UDC 004.55

RESEARCH & DEVELOPMENT OF SMART HOME PROTOCOL STRUCTURE, SAFETY AND SECURITY

S.S. Surkov, PhD O.M. Martynyuk

Odessa National Polytechnic University
Ukraine, Odessa
k1x0r@ukr.net, anmartynuk@ukr.net

This paper describes the communication between smart home componens such as central server and smart home modules and safety and security of the communication. The foundation of our smart home solution is communication protocol which needs to be reliable and protected against network attacks. The model of communication of our Smart Home solution is based on WiFi microcontrollers and non-platform dependent central server.

Keywords: microcontrollers, protocol buffers, smart home, binary protocol, websockets

Smart Home is a hardware and software solution to establish control of smart home devices by PC/Smartphones over WiFi. The foundation of our Smart Home solution is communication protocol between central server [1] and smart home modules and control device. This work describes communication protocol structure between smart home modules in which important part plays Google ProtoBuff[3]. Using this protocol allows to serialize complex data structures in binary format without the necessity of developing custom serialization protocol.

To communicate between components, Web Socket [4] protocol over TCP is used. Other than this, a command may be transferred via unreliable UART interface between AtMega and ESP8266 chips. To prevent data corruption during transmission by UART port CRC16 fields were added. Protocol frame structure is shown in figure 1:

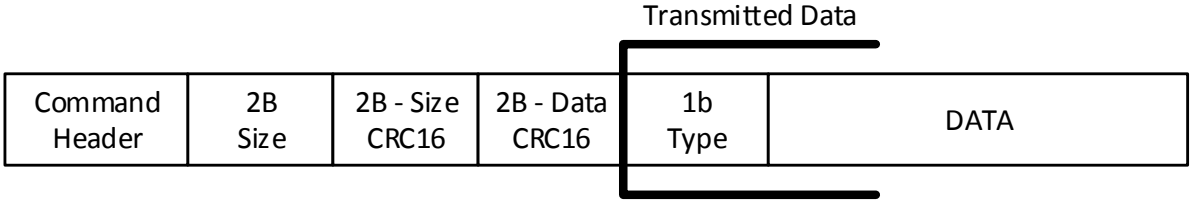

Fig. 1 Smart Home Protocol Structure for Serial and WiFi connection

The section in transmitted data is used for actual data and type of data. The other part of the message is used to verify the integrity of the data in case of unreliable communication channel. “Command header” field is unique header which purpose is to determine if the new command is started. “Size” field is used to detect how many bytes is expected to retrieve. “Size CRC16” and “Data CRC16” are used to check consistency of transmitted data and size field. If CRC16 of size field or transmitted data doesn’t match the calculated CRC16 it means that data is corrupted, and in this case command will be skipped.

For websocket communication only transmitted data section is sent through websocket frame. However entire structure may be transmitted via websocket in the case if the structure is going to be sent via UART interface. This way we decrease the load for a module and simplify message handling logic on the ESP8266 MCU.

In transmitted data section the first byte is type of Protobuf message which is going to be deserialized. To simplify development and ensure consistency of the data we suggest to define the values for it right in .proto file. After matching the data type, data is deserialized through protobuf library.

Commands at the moment of transmission through network are vulnerable to any kind of analysis and attacks. The other case might be at the moment of establishing connection to server [5] if rogue server will be found in network. To secure messages HMAC approach is used.

To ensure that the same message [6, 7] won't be sent twice Nonce and Timestamp are used. Nonce is pseudo-random generated number which is used to be sure the request wasn't sent before and timestamp is used to ensure that request is neither too old or too new. Checking timestamp allows to keep nonces only within current time. Of course for MCUs there's no possibility to keep large amount of data and to verify nonces cyclic array is used. By checking nonces and timestamps we prevent reusing already sent messages. This protocol of authorization we call ProtoAuth. Structure of ProtoAuth message is shown in figure 2.

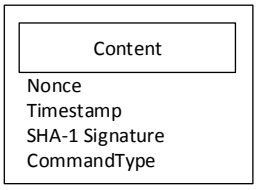

Figure 2. Structure of Websocket Message

The main field in websocket message is signature field which purpose is to verify that message is came from trusted server and wasn't modified during transmission. The SHA-1 signature is taken from other part of message plus shared secret. Shared secret is the key private parameter in this signing the message if it's exposed to attacker then he can easily hack the system.

For HMAC systems it's proven that SHA-1 algorithm is very secure. Finding of SHA-1 collisions in HMAC case may make a system unstable with high cost of finding them, only finding original message may endanger the system. Other than this with today computing powers finding a collision costs about $75,000 and $120,000 using computing power from Amazon's EC2 cloud over a period of a few months [8]. These kind of attacks are used to break HTTPS SSL certificates, but for HMAC case with message 30 minutes' live time now it's no threat at all.

The newly developed protocol allows Smart Home reliable serial communication and secure communication through WiFi. For serial communication we developed protocol structure of Smart Home message which allows verifying integrity of the command. For WiFi communication we developed a secure protocol based on HMAC which makes almost impossible to modify the data during transmission without knowing shared secrets. The result of our research might be used in many areas such as Smart Home, embedded systems, REST API development and gives to the systems additional security and reliability.

REFERENCES

1. S.S. Surkov, O.M. Martynyuk Method of Migration from Single Server System to Server Cluster. Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015)

2. Google Protocol Buffers https://developers.google.com/protocol-buffers/

3. The WebSocket Protocol. Internet Engineering Task Force (IETF) I. Fette, Google, Inc., A. Melnikov ISSN: 2070-1721 Isode Ltd., December 2011, https://tools.ietf.org/html/rfc6455

4. Foss S., Korshunov D. Heavy Tails in Multi- Server Queue // Queueing Systems. 2006. Vol. 52.

5. С.С.Сурков, А.Н.Мартынюк, И.Г. Милейко Модификация открытого протокола авторизации для верификации запросов. – Електротехнічні та комп'ютерні системи: теорія і практика, Спеціальний випуск 2015

6. С.С.Сурков, А.Н.Мартынюк Авторизация автомобