Кирилл Юрьевич Пономарев,
аспирант кафедры информационной безопасности,
Тюменский государственный университет

РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. Статья посвящена описанию протокола распределения ключей для схем шифрования на основании атрибутов. Данная модель может найти применение для построения механизмов контроля доступа в сетях Интернета вещей. При использовании контекста устройств в качестве атрибутов контроля доступа, возникает проблема частой передачи секретного ключа. В качестве решения описывается протокол передачи ключа с использованием доверенной стороны.

Ключевые слова: Интернет вещей, шифрование на основании атрибутов.

Abstract. In this paper key distribution protocol for attribute-based encryption schemes was described. This model can be used in access control mechanisms for the Internet of Things. Problem of frequent secret key transmission appears using device context as attributes of access control. With the purpose of solving this problem key exchange protocol with trusted third party was described.

Key words: The Internet of things, encryption-based attributes.

Интернет вещей (англ. Internet of Things, IoT) — концепция современных информационных систем, в которой физические предметы имеют средства для взаимодействия друг с другом и устройствами вычислительных сетей. Можно привести следующие примеры использования IoT: отслеживание поставок материалов с помощью RFID-меток, измерение датчиками уровня кислорода в шахтах, оплата покупок электронными средствами, «умный дом» и др.

Большую роль в обеспечении контроля доступа играет контекст или окружение, в котором находятся устройства. Под контекстом понимаются: характеристики окружающей среды, время, пользователь, системные данные. В работе [1] была высказана идея: использовать значения контекста в криптографических преобразованиях, например, в шифровании на основании атрибутов (англ. Attribute Based Encryption, ABE).

Впервые ABE-схемы были рассмотрены в статье [2]. При построении систем с ABE шифрованием определяется множество атрибутов, по которым регулируется доступ к информации. Каждое передаваемое в системе 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 выдает 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.

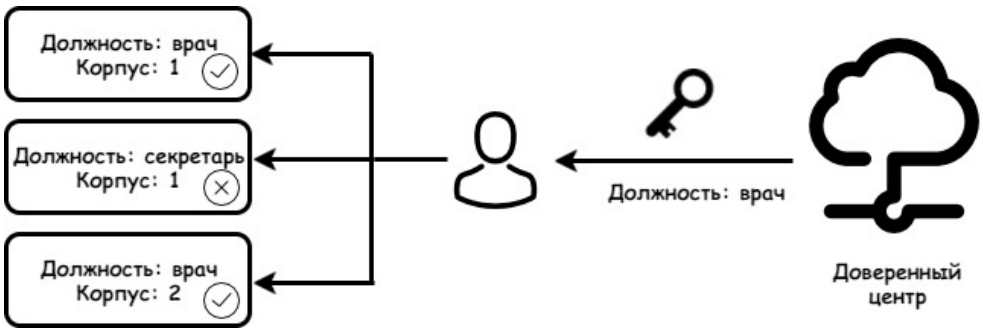

Рис. 1. KP-ABE

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 определенным 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 выдается доверенным центром (англ. Attribute Authority) заранее. В сетях IoT изменения контекста происходят часто, а значит необходимо динамически обновлять ключи устройств.

Проблемы распределения ключей в распределенных системах IoT, в частности в беспроводных сенсорных сетях (англ. Wireless Sensor Networks, WSN), были рассмотрены в [3]. В работе были проанализированы два подхода: криптография на основе отрытых ключей (public key cryptography) и общих, заранее распределенных, 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 [4]. 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. Далее будем предполагать, что AA имеет некий механизм проверки подлинности нового набора атрибутов, а их передачу инициирует само устройство.

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
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.

$$N \to AA : I, N, AA, E_N(R_n, attr_{пвw}, I, N, AA).$$

2. Центр атрибутов передает полученное шифрованное сообщение TA, а также шифрует на их общем ключе свое псевдослучайное число.

$$AA \to TA : I, N, AA, E_N(R_n, attr_{пвw}, I, N, AA), E_A(R_A, I, N, AA).$$

3. TA 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 передает их AA.

$$TA \to AA : I, E_N(K, R_n, attr_{пвw}), E_A(K, R_A, attr_{пвw}).$$

4. На данном шаге AA проверяет равенство полученного случайного числа сгенерированному ранее, проверяет номер сессии. Далее он формирует по полученным атрибутам новый ключ схемы шифрования на основе атрибутов. Передает его N симметричным шифром с использованием полученного от TA сеансового ключа. Здесь AA может удостовериться, что TA именно тот, за кого себя выдает — 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 TA именно тот, за кого себя выдает, проверив псевдослучайное число. Можно отправить AA ответное сообщение о доставке.

В работе был рассмотрен протокол распределения ключей с доверенным центром. Заметим, что атрибуты становятся известны третьей стороне, доверенному центру. Такая ситуация может быть недопустимой, например, в системах с медицинскими или персональными данными.

СПИСОК ЛИТЕРАТУРЫ

1. 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.
2. Sahai, A. Fuzzy Identity-Based Encryption / A. Sahai, B. Waters // Advances in Cryptology V Eurocrypt. — 2005. — P. 457-473.
3. 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. — P. 147-159.
4. Otway, D. Efficient and Timely Mutual Authentication / D. Otway, O. Rees // Operating Systems Review. — 1987. — V. 24, № 1. — P. 8-10.