ОСОБЕННОСТИ АУТЕНТИФИКАЦИИ В СИСТЕМАХ IoT

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Руденко Н.С.

Власова Г.А. – к.т.н., доцент

В работе рассматриваются основные факторы, которые необходимо учитывать при разработке протокола аутентификации в системах интернета вещей (англ. *Internet of Things, IoT)*. Рассматриваются алгоритмы шифрования, пригодные для использования в системах IoT. А также известные уязвимости таких систем.

Стремительное развитие микроэлектронной промышленности и информационных технологий сделало возможным повсеместное внедрение практических решений для реализации концепции интернета вещей. Так как масштабы использования IoT постоянно растут – возникает необходимость обеспечения информационной безопасности в системах, использующих такую концепцию. Однако, так как устройства, используемые в таких системах, не обладают достаточной вычислительной мощью, для их защиты необходимо использовать криптографические алгоритмы, стойкость которых снижается незначительно, в отличие от объема требуемых ресурсов, которые называются алгоритмами легковесной (lightweight) или малоресурсной криптографии. Возникают серьезные требования к конфиденциальности, когда речь заходит о домашней автоматизации, поскольку она генерирует огромное количество персонализированных данных. По прогнозам Gartner, к 2022 году в домохозяйстве будет задействовано более 500 смарт-устройств для каждого домохозяйства, поэтому поставщикам необходимо серьезнее относиться к конфиденциальности и безопасности.

В настоящее время наиболее «легковесными» являются алгоритмы асимметричной криптографии, работающие с эллиптическими кривыми (ECC – Elliptic Curves Cryptography). Типичными значениями параметров различных процессоров, предназначенных для вычислений с эллиптическими кривыми, являются величины в пределах 10-40μW и 10,000-20,000 GE. Близкими к ним являются и значения параметров у процессоров, предназначенных для вычислений с гиперэллиптическими кривыми (HECC – Hyper Elliptic Curves Cryptography). Таким образом, по сравнению с симметричной криптографией, асимметричная криптография с безопасной длиной ключа, реализованная на аппаратном уровне, по прежнему требует значительно больших ресурсов (по крайней мере, 10000 дополнительных логических элементов), при этом реализуется вполне приемлемая скорость работы. Для криптографии с открытым ключом верхняя граница на размер микросхемы устанавливается в 15,000 GE. Что касается программной реализации, то тщательная оптимизация алгоритмов позволяет микроконтроллерам выполнять операции ассиметричной криптографии менее чем за 1 секунду, что вполне достаточно для большинства приложений. При этом программно-аппаратная реализация, по-видимому, создаёт наилучший баланс между размером и скоростью для многих распространенных вычислительных приложений.

Одним из самых распространенных стандартов, применяемых в устройствах интернета вещей является ZigBee. Однако в последние несколько лет устройства, использующие его, многократно подвергались успешным атакам со стороны исследователей и злоумышленников, что дает повод для сомнений в надежности данного стандарта. Проблема слабой защищенности ZigBee создана вендорами, увязшими в погоне за продажами. Некоторые поставщики не думают о безопасности и реализуют минимум функций, требуемых для сертификации. На Def Con 23 Тобиас Зилнер отметил, что для безопасности важно выполнить следующие предварительные приготовления на стороне производителя:

- Обнаружение подделки: “Устойчивый к несанкционированному использованию узел может стереть конфиденциальную информацию, включая ключи безопасности, если обнаружено несанкционированное вмешательство”.
- Транспортировка ключей: «TC-ключ по умолчанию не должен использоваться, поскольку этот ключ считается общедоступным и, следовательно, обеспечивает тот же уровень безопасности, что и незашифрованный транспорт ключей».
- Создание ключа: «Мастер ключи, используемые при создании ключа, должны быть распределены по внеполосным каналам». Это может быть достигнуто с помощью такого простого решения, как например наклейка с мастер ключом, наклеенная на устройство.
- Смена ключей: «Безопасность связи зависит от секретности сетевого ключа и ключей связи. Сетевой ключ должен периодически меняться. Управление ключами должно быть реализовано в форме изменения сетевого ключа в определенный период времени или после ввода определенного количества сообщений. В противном случае могут быть осуществимы многие атаки на безопасность».

Список использованных источников:

1. Жуков Алексей Евгеньевич. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. 2015. №1.
2. Tobias Zillner. ZIGBEE EXPLOITED. The good, the bad and the ugly // Режим доступа: https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf