DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.1.3

УДК 004.4
ББК 32.973.2

ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ IPv6 ДЛЯ «ИНТЕРНЕТА ВЕЩЕЙ» С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александра Владимировна Власенко

Кандидат технических наук, доцент,
и.о. заведующего кафедрой компьютерных технологий и информационной безопасности,
Кубанский государственный технологический университет
Alex_Vlasenko@list.ru
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Алексей Алексеевич Мусиенко

Студент,
Кубанский государственный технологический университет
alexmus97@gmail.com
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Аннотация. Данная работа посвящена набирающей популярность концепции Интернета вещей. Проанализированы возможности, а также уязвимости Интернета вещей. В результате работы выявлено, что применение интернет-протокола версии 6 разрешит многие проблемы данной концепции, в том числе и связанные с обеспечением безопасности.

Ключевые слова: Интернет вещей, интернет-протокол версии 6, безопасность, Умный дом.

Интернет вещей (англ. *Internet of Things*, далее IoT) – концепция вычислительной сети физических предметов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

Интернет вещей состоит из слабо связанных между собою разрозненных сетей, каждая из которых была развернута для решения своих специфических задач. К примеру, в современных автомобилях работают сразу несколько сетей: одна управляет работой двигателя, другая – системами безопасности, третья поддерживает связь и т. д. В офисных и жилых зданиях также устанавливается множество сетей для управления отоплением, вентиляцией, кондиционированием, телефонной связью, безопасностью, освещением. По мере развития Интернета вещей эти и многие другие сети будут подключаться друг к другу и приобретать все более широкие возможности в сфере безопасности, аналитики и управления. В результате Интернет вещей приобретет еще больше возможностей открыть человечеству новые, более широкие перспективы.

По данным мировых аналитиков, на начало 2016 г. в использовании технологий Ин-

тернета вещей компании ориентируются в первую очередь на массовые сегменты IoT, где побуждением конечных пользователей к использованию решений и сервисов IoT являются рыночные стимулы, такие как:

– решения для создания интеллектуальных сервисов безопасности (Умный дом);

– решения для создания интеллектуальных сервисов оптимизации использования ресурсов домохозяйствами.

Интернет вещей набирает большую популярность благодаря тому, что многие устройства значительно упрощают быт, обеспечивают безопасность, повышают комфорт.

Внедрение нового интернет-протокола версии 6 (далее – IPv6) внесет большой вклад в развитие Интернета вещей [1–3]. Существует несколько уникальных особенностей IPv6, которые подтолкнут IoT вперед.

1. Ограниченность адресного пространства IPv4 являлась одной из главных проблем протокола. В свою очередь, IPv6 предоставляет $3{,}4 * 10^{38}$ уникальных адресов, что позволяет подключить к Интернету практически неограниченное число устройств.

2. В шестой версии интернет-протокола значительно упрощен заголовок пакетов. Были убраны поля, отвечающие за фрагментацию дейтаграмм, следовательно, IPv6 снижает нагрузку на маршрутизаторы, а также и на устройства Интернета вещей.

3. Революцией в IPv6 стала технология EUI-64. Данная технология позволяет присвоить IPv6-адрес, основываясь на MAC-адресе устройства. Благодаря EUI-64 нет необходимости в использовании дополнительных протоколов, отвечающих за присвоение IP-адресов устройствам.

Доступность всех устройств IoT из глобальной сети заставляет обратить внимание на безопасность. Например, в ноябре 2016 г. преступники сумели отключить отопление в домах города Лаппеенранта в Финляндии, заставив контроллеры постоянно перезапускать сеть. Атаке была подвергнута и сеть общественного транспорта Сан-Франциско. Киберпреступникам удалось взломать автоматизированную систему по продаже билетов, в результате чего в течение суток пассажиры смогли ездить на автобусах и троллейбусах города бесплатно. Автоматы на станциях при этом транслировали надпись «Не работает», а на ПК сотрудников компании поступали сообщения о взломе с требованием выкупа.

И снова на помощь приходит IPv6. В редакции (RFC 4294) технических условий узла IPv6 поддержка IPsec стала обязательной.

IPsec (сокращение от IP Security) – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и шифрование IP-пакетов.

Отличительной чертой IPv6 является поддержка протокола CGA. Данный механизм позволяет создать уникальный IPv6-адрес, который считается невозможным подменить за разумное время, не зная всех параметров, на основании которых генерируется CGA.

Главная идея протокола CGA состоит в том, чтобы создать идентификатор интерфейса (правые 64 бита) IPv6-адреса при помощи вычисления криптографического хэша публичного ключа устройства. Затем приватный ключ может быть использован для подписи исходящих от устройства сообщений.

Для того чтобы проверить подпись, получателю необходимо знать: исходный адрес, публичный ключ и значения дополнительных параметров. Данный протокол позволит исключить возможность злоумышленника удаленно подключиться к какому-либо устройству, повышая безопасность Интернета вещей.

СПИСОК ЛИТЕРАТУРЫ

1. Власенко, А. В. Разработка алгоритмов и программ выбора оптимального набора компонент нейтрализации актуальных угроз на основе описания модели и интеграции их в web-приложение / А. В. Власенко, П. И. Дзьобан // Вестник Адыгейского государственного университета. Серия 4, Естественно-математические и технические науки. – 2014. – Вып. 3. – С. 189–193.

2. Власенко, А. В. Разработка и системный анализ математической модели угроз, модели нарушителя, процедур защиты web-приложений на всех этапах функционирования / А. В. Власенко, П. И. Дзьобан // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ). – 2014. – № 101. – Электрон. текстовые

дан. – Режим доступа: http://ej.kubagro.ru/2014/07/pdf/143.pdf. – Загл. с экрана.

3. Власенко, А. В. Разработка алгоритмов, инструментов и методов авторизации пользователей в web-приложениях с использованием хеш-функций / А. В. Власенко, П. И. Дзьобан, М. В. Тимченко // Вестник Адыгейского государственного университета. Серия 4, Естественно-математические и технические науки. – 2015. – Вып. 4. – С. 144–150.

REFERENCES

1. Vlasenko A.V., Dzoban P.I. Razrabotka algoritmov i programm vybora optimalnogo nabora komponent neytralizatsii aktualnykh ugroz na osnove opisaniya modeli i integratsii ikh v web-prilozhenie [Development of Algorithms and Programs for Selecting the Optimal Set of Components for Neutralizing Current Threats Based on the Description of the Model and Their Integration into a Web Application]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4, Estestvenno-matematicheskie i tekhnicheskie nauki*, 2014, iss. 3, pp. 189-193.

2. Vlasenko A.V., Dzoban P.I. Razrabotka i sistemnyy analiz matematicheskoy modeli ugroz, modeli narushitelya, protsedur zashchity web-prilozheniy na vsekh etapakh funktsionirovaniya [Development and System Analysis of the Mathematical Model of Threats, the Model of the Violator, Procedures for Protecting Web-Applications at All Stages of Functioning]. *Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta*, 2014, no. 101. URL: http://ej.kubagro.ru/2014/07/pdf/143.pdf.

3. Vlasenko A.V., Dzoban P.I., Timchenko M.V. Razrabotka algoritmov, instrumentov i metodov avtorizatsii polzovateley v web-prilozheniyakh s ispolzovaniem khesh-funktsiy [Development of Algorithms, Tools and Methods for User Authorization in Web Applications Using Hash Functions]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4, Estestvenno-matematicheskie i tekhnicheskie nauki*, 2015, iss. 4, pp. 144-150.

ADVANTAGES OF USING IPV6 FOR *THE INTERNET OF THINGS* FROM THE VIEWPOINT OF INFORMATION SECURITY

Aleksandra Vladimirovna Vlasenko

Candidate of Sciences (Engineering), Associate Professor,
Acting Head of Department of Computer Technologies and Information Security,
Kuban State Technological University
Alex_Vlasenko@list.ru
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Aleksey Alekseevich Musienko

Student,
Kuban State Technological University
alexmus97@gmail.com
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Abstract. The Internet of Things is a concept of a computer network of physical objects ("things") equipped with built-in technologies for interaction with each other or with the external environment, considering the organization of such networks as a phenomenon capable of restructuring economic and social processes, excluding the need for human actions and operations.

The Internet of things consists of loosely connected disparate networks, each of which is deployed to solve specific tasks. For example, in modern cars there are multiple networks for controling the operation of the engine and other systems, for supporting third communications, etc. The offices and residential buildings are also equipped with many networks for controlling heating, ventilation, air-conditioning, telephone, security,

lighting. As the Internet of things evolves, these and many other networks will be connected to each other and gain a higher level of security. As a result, the Internet of things will gain even more opportunities to open up new, broader perspectives for humanity.

This article is devoted to the popular concept *the Internet of things*. The author analyzes the opportunities, as well as vulnerabilities of this phenomenon. It has benn suggested that the use of Internet Protocol of version 6 will solve many problems of this concept including those related to security.

Key words: Internet of things, Internet protocol of version 6, security, smart house.