Методы аутентификации для архитектуры Интернета вещей

УДК 004.056

С.В. ШЕВЕЛЕВ, доцент НИУ МГСУ кандидат технических наук, Д.С. ФЕДЧЕНКОВ, магистр МТУСИ

Методы аутентификации для архитектуры Интернета вещей
The Authentication Methods for the IoT Architectures

Интернет вещей состоит из большого количества связанных объектов, которые обмениваются данными друг с другом. Чтобы поддерживать надежную связь между взаимодействующими объектами IoT, должны применяться эффективные процедуры аутентификации. В статье проведен обзор наиболее популярных на сегодняшний день методов аутентификации IoT. Представлено сравнение этих методов по их устойчивости к распространенным сетевым атакам.

The Internet of Things consists of a large number of connected objects that exchange data with each other. In order to maintain reliable communication between interacting IoT objects, effective authentication procedures must be applied. The article provides an overview of the most popular IoT authentication methods to date. A comparison of these methods in terms of their resistance to common network attacks is presented.

Ключевые слова: Интернет вещей, методы аутентификации, сетевые атаки, архитектуры Интернета вещей.
Keywords: *Internet of Things, authentication methods, network attacks, IoT architectures.*

Введение

В начале 1990-х годов словом “Интернет” стали обозначаться технологии, соединяющие компьютеры по всему миру с помощью проводных или беспроводных коммуникаций. С тех пор Интернет эффективно используется для обмена файлами, просмотра веб-страниц, ведения электронного бизнеса, социальных сетей и т. д. [1]. Развитие и внедрение интеллектуальных технологий вызвали повсеместное соединение вещей друг с другом. Все это свидетельствует о необходимости разработки более сложных технических решений для поддержки новой связи “машина — машина” (M2M, Machine-to-Machine) [2]. Интернет вещей (IoT) был представлен как будущее Интернета для развития нового мира подключенных объектов.

Поскольку IoT является частью Интернета, он должен гарантировать безопасность. Аутентификация является важным фактором, побуждающим людей использовать новые технологии и безопасно получать доступ к различным ресурсам IoT. Пользователи не захотят делиться своими данными и личной информацией, если не гарантированы схемы защиты для предотвращения угроз безопасности. Следовательно, для широкого и быстрого развертывания IoT необходимы эффективные методы безопасности и аутентификации [3].

В данной статье представлены различные методы аутентификации для Интернета вещей в облачной среде и для устройств с ограниченными ресурсами. Также проведено сравнение методов на основе их безопасности.

Проблемы безопасности аутентификации в многоуровневой архитектуре Интернета вещей

Интернет вещей состоит из миллиардов связанных между собой объектов: датчиков, исполнительных механизмов, встроенных устройств, традиционных компьютеров, смартфонов и т. д. Для управления связью между различными объектами традиционные интернет-протоколы TCP/IP, такие как протокол передачи гипертекста (HTTP), транспортный протокол (TCP), не эффективны при поддержке связи M2M.

Основные цели транспортного уровня — гарантировать доставку пакетов и выполнять сквозное управление перегрузкой. В обычном понимании Интернета протокол, используемый на транспортном уровне для надежной связи, — это протокол управления передачей (TCP). Очевидно, что TCP не подходит для Интернета вещей по следующим причинам:

настройка подключения. TCP ориентирован на подключение, и каждый сеанс начинается с процедуры настройки соединения (так называемое трехстороннее рукопожатие). В этом нет необходимости, учитывая, что большая часть коммуникаций в IoT будет включать обмен небольшими объемами данных, и, следовательно, этап настройки будет длиться значительную часть времени сеанса. Кроме того, на этапе настройки подключения данные должны обрабатываться и передаваться на оконечные устройства, которые в большинстве случаев ограничены как с точки зрения энергии, так и с точки зрения ресурсов связи, таких как узлы датчиков и метки RFID;

Статью целиком читайте в бумажной версии журнала