СПбГУТ)))
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
Сентябрь 2016 Том 4 № 3 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
September 2016 Vol. 4 Iss. 3 ISSN 2307-1303 http://www.itt.sut.ru

ИССЛЕДОВАНИЕ МЕТОДОВ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

К. Н. Данилов[1], В. А. Кулик[1], Р. В. Киричек[1*]

[1] СПбГУТ, Санкт-Петербург, 193232, Российская Федерация
* Адрес для переписки: kirichek@sut.ru

Аннотация
Предмет исследования. Методы идентификации и аутентификации устройств Интернета Вещей. **Метод.** Сравнительный анализ существующих системы идентификации DOI и URI. **Основные результаты.** Согласно проведенному анализу показано, что наиболее подходящей системой, используемой для идентификации цифровых объектов в глобальной сети, является система DOI. **Практическая значимость**. Результаты анализа могут быть использованы для выбора методов идентификации и аутентификации устройств Интернета Вещей в различных приложениях.
Ключевые слова
Интернет Вещей, DOI, URI, идентификация, аутентификация.

Информация о статье
УДК 004.725.7
Язык статьи – русский.
Поступила в редакцию 15.06.16, принята к печати 26.08.16.

Ссылка для цитирования: Данилов К. Н., Кулик В. А., Киричек Р. В. Исследование методов идентификации и аутентификации устройств Интернета Вещей // Информационные технологии и телекоммуникации. 2016. Том 4. № 3. С. 49–57.

REVIEW AND ANALYSIS OF METHODS OF IDENTIFICATION AND AUTHENTICATION OF THE INTERNET OF THINGS DEVICES

K. Danilov[1], V. Kulik[1], R. Kirichek[1*]

[1] SPbSUT, St. Petersburg, 193232, Russian Federation
* Corresponding author: kirichek@sut.ru

Abstract—Research subject. Methods of identification and authentication devices, the Internet of Things. **Method.** A comparative analysis of the existing DOI and URI identification system. **Core results.** According to the analysis showed that the most suitable system used to identify digital objects in the global network is the DOI system. **Practical relevance.** The results of the analysis can be used to select the methods of identification and authentication of the Internet of Things devices in various applications.
Keywords—Internet of Things, DOI, URI, identification, authentication.

Article info
Article in Russian.
Received 15.06.16, accepted 26.08.16.

For citation: Danilov K., Kulik V., Kirichek R.: Review and analysis of methods of identification and authentication of the Internet of Things devices // Telecom IT. 2016. Vol. 4. Iss. 3. pp. 49–57 (in Russian).

Введение

В настоящее время одной из самых дискуссионных проблем развития сетей связи пост-NGN являются проблемы идентификации устройств Интернета Вещей (ИВ). Данные проблемы обуславливаются невозможностью обнаружения и контроля устройствами ИВ современными методами, применяемыми для поиска устройств в сети связи общего пользования (ССОП) [1, 2, 3]. Современные методы анонимизации и предполагаемое огромное число устройств Интернета Вещей подключенных к ССОП [4, 5], делают современные системы связи уязвимыми перед злоумышленниками. Уязвимость безопасности, заключающейся в невозможности аутентификации устройства Интернет Вещей, открывает для злоумышленников возможность для производства контрфактной физической и виртуальной продукции.

Одним из направлений обеспечения гарантированной аутентификации устройств ИВ является использование уникального идентификатора устройства ИВ в ССОП, в совокупности с системой аутентификации данной реальной или виртуальной вещи в ССОП. В связи с этим одной из самых важных проблем является выбор системы идентификации для всех устройств ИВ, подключенных к ССОП. В качестве уникального глобального идентификатора предлагается множество различных программных и аппаратных решений. В частности, в качестве аппаратных идентификаторов предлагаются системы аппаратной идентификации MAC, IPv6, IPv4+MAC, IMEI и др. Данные системы представляют собой пример аппаратных идентификаторов устройств ИВ, но обладают рядом недостатков, в частности:

– возможность программного изменения идентификатора сетевого интерфейса (MAC, IMEI и др.);

– возможность генерации пакетов, благодаря которым возможно взаимодействие контрафактных устройств ИВ с сервисами ИВ, что приводит к угрозе похищения личных данных пользователя (MAC, IPv6, IPv4+MAC и др.) [2, 3, 4];

– привязка к аппаратным идентификаторам исключает возможность идентификации цифровых объектов устройств ИВ.

В связи с данными недостатками предлагаются альтернативные программные решения для идентификации такие как DOI, URI, XRI, IRI и др. Данные системы позволяют идентифицировать любой виртуальный или реальный объект

в ССОП, вне зависимости наличия или отсутствия сетевого интерфейса. Тем не менее данные системы, так же, как и системы аппаратной идентификации, не подразумевают аутентификацию объектов без использования различных сторонних технологий.

В данной статье исследуются системы идентификации DOI и URI, их архитектура, структура идентификаторов и методы аутентификации.

Идентификатор URI

URI (*Uniform Resource Identifier* – унифицированный идентификатор ресурсов) – последовательность символов, определяющие какой-либо абстрактный или физический ресурс, как в ССОП, так и в локальной сети [6]. Используется для доступа к определенному интернет-ресурсу (веб-ресурсу), с помощью системы DNS.

URI составлен из набора символов, состоящих из цифр, букв и нескольких графических символов. Данные символы используют кодировку ASCII. Символы в URI делятся на зарезервированные и незарезервированные. Зарезервированное символы используются для разграничения незарезервированных символов, используемые в качестве идентификатора ресурса или объекта.

Зарезервированные символы делятся на два типа:

– gen-delims, они же выступают основными «разделителями», т. е. символами, разделяющие URI на компоненты. Пример: ":", "/", "?", "#", "[", "]", "@";

– sub-delims, они же «подразделители» – символы, которые разделяют текущий крупный компонент, на более мелкие составляющие, определяемые ресурсом. Пример: "!", "$", "&", "'", "(", ")", "*", "+", ",", ";", "=";

В незарезервированные символы входят:

{символы}, {числа}, "-", ".", "_", "~",

где {символы} – любая буква верхнего и нижнего регистров с кодировкой ASCII (A-Z, a-z),

{числа} – любая цифра (0–9).

Комбинация зарезервированных и незарезервированных символов составляет URI-адрес. Адрес URI состоит из следующих компонентов:

1) Scheme (схема) – начальный набор символов для URI, отвечающий за формат следующих за схемой компонентов. Название схемы обязательно начинается с буквы и далее может быть продолжено любым количеством разрешенных символов.

Разрешенные символы для схемы:

{символы}, {числа}, "+", "-", "."

2) Authority (авторизация) – компонент, следующий за компонентом схема и используемый для определения ресурса обращения. Данный компонент начинается с двойного слеша (//) и заканчивается слешем (/), знаком вопроса (?) или октоторпом (#) или концом URI.

Авторизация состоит из:

[userinfo "@"] host [":" port],

где в квадратных скобках указаны опциональные компоненты.

3) Path (путь) – компонент, содержащий пути данные, организованные в иерархической форме, которые, вместе с данными в неиерархическом компоненте запроса (Query), служит для идентификации ресурса в рамках схемы URI и компонента авторизации (если данный компонент указан). Путь начинается со слеша (/) и заканчивается знаком вопроса (?), октоторпом (#) или концом URI.

Разрешенные символы для пути:

Незарезервированные, процентно-кодированные, sub-delims, ":", "@"

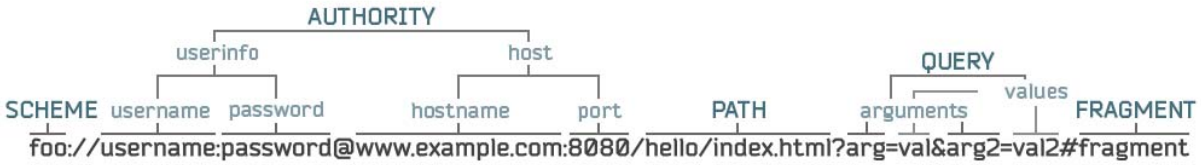

Рис. 1. Структура идентификатора URL

4) Query (запрос) – неиерархический компонент, используемый в совокупности с иерархическими данными компонента путь для идентификации ресурса в рамках системы URI. Разрешенные символы для запроса:

Незарезервированные, процентно-кодированные, sub-delims, ":", "@", "/", "?"

