К.Ю. Пономарев, О.В. Ниссенбаум
Тюменский Государственный Университет, г. Тюмень

УДК 004.056

ИНТЕРНЕТ ВЕЩЕЙ: ПРОБЛЕМЫ КОНТЕКСТНО-ОРИЕНТИРОВАННОГО КОНТРОЛЯ ДОСТУПА

Аннотация. В статье рассматриваются вопросы, связанные с безопасностью в сетях Интернета вещей. Говорится о значимости контекста устройств, проблемах, возникающих при использовании контекста для построения системы контроля доступа - проверке подлинности контекста и распределении ключей. Приводится модель верификации атрибутов контекста.

Ключевые слова. Контроль доступа, шифрование на основании атрибутов, Интернет вещей, криптографические протоколы.

Введение. Интернет вещей (англ. Internet of Things, IoT) – динамическая глобальная сетевая инфраструктура с возможностью самонастройки на основе стандартных и совместимых протоколов связи, где физические и виртуальные вещи имеют идентификаторы, физические атрибуты, используют интеллектуальные интерфейсы и интегрируются в информационную сеть [1]. Система IoT может быть представлена как совокупность взаимодействующих интеллектуальных устройств. Можно привести следующие примеры внедрения IoT: система производственного контроля (анализ данных от датчиков температуры, выбросов углерода, влажности, шума, вибрации и т.д.), интеллектуальная система мониторинга энергопитания, динамическое планирование маршрута для доставки товаров, промышленная автоматизация [2]. Пристальное внимание в таких системах уделяется вопросам информационной безопасности. Традиционные решения по защите информации, принятые в обычных информационных системах и Интернете, не подходят для внедрения из-за свойств IoT: ограничений на вычислительную

мощность, большого количества устройств и соответствующей проблемы масштабируемости, высокой разнородности систем, иных функциональных задач.

Существенную роль в обеспечении контроля доступа и функционировании IoT играет контекст или окружение, в котором находятся устройства. Под контекстом понимаются: характеристики окружающей среды (температура, влажность, шум и т.д.), местоположение, время, пользователь, системные данные и т.п. Главной особенностью контекста является динамичность, то есть изменение его характеристик с течением времени. Приведём пример: в случае чрезвычайной ситуации все, кто рядом с пострадавшими, могут получить доступ к данным о группе крови, но только врачебный персонал может получить полную медицинскую информацию.

В работе [3] была представлена идея: использовать значения контекста в криптографических преобразованиях, например, в шифровании на основании атрибутов (англ. Attribute Based Encryption, ABE), для построения моделей контроля доступа.

Шифрование на основе атрибутов. Кратко опишем принцип функционирования ABE. В системе определено множество атрибутов, по которым регулируется доступ к информации. Каждое передаваемое сообщение обладает неким набором значений атрибутов. В ключе каждого пользователя зашифровано дерево доступа, указывающее значения набора атрибутов. Проверяется соответствие между значениями атрибутов ключа и данных. Если атрибуты пакета удовлетворяет ключу пользователя, то он может расшифровать сообщение. Такой подход носит название Key Policy (KP-ABE). Ключи пользователям выдаёт единый доверенный центр, он же проверяет подлинность значений атрибутов, то есть что пользователи действительно ими обладают. Другая методика Cipher text Policy (CP-ABE): дерево доступа шифруется в пакет данных, а ключ пользователя включает в себя атрибуты проверки. Подробное построение ABE-модели, начиная со схемы разделения секрета, приведено в [4].

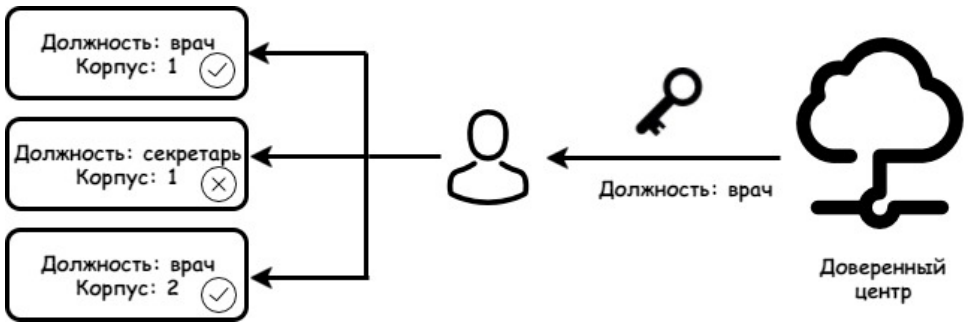

Рис. 1. KP-ABE

Верификация атрибутов. Рассмотрим следующую модель шифрования на основании атрибутов: свойства окружения или некоторые характеристики устройств будут считаться атрибутами доступа. В соответствии со своим контекстом, устройства будут получать доступ только к определённым сообщениям. Например, в медицинских системах в качестве атрибутов могут выступать жизненные показатели пациентов, их местоположение, гражданство и т.д. В классических ABE-схемах секретный ключ, содержащий дерево доступа, каждому узлу выдаётся доверенным центром (англ. Attribute Authority) заранее. В сетях IoT изменения контекста происходят часто, а значит необходимо динамически обновлять ключи устройств.

Целесообразно поставить следующий вопрос: как определять подлинность атрибутов, или точнее говоря изменений контекста? Для верификации атрибутов шифрования можно ввести два дополнительных узла: супервайзер (Supervisor, SV) и центр сертификации (англ. Certification Authority, CA). Супервайзер – лицо или центр, обладающее полномочиями на изменение атрибутов устройств. Таких сущностей в системе может быть несколько, причем каждый из них может обладать различными правами. Например, возможно задать ограничения на диапазоны устройств, видов и значений атрибутов, которые уполномочен изменять данный супервайзер. Супервайзер регистрируется в центре сертификации, который хранит данные о правах этого супервайзера относительно атрибутов устройств. При регистрации SV и CA вырабатывают общий секретный ключ для аутентификатора.

Процесс изменения атрибутов устройства происходит в предлагаемом протоколе, использующем алгоритмы цифровой подписи (S), аутентификатор (англ. Message Authentication Code, MAC), и применяются следующие обозначения:

- $attr_{old}$, $attr_{new}$ – старые и новые атрибуты устройства соответственно;
- MAC(x) – аутентификатор SV под сообщением x;
- S(x) – цифровая подпись CA под сообщением x.

Протокол изменения контекста состоит из следующих шагов.

1. Изменился контекст, в котором находится устройство – необходимо получить новый секретный ключ, чтобы читать сообщения, предназначенные для новых атрибутов. Устройство посылает супервайзеру наборы старых и новых значений атрибутов и подпись центра сертификации под старыми.
2. Супервайзер проверяет подлинность изменений, он также уполномочен отвечать устройству отказом. В случае принятия изменений контекста устройства, супервайзер отсылает CA старый и новый наборы атрибутов устройства, подпись CA под старыми атрибутами и аутентификатор, вычисленный им на секретном ключе, под новыми атрибутами.
3. Каждый супервайзер ограничен набором прав, в пределах которых он может изменять или подтверждать изменения атрибутов. Если супервайзер превысил свои полномочия, CA отвечает отказом. Иначе он подписывает набор атрибутов и передаёт новые атрибуты и подпись устройству.
4. Далее, по логике KP-ABE, устройство предъявляет атрибуты доверенному центру, AA также проверяет под ними подпись CA.
5. Наконец AA отправляет устройству новый секретный ключ.

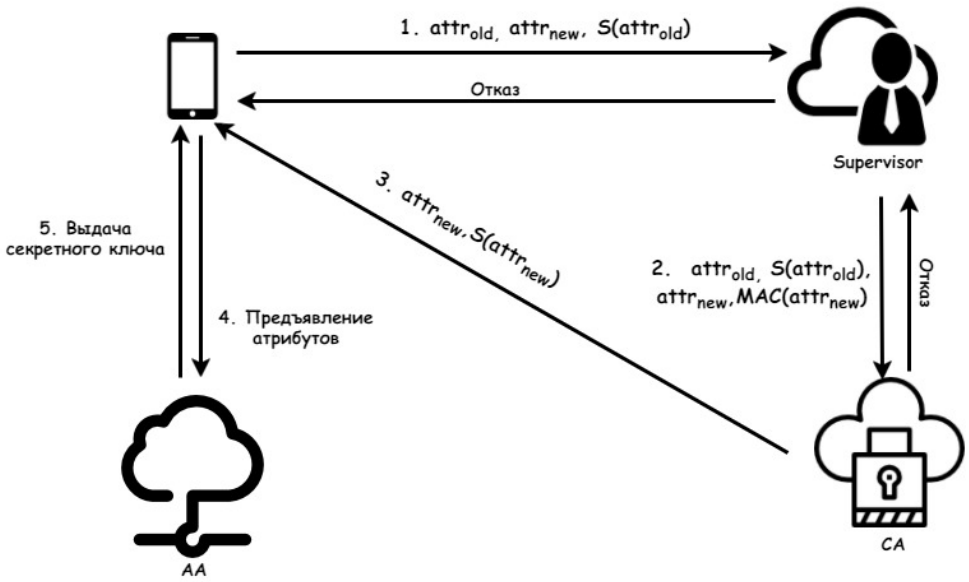

Рис. 2. Схема верификации атрибутов с супервайзером

Отметим, что данную схему можно делать децентрализованной, когда в системе присутствует несколько центров сертификации. В таком случае можно применять метод кросс-сертификации. Также за разные множества атрибутов могут отвечать различные доверенные центры, тогда идёт построение MA-ABE (англ. Multi-authority) схем. Заметим, что в предложенной схеме набор атрибутов становится известным третьим лицам: центру сертификации и супервайзеру. Ограничения на чтение атрибутов могут быть полезны в системах, в которых циркулируют медицинские или персональные данные.

Протокол Отвея-Рииса. В связи с частым обновлением контекста не остаётся без внимания вопрос о передаче секретного ключа от центра к устройству. Проблемы распределения ключей в распределённых системах IoT, в частности в беспроводных сенсорных сетях (англ. Wireless Sensor Networks, WSN), были рассмотрены в [5]. В работе были проанализированы два подхода: криптография на основе отрытых ключей (public key cryptography) и общих, заранее распределённых, ключей (pre-shared keys). Оба становятся неэффективными при большом количестве узлов в системе. По мнению авторов, первый способ может быть жизнеспособным решением, когда соединения происходят время от времени. Причиной этому является вычислительная сложность. Второй способ применим в маленьких

приложениях, так как ключи должны быть предварительно загружены в узлы перед стартом работы. Таким образом следует обратить внимание на возможность использования третьей доверенной стороны для передачи ключа, содержащего новое дерево доступа (KP-ABE) или же сами атрибуты (CP-ABE).

Опишем процесс передачи ключа с использованием протокола Отвея-Рииса. Он является криптографическим симметричным протоколом обмена ключами с использованием доверенной стороны (англ. Trusted Authority, TA). Будем считать, что каждый узел системы и каждый AA имеют свой общий секретный ключ с TA.

Таблица. 1. Используемые обозначения

N	Узел, который запрашивает новый ключ при изменении контекста
AA	Доверенный центр, отвечающий за раздачу ключей на основе атрибутов
TA	Доверенный центр, отвечающий за обмен ключами между AA и N
I	Идентификационный номер сессии
E	Симметричный алгоритм шифрования
S	Подпись супервайзера, верифицирующего контекст и набор атрибутов
attr	Набор атрибутов и их значений
R	Случайное число
K	Сеансовый ключ

1. Устройство отправляет AA номер сессии, сгенерированное псевдослучайное число и зашифрованные на общем с TA ключе набор атрибутов и подпись супервайзера.

$$N \rightarrow AA: I, N, AA, E_N(R_n, attr_{new}, S(attr_{new}), I, N, AA)$$

2. Центр атрибутов передаёт полученное шифрованное сообщение ТА, а также шифрует на их общем ключе своё псевдослучайное число.

$$AA \rightarrow TA: I, N, AA, E_N(R_n, attr_{new}, S(attr_{new}), I, N, AA), E_A(R_A, I, N, AA)$$

3. ТА расшифровывает полученные сообщения, извлекает параметры (I, N, AA) и проверяет их равенство с теми, что были переданы в открытом виде. Если значения не совпадет он должен прервать протокол или направить запрос на повторную отправку. Также он генерирует общий сеансовый ключ для N и AA. Из сообщения от N он извлекает атрибуты и подпись и передаёт их AA.

$$TA \rightarrow AA: I, E_N(K, R_n, attr_{new}), E_A\big(K, R_A, attr_{new}, S(attr_{new})\big)$$

4. На данном шаге AA проверяет равенство полученного случайного числа сгенерированному, проверяет номер сессии и подпись супервайзера под атрибутами. Далее он формирует по полученным атрибутам новый ключ схемы шифрования на основе атрибутов. Передаёт его N симметричным шифром с использованием полученного от ТА сеансового ключа. Здесь AA может удостовериться, что ТА именно тот, за кого себя выдаёт – иначе он бы не смог расшифровать сообщение и вернуть тоже псевдослучайное число.

$$AA \rightarrow N: I, E_N(K, R_n, attr_{new}), E_K(K_{ABE})$$

5. Устройство расшифровывает сообщения. С помощью сеансового ключа извлекает ключ, содержащий дерево доступа (KP-ABE) или же сами атрибуты (CP-ABE). Также необходимо проверить на соответствие предыдущим значениям набор атрибутов. N удостоверяется, что ТА именно тот, за кого себя выдаёт, проверив псевдослучайное число. Можно отправить AA сообщение о доставке.

Заключение. Мы рассмотрели две проблемы, возникающие при использовании контекстно-ориентированного подхода для шифрования на основе атрибутов: подлинность контекста и распределение ключей. Были описаны модели решения: верификация атрибутов супервайзером и

использование протокола с доверенного центра. Заметим, что в обоих случаях атрибуты становятся известны третьей стороне: супервайзеру или доверенному центру. Такая ситуация может быть недопустимой, например, в системах с медицинскими или персональными данными.

СПИСОК ЛИТЕРАТУРЫ

1. Internet of Things Global Standards Initiative [Электронный ресурс]. – Режим доступа: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (дата обращения: 02.04.2017).
2. Куприяновский, В.П. Интернет Вещей на промышленных предприятиях / В.П. Куприяновский, Д.Е. Намиот, В.И. Дрожжинов, Ю.В. Куприяновская, М.О. Иванов // International Journal of Open Information Technologies. – 2016. – vol. 4, № 12.
3. Lee, J. A Work in Progress: Context based encryption scheme for Internet of Things / J. Lee, S. Oh, J. Wook Jang // The 10th International Conference on Future Networks and Communications. – 2015.
4. Chase, M. Multi-authority Attribute Based Encryption // Proceedings of the 4th Theory of Cryptography Conference. – 2007. – pp. 515 – 534.
5. Rodrigo, R. Key management systems for sensor networks in the context of the Internet of Things / R. Rodrigo, C. Alcaraz, J. Lopez, N. Sklavos // Computers and Electrical Engineering. – 2011. - № 37. – pp. 147-159.