не превышает 150 нА.

Криптоэлементы исполняют алгоритмы внутри схемы, принимая входные данные от процессора, и возвращают

результаты вычислений (то есть подпись, аутентификацию, сеансовые ключи и т. д.), не раскрывая способ вычислений. Высококачественный генератор истинных случайных чисел (TRNG) помогает предотвратить повтор транзакции. Внутренний серийный номер гарантирует уникальность ключа, а для отслеживания сеансов аутентификаций предусмотрены счетчики большой емкости.

Можно предложить следующие физические и криптографические контрмеры, которые не позволят злоумышленнику проанализировать работу устройства, чтобы получить ключи.

- Все устройство нужно экранировать сеточным рисунком металлизации, которая препятствует детектированию внутренних сигналов по электромагнитному излучению и обеспечивает визуальную защиту против тех, кто вскрывает корпус для исследования работы устройства. Экран должен быть электрически соединен с остальной частью схемы – в случае его повреждения устройство больше не будет работать, что не позволит злоумышленнику исследовать узлы схемы.
- Можно использовать стабилизаторы напряжения и счетчики так, чтобы замаскировать шины питания и сигналы схемы.
- Исключить внутренние контактные площадки для тестирования и отладки, чтобы не было дополнительных точек доступа к схеме.

Важное преимущество криптоэлементов Microchip заключается в том, что обеспечение защиты в процессе производства упрощается благодаря применению простых модулей (доступных от компании Microchip), которые гарантируют безопасное введение секретной информации и подписанных сертификатов в эти микросхемы.

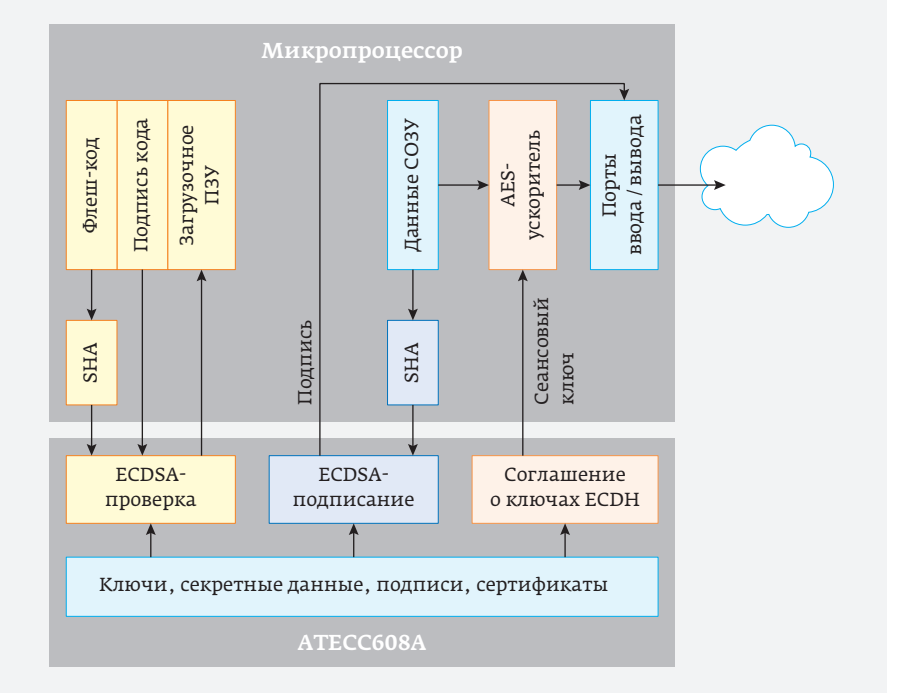

Рис. 2. ATECC608A работает совместно с любым микропроцессором для обеспечения конфиденциальности, целостности данных и аутентификации

ЗАКЛЮЧЕНИЕ

Безопасность имеет основополагающее значение для успешного развертывания сети Интернета вещей. Граничные узлы в настоящее время являются самым слабым звеном в обеспечении безопасности IoT. Защита криптографических ключей позволяет блокировать доступ к граничным узлам. Лучший способ добиться надежной блокировки – защищенное оборудование. Это единственный метод сохранения ключей и других секретных данных подальше от посторонних глаз. Семейство микросхем Microchip CryptoAuthentication – надежное средство хранения ключей в защищенном оборудовании и управления этими ключами для обеспечения многоуровневой защиты. Широкая номенклатура микроконтроллеров, беспроводных устройств и криптоэлементов от Microchip позволяет реализовать интеллектуальное и безопасное подключение устройств к сети IoT и не только.

ЛИТЕРАТУРА

1. The Search Engine for the Internet of Things // Shodan, 2015, www.shodan.io
2. FREAK // Wikipedia, September 5, 2015, http://en.wikipedia.org/wiki/FREAK
3. Smarter Security For Your Everything, Atmel Has You Covered // Microchip, 2019, https://www.microchip.com/design-centers/security-ics
4. **Boldt B.** ECDH Key Exchange is Practical Magic // SemiWiki.com, October 28, 2014, www.semiwiki.com/forum/content/3966-ecdh-key-exchange-practical-magic.html
5. **Boldt B.** The ABCs of ECDSA // Atmelcorporation.wordpress.com, August 6, 2014, https://atmelcorporation.wordpress.com/2014/08/06/the-abcs-of-ecdsa-part-1/
6. **Boldt B.** Is the Internet of Things Just a Toy? // SemiWiki.com, March 1, 2015, https://semiwiki.com/semiconductor-manufacturers/4146-is-the-internet-of-things-just-a-toy/

Testing&Control

22–24 октября 2019
Москва, Крокус Экспо

16-я Международная выставка испытательного и контрольно-измерительного оборудования

testing-control.ru

- Измерительное и метрологическое оборудование
- Оборудование для лабораторного контроля
- Испытательное оборудование
- Оборудование для неразрушающего контроля и технической диагностики
- Производственный контроль и машинное зрение
- Системы диагностики и мониторинга

Получите бесплатный электронный билет по промокоду **technosphera19**

Организатор

Международная Выставочная Компания

+7 (495) 252 11 07
control@mvk.ru