Е.А. Суханова, А.В. Шаброва, О.В. Ниссенбаум

Тюменский государственный университет, г. Тюмень

УДК 004.056

УЯЗВИМОСТИ В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ НА ПРИМЕРЕ ПЛАТФОРМЫ FIWARE

Аннотация. FIWARE представляет концепцию Интернета будущего, предоставляя библиотеки для работы с разнородными устройствами, объединяя их в единую сеть. Однако, данная система имеет ряд уязвимостей: отсутствие доверия к издателям сертификатов ключей и протоколов, отсутствие юридической защиты пользователя и производителя «умных» вещей, отсутствие защиты передаваемой между устройствами информации.

Ключевые слова: FIWARE, Интернет вещей, доверие к сертификатам, ABE, юридическая безопасность.

Введение

Концепция Интернета будущего набирает обороты в странах Европы, и этому есть ряд причин: упрощение работы с разнородными устройствами, возможность собирать и обрабатывать информацию с множества устройств в реальном времени для прогнозирования, выведения статистики и работы бизнес-процессов. В дальнейшем концепция FIWARE и ей подобные будут только набирать обороты, однако данная концепция имеет ряд уязвимостей.

Доверие к сертификатам

В [1] рассматривается схема взаимодействия издателя, пользователя и владельца службы. В данной схеме ни владелец службы, ни пользователь не защищены от издателя сертификатов, подтверждающего учётные данные. Издатель может помочь злоумышленнику получить доступ к службе или вызвать отказ в обслуживании у добросовестного пользователя. Ассиметричное шифрование позволяет убедиться в подлинности издателя, но не в его надёжности. Концепция Интернета будущего предлагает для пользователя SSO (единый вход для многих сервисов), однако доверять

крупному сертификационному центру не всегда целесообразно, особенно, если данный центр не контролируется законодательством, например, находясь за пределами доверенного государства. Вызвав отказ в обслуживании, данный центр может парализовать на время работу множества компаний, поэтому концепция Интернета будущего не применима без чётких юридических рамок для издателей, предоставляющих заверенные учётные данные для множества различных сервисов.

«Умные» вещи и их возможности

«Умные» вещи имеют малый запас памяти и вычислительных мощностей, однако существует множество «лёгких» шифров, таких как Present-80 и MIBS-8, Khudra и SKINNY, которые, несмотря на попытки взлома[2;3;4,5], остаются стойкими к атакам. В концепции FIWARE «умные» вещи общаются через единый шлюз, обладающий большими вычислительными мощностями, однако данный подход требует дополнительных затрат и КЗ между данным устройством и датчиками, что не всегда достижимо. На данный момент легковесные симметричные шифры и атрибутно-основанное шифрование (Attribute-Based Encryption, ABE) позволяют осуществлять защиту, однако, как было отмечено в [6], такое шифрование не может быть использовано при обновлении прошивки, так как устройство не сможет с достаточной надёжностью убедиться в подлинности издателя прошивки. С другой стороны, атрибутно-основанное шифрование привлекает внимание разработчиков, поскольку предоставляет возможность осуществлять гибкий контроль доступа на основе атрибутов. Также такой вид шифрования удобен в системах, где есть множество различных устройств (датчиков), генерирующих данные, и такое же множество устройств, обрабатывающих эти данные. Это объясняется тем, что одно сообщение, зашифрованное на определенном множестве атрибутов, могут расшифровать сразу несколько получателей, имеющих соответствующий для расшифровки атрибутный набор. Это упрощает взаимодействие устройств, поскольку не требует обмена ключами между каждыми сторонами общения.

Необходимость государственного регулирования

Данная проблема была рассмотрена в контексте Интернета вещей в [7]. В контексте же Интернета будущего проблема намного глубже.

Сейчас всё больше Российских сервисов делают аутентификацию через google+, так как это не отвлекает клиентов на регистрацию и просто во внедрении. Однако такие компании и их ресурсы зависят от сторонней фирмы, что не является безопасным и может повлечь отказ в обслуживании. Похожая ситуация и с концепцией Интернета будущего, сервисы которого будут глубже интегрироваться в нашу жизнь: в медицину, транспорт, продажи, поэтому отказ в обслуживании таких сервисов может принести колоссальный ущерб. Из этого следует необходимость государственного регулирования, как служб, которые предоставляют ресурсы, так и издателей. Например, целесообразно было бы обязать сервисы заверять аутентификационные данные на территории Российской Федерации, а также контролировать издателей, которые заверяют такие данные.

На данный момент IoT устройства не имеют под собой крепкого юридического основания, производители таких устройств стараются экономить на их содержании. Такая тенденция может привести к атакам на данные устройства, как на самые уязвимые, и внедрение червя с целью выведения из строя как можно большей части сети. Также не до конца определены виновные в случае инцидента, размеры компенсаций и фонды для выплат при таких инцидентах для производителей. Допустим, производитель произвёл устройство, которое было взломано и в результате было повреждено огромное количество устройств, подобный инцидент приведёт к банкротству, поэтому государство должно обязывать производителей вносить в стоимость устройства сумму, из которой будет формироваться фонд для выплат в случае инцидентов.

Выводы

Для защиты сетей в быстроразвивающейся концепции взаимодействия устройств Интернета будущего необходимо государственное регулирование,

накладывающее ограничения, как на издателя, так и на тех, кто предоставляет сервисы. А также нужна доработка законодательства об ответственности лиц в случае инцидентов, связанных с «умными» вещами. Также требуется иметь к «умным» вещам особый подход и отдельные протоколы для работы, чтобы охватить больший круг возможностей.

СПИСОК ЛИТЕРАТУРЫ

1. FIWARE.OpenSpecification.Security.Privacy Generic Enabler [Электронный ресурс] // forge.fiware.org: информ.-справочный портал. URL: https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Security.Privacy_Generic_Enabler, свободный (дата обращения: 15.03.2018).

2. Abed F., Forler C., List E., Lucks S., and Wenzel J. Bi-clique cryptanalysis of present, led, and klein /Abed F., Forler C., List E., Lucks S., and Wenzel J. //Cryptology ePrint Ar-chive: Report 2012/591– 2012.

3. Sereshgi F., Dakhilalian M., Shakiba M. Biclique cryptanalysis of MIBS□80 and PRESENT□80 block ciphers //Security and Communication Networks. – 2016. – Т. 9. – №. 1. – С. 27-33.

4. Yang Q., Hu L., Sun S., Song L. Related-key impossi-ble differential analysis of full khudra //International Workshop on Security. – Springer International Publishing, 2016. – С. 135-146.

5. Tolba M., Abdelkhalek A., Youssef A. M. Impossible Differential Cryptanalysis of Reduced-Round SKINNY /Tolba M., Abdelkhalek A., Youssef AM. //Cryptology ePrint Archive: Report 2016/1115– 2016.

6. Ronen E., Shamir A., Weingarten A. O., O'Flynn C. IoT goes nuclear: Creating a ZigBee chain reaction //Security and Privacy (SP), 2017 IEEE Symposium on. – IEEE, 2017. – С. 195-212.

7. Shamir A., Biryukov A., Perrin L. P. Summary of an Open Discussion on IoT and Lightweight Cryptography //Proceedings of Early Symmetric Crypto workshop, 2017. – University of Luxembourg, 2017.