В запросе чаще всего передаются данные в формате key=value (ключ=значение).

5) Fragment (фрагмент) – компонент, используемый для идентификации подресурса обращения относительно ресурса. Семантика фрагмента никак не ограничена, фрагмент начинается октоторпом(#) и заканчивается концом URI, при этом может состоять из абсолютно любого набора символов.

В качестве примера на рис. 1 приведена структура идентификатора URL. Аутентификация для данной системы идентификации реализуется с помощью защищенных протоколов передачи данных, использующих центры сертификации (*Certification authority*), например, https, sftp и др.

Идентификатор DOI

DOI (*Digital Object Identifier* – цифровой идентификатор объекта) – система идентификации цифровых объектов в ССОП[1] [7]. Цифровой объект – это структурированные данные, которым присвоен уникальный идентификатор – хэндл (handle). Handle system (система резолюции) связывает эти идентификаторы с информацией о состоянии цифровых объектов. Создатель объекта или авторизованный администратор предоставляет эту информацию с исполь-

[1] ГОСТ Р ИСО 26324-2015. Система стандартов по информации, библиотечному и издательскому делу. Система дискретных идентификаторов объекта. 2016.

зованием инфраструктуры ассиметричного шифрования, которая интегрирована в DOI. Данная система основана на концепции системы указателей (*Handle System*), предполгающей идентификацию не отправляемой информации (пакета), а самих объектов взаимодействия, именуемых цифровыми объектами. Цифровой объект – это представление какого-либо устройства, либо данных в цифровом формате в ССОП. В настоящее время система DOI используется для идентификации публикаций в ССОП.

ПО Handle System, отвечающее за организацию локального сервиса, содержащего данные о продукции, является условно-бесплатным ПО, доступным для пользователя, при условии регистрации и получения номера авторизации – префикса. Использование префиксов гарантирует отсутствие дублирования идентификаторов.

Базовая архитектура DOI состоит из трех компонентов:

1) Digital Object Repository (репозиторий цифровых объектов) – это хранилище, используемое для хранения и доступа к информации о цифровых объектах цифровым объектам, при помощи уникального идентификатора;

2) Handle System (система резолюции) – система преобразования идентификатора в хэндлы, содержащие информацию о искомом объекте. В данных хэндлах хранится различная информация о объекте, например, физическое или логическое местонахождение объекта, наименование, тип, свойства объекта, публичные ключи шифрования и др. Данная система состоит из двух уровней резолюции:

– GHR – *global handle registry* (глобальный реестр);

– LHR – *local handle registry* (локальный реестр).

При установке локального сервиса (LHS) создается пара ключей, публичный отправляется в GHR (частный храниться в LHR), а сервису выделяется префикс и права на изменение записей.

3) Digital Object Registry (система реестров) – используется для создания коллекций цифровых объектов и регистрации объектов, информация о которых может храниться в множестве различных реестров. Используется для поиска ранее зарегистрированных объектов. Результатами такого поиска является список данных, содержащих различные данные о объекте и номер последней транзакции о изменении данных объекта.

В последних версиях реализации системы DOI репозитории и реестры объединены. В каждом репозитории хранится реестр объектов, а каждый реестр использует репозиторий для хранения данных собственных объектов.

