УДК 530.1, 681.3.06

Kulymbetov V.A., Tukushev T.K.
International Information Technologies University
Almaty, Kazakhstan
Scientific supervisor: Nurlybayev T.A.

COMMUNICATION PROTOCOLS AND SECURITY IN IOT

Abstract. *There are about 26.66 billion of active IoT devices and this number rises every year. These devices are everywhere around us starting from smart thermostats and ending with smart buildings and factories. All these devices connected to the Internet and communicates with each other using various communication and security protocols. This article collects information about number of communication protocols and security techniques applied in these protocols.*

Key words*: security protocol, internet of things, network security, rest api, amqp, jwt token.*

Introduction

AMQP protocol. Advanced Message Queuing Protocol is a protocol with an open standard that provides communication between software applications and systems no matter which client library, or platform was used. It was developed in 2003 by John O'Hara. Because it was originated as open standard protocol - many companies take part in developing it nowadays. Cisco Systems, Red Hat, Microsoft Corporation, VMware and many other companies took part in AMQP protocol development.

Basis of AMQP is AMQ model. There are two main actors in AMQP model - publisher and subscriber. Publisher is message supplier. Subscriber is message consumer. AMQ model consists of three main components. These components connected into chain in order to create desired functionality:

- **Exchange** - main entry point in AMQP server. It receives message from publishers and transfers them to the message queues based on some criteria. Exchange never stores messages, only sends them to the particular queue.
- **Message queue** - stores messages in memory or on hard drive where messages stay until they will be successfully processes by consumer. Has FIFO structure according to its name. The message that came first, will be passed to the client first too.
- **Binding** - acts like connection between exchange and message queue. Basically it is the set of that defines to which queue new message will be routed from exchange.

In simple words, AMQP is logistic company that accepts cargo in company office called exchange from applications called publishers, processes and defines to which city or terminal it should send this cargo with help of specific rules called binding and sends it to the destination terminal called message queue where another application can get it.

AMQP allows many different applications or devices in IoT network communicate with each other using AMQP as message broker that routes messages between applications using predefined routing patterns.

REST API

Representational State Transfer - REST. Was first introduced in 2000 by Roy Fielding in his dissertation. REST is communication protocol based on HTTP/HTTPS application protocol. As other protocols, REST has its own set of rules. Set of rules is listed below:

- **Stateless -** Client must provide all required information to the server in order to server could process it without problems
- **Client-server -** Client should send data, server must response to this data in different ways, but, anyway, there is only one-way communication - from client-to the server.
- **Layered -** there must be no difference for the client whether it is communicating with real server or proxy server.

- **Cacheable -** server response may be labeled as cacheable or not depending on settings.

Server records and actions are regulated using data endpoints which looks like ordinary URL string with domain address, port (optional), and parameters in case of GET request. Data manipulation organized using four default HTTP/HTTPS methods listed in the table below:

HTTP method	Logical action	Action
GET	read	Returns required data
POST	create	Creates a new data
PUT/PATCH	update	Updates an existing data
DELETE	delete	Deletes an existing data

Server must process these methods properly and return corresponding HTTP response code depending on result. There is also may be some response data in response body often in JSON format.

Security measures

The first and main security measure during REST API connection is to ensure that data passed through the secured channel. Securing channel using SSL certificate ensures that all your data and credentials is properly secured because of end-to-end encryption.

The next point of security is API tokens. API token issued by the server and it ensures that only clients that has this token can pass and get data from the server. The best practice token standard nowadays is JWT token. JWT stands for JSON Web Token. It is the digitally signed collection of key-value dictionary that collects many information including expire date, token owner, tenant in multi-tenant application, etc.

AMQP-based solutions like RabbitMQ has TLS security that allows to send messages using end-to-end encryption. Because of AMQP server can act as one entrance point for all types of data from public data like some simple log messages to classified data like user private information including document ID’s, credit card information and other, it has data partition option called Virtual Host. Each virtual host has its own set of exchanges, queues and bindings, which leads to data separation by security rate. Separate virtual hosts could be accessible from consumers and publishers by corresponding login and password. So it it's good practice to have strong passwords that must be at least 8 characters long including letters, numbers and special characters.

Conclusion

It is unlikely that one of the considered protocols will be enough to cover all communication in the system, starting with devices with limited computing resources and ending with cloud servers. As practice shows, there are different protocols suite different situations but the most important aspect during protocol usage is security measures that must be implemented in any situation. For example, AMQP and RESTful HTTP include many well-documented and successful implementations and online resources. On the basis of which you can create a secure connection between IoT devices.

REFERENCES

1. AMQP protocol specification // A General-Purpose Messaging Standard – 2008 pp 6, 26.
2. Richardson, A. AMQP business messaging for predictable, scalable, available SOA // Microsoft Architects Insight Conference – 2008.

3. Hittu Garg, Mayank Dave Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware // IEEE – 2019.
4. Abdullah Ahmed Omar Bahashwan, Selvakumar Manickam a Brief Review of Messaging Protocol Standards for Internet of Things – 2019.
5. Soumya Kanti Datta, Christian Bonnet Securing IoT Platforms // IEEE – 2019.
6. F. D. Hudson, Enabling trust and security: Tips for IOT // IT Professional, vol. 20, pp. 15–18 - 2018.

Кулымбетов В.А, Тукушев Т.К.
Ғылыми жетекші: Нурлыбаев Т.А.

Байланыс протоколдары және заттардың Интернет қауіпсіздігі

Аңдатпа: Әлемде шамамен 26,66 миллиард белсенді IoT құрылғысы бар және бұл сан жыл сайын өсіп келеді. Бұл құрылғылар айналамыздағы ақылды термостаттардан бастап ақылды ғимараттар мен зауыттарға дейін. Барлық осы құрылғылар Интернетке қосылған және бір-бірімен әртүрлі байланыс және қауіпсіздік протоколдарын қолдана отырып байланысады. Бұл мақалада әртүрлі байланыс протоколдары және осы протоколдарда қолданылатын қауіпсіздік әдістері туралы ақпарат бар.

Кілт сөздер: қауіпсіздік протоколы, заттардың интернеті, желінің қауіпсіздігі, rest api, amqp, jwt token.

Кулымбетов В.А, Тукушев Т.К.
Научный руководитель: Нурлыбаев Т.А.

Коммуникационные протоколы и безопасность в Интернете вещей

Аннотация. В мире насчитывается около 26,66 миллиардов активных устройств IoT, и это число растет с каждым годом. Эти устройства повсюду вокруг нас, начиная от умных термостатов и заканчивая умными зданиями и фабриками. Все эти устройства подключены к Интернету и общаются друг с другом с использованием различных протоколов связи и безопасности. В этой статье собрана информация о разных протоколах связи и методах обеспечения безопасности, применяемых в этих протоколах.

Ключевые слова: протокол безопасности, интернет вещей, сетевая безопасность, rest api, amqp, jwt token.

About authors:

Kulymbetov Vladislav Aleksandrovich, graduated with bachelor's degree and studying for a master's degree at the International Information Technology University.

Tukushev Temirlan Kanatovich, graduated with bachelor's degree and studying for a master's degree at the International Information Technology University.