На рис. 2 изображена архитектура системы DOI. Идентификация цифрового объекта происходит следующим образом:

– пользователь (либо пользовательское устройство) производит запрос на получения информации о товаре (например, с помощью механизма преобразования идентификатора URI в DOI), с помощью имеющегося открытого идентификатора DOI;

– данный запрос обрабатывается сервисом GHR, который отправляет запрос в систему реестров, затем в репозиторий, где находиться информация о LHR отвечающих за запрашиваемый цифровой объект;

– данная информация отправляется пользовательскому устройству, которое устанавливает защищенное соединение с сервисом LHR, при помощи алгоритмов ассиметричного шифрования;

– после обработки данного запроса LHR отправляет данные об объекте пользовательскому устройству.

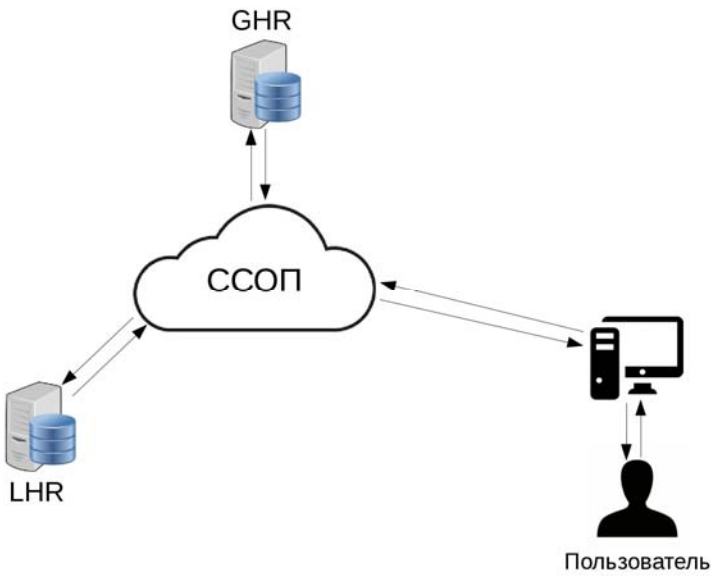

Рис. 2. Архитектура системы идентификации DOI

Идентификатор DOI состоит из префикса производителя, который хранится в GHR, разделительного символа «/» и постфикса продукта, хранящегося в LHR и состоящего из произвольного набора символов (рис. 3). Для обнаружения цифрового объекта в ССОП, возможно использование как программных интерфейсов доступа (API), так и с помощью интрефейса преобразования URI запроса в DOI. Для запроса информации о цифровом объекте через систему URI, в начало комбинации префикс-постфикс необходимо добавить строку: http://www.doi.org/{идентификатор DOI}.

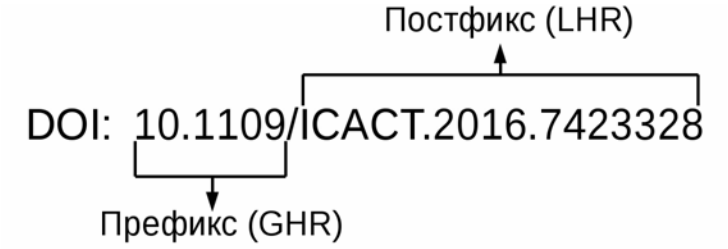

Рис. 3. Формат идентификатора DOI

Аутентификация для данной системы идентификации реализуется с помощью защищенных протоколов передачи данных, использующих центры сертификации (*Certification authority*), например, https, sftp и др.

Сравнение идентификаторов URI и DOI

Для сравнения систем идентификации DOI и URI необходимо определить требования к системам идентификации и определить соответствие данные систем по данным критериям.

Для систем идентификации цифровых объектов в ССОП можно выделить следующие критерии [7]:

– каждый объект в ССОП должен иметь один или более идентификаторов;

– идентификаторы должны обнаруживаться в ССОП, при этом должна быть обеспечена совместимость с основными технологиями сети Интернет: IP, WWW, URI и др.;

– идентификаторы должны отвечать на множественные запросы. Идентификатор может указывать на различные местоположения объекта в зависимости от типа данных о нем;

– для работы с идентификаторами необходимы различные уровни доступа. Процесс регистрации идентификаторов должен проходить под контролем доверительных центров, имеющих повышенные требования к политикам безопасности и уровни разграничения прав для пользователей центра;

– информация должна храниться отдельно от цифрового объекта. То есть информация должна быть доступна по запросу для любого пользователя в ССОП;

– идентификатор не должен содержать динамические элементы или данные о цифровом объекте.

На основе данных требований к системе идентификации цифровых объектов возможно провести анализ систем DOI и URI на их соответствие (табл.).

Таким образом, согласно вышеприведенным требованиям наиболее подходящей системой, используемой для идентификации цифровых объектов в глобальной сети, является система DOI.

Таблица

Анализ систем DOI и URI на соответствие требованиям
к системам идентификации цифровых объектов

Требования к системе	**Система URI**	**Система DOI**
Каждый объект в ССОП должен иметь один или более идентификаторов	В системе URI один ресурс может иметь один и более идентификаторов, которые присваиваются ресурсу с помощью системы доменных имен (DNS). Тем не менее данная система не возвращает идентификационной информацию о ресурсе после запроса	Система DOI может присваивать несколько идентификаторов для каждого объекта. После запроса идентификации система возвращает информацию о объекте
Идентификаторы должны обнаруживаться в ССОП	Система URI используется DNS для однозначного нахождения ресурса по его идентификатору. Данная система полностью совместима с основными технологиями ССОП	Для обнаружения цифрового объекта в ССОП, возможно использование как программных интерфейсов доступа (API), так и с помощью интрефейса преобразования URI запроса в DOI. Для запроса информации о цифровом объекте через систему URI, в начало комбинации префикс-постфикс необходимо добавить строку: http://www.doi.org/{идентификатор DOI}. Данная система имеет совместимость с основными технологиями ССОП

Требования к системе	Система URI	Система DOI
Для работы с идентификаторами необходимы различные уровни доступа	Сервера DNS, используемые идентификаторами URI, являются одними имеют высокий уровень безопасности и систему авторизации пользователей	Сервера Handle System, используемые являются одними имеют высокий уровень безопасности и систему авторизации пользователей
Информация должна храниться отдельно от цифрового объекта	Идентификатор URI не содержит информации о ресурсе. Система URI не предполагает возврат информации о ресурсе по запросу	Идентификатор DOI не содержит информации о цифровом объекте. Система DOI предполагает возврат информации об идентифицируемом объекте при процессе идентификации. Данная информация хранится в репозитории цифровых объектов
Идентификатор не должен содержать динамические элементы или данные о цифровом объекте	Идентификатор URI может содержать в строке запроса как динамические данные, так и данные о ресурсе	Идентификатор DOI не содержит динамические данные или данные о цифровом объекте

Заключение

В данной статье были исследованы системы идентификации DOI и URI, их архитектура, структура идентификаторов и методы аутентификации. Были определены требования к системам идентификации цифровых объектов в ССОП, и на основе данных требований было проведено сравнение систем DOI и URI друг с другом. В результате сравнения было установлено, что DOI является более предпочтительной системой для идентификации в ССОП.

В дальнейшем планируется провести исследование возможности применения идентификационной системы DOI для аутентификации устройств Интернета Вещей, на базе модельной сети лаборатории Интернета Вещей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича [8, 9, 10].

Литература

1. Данилов К. Н., Киричек Р. В., Кулик В. А. Методы обнаружения интернет вещей в глобальной сети // Информационные технологии и телекоммуникации. 2015. № 4. С. 48–56. URL: http://www.sut.ru/doci/nauka/review/4-15.pdf

2. Киричек Р. В., Кулик В. А., Владыко А. Г., Богданов И. А., Кучерявый А. Е. Ложные облака для интернета вещей. Методы защиты // Информационные технологии и телекоммуникации. 2015. № 3. С. 27–39. URL: http://www.sut.ru/doci/nauka/review/3-15.pdf

3. Kirichek R., Kulik V., Koucheryavy A. False clouds for Internet of Things and methods of protection // 18th International Conference on Advanced Communication Technology (ICACT). 2016. pp. 201–205.

4. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.

5. Evans D. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. CISCO White Papers. 2011.

6. Berners-Lee T., Fielding R., Masinter L. RFC 3986. Uniform Resource Identifier (URL): Generic Syntax. URL: https://www.ietf.org/rfc/rfc3986.txt

7. Цифровая идентификация объектов: технология и не только / Под ред. М. А. Медриша. М.: Научное обозрение, 2016. 228 с. ISBN 978-5-9906425-4-6.

8. Kirichek R., Koucheryavy A. Internet of Things Laboratory Test Bed // Lecture Notes in Electrical Engineering. 2016. Vol. 348. pp. 485–490. DOI: 10.1007/978-81-322-2580-5_44.

9. Kirichek R., Vladyko A., Zakharov M., Koucheryavy A. Model Networks for Internet of Things and SDN // 18th International Conference on Advanced Communication Technology (ICACT). 2016. pp. 76–79.

10. Киричек Р. В., Владыко А. Г., Захаров М. В., Кучерявый А. Е. Модельные сети для Интернета Вещей и программируемых сетей // Информационные технологии и телекоммуникации. 2015. № 3. С. 17–26. URL: http://www.sut.ru/doci/nauka/review/3-15.pdf

References

1. Danilov, K. N., Kirichek, R. V., Kulik, V. A. Methods for Detection of Internet of Things in the Global Network // Telecom IT. 2015. No. 4. pp. 48–56. URL: http://www.sut.ru/doci/nauka/review/4-15.pdf

2. Kirichek, R. V., Kulik, V. A., Vladyko, A. G., Bogdanov, I. A., Koucheryavy, A. E. False Clouds for Internet of Things. Methods of Protection // Telecom IT. 2015. No. 3. pp. 27–39. URL: http://www.sut.ru/doci/nauka/review/3-15.pdf

3. Kirichek, R., Kulik, V., Koucheryavy, A. False Clouds for Internet of Things and Methods of Protec-tion // 18th International Conference on Advanced Communication Technology (ICACT). 2016. pp. 201–205.

4. Koucheryavy, A. E. Internet of Things // Electrosvyaz'. 2013. No. 1. pp. 21–24.

5. Evans, D. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. CISCO White Papers. 2011.

6. Berners-Lee, T., Fielding, R., Masinter, L. RFC 3986. Uniform Resource Identifier (URL): Generic Syntax. URL: https://www.ietf.org/rfc/rfc3986.txt

7. Digital Object Identifiers: Not Only Technology / Edited by M. A. Medrish. M.: Nauchnoe Obozrenie, 2016. 228 p. ISBN 978-5-9906425-4-6.

8. Kirichek, R., Koucheryavy, A. Internet of Things Laboratory Test Bed // Lecture Notes in Electrical Engineering. 2016. Vol. 348. pp. 485–490. DOI: 10.1007/978-81-322-2580-5_44.

9. Kirichek, R., Vladyko, A., Zakharov, M., Koucheryavy, A. Model Networks for Internet of Things and SDN // 18th International Conference on Advanced Communication Technology (ICACT). 2016. pp. 76–79.

10. Kirichek, R. V., Vladyko, A. G., Zakharov, M. V., Koucheryavy, A. E. Model Networks for Internet of Things and SDN // Telecom IT. 2015. No. 3. pp. 17–26. URL: http://www.sut.ru/doci/ nauka/review/3-15.pdf

Данилов Кирилл Николаевич – магистрант, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, kirill1994danilov@yandex.ru

Кулик Вячеслав Андреевич – ассистент, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, vaklicr@gmail.com

Киричек Руслан Валентинович – кандидат технических наук, доцент, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, kirichek@sut.ru

Danilov Kirill – undergraduate, SPbSUT, St. Petersburg, 193232, Russian Federation, kirill1994danilov@yandex.ru

Kulik Vyacheslav – assistant, SPbSUT, St. Petersburg, 193232, Russian Federation, vaklicr@gmail.com

Kirichek Ruslan – Ph.D., associate professor, SPbSUT, St. Petersburg, 193232, Russian Federation, kirichek@sut.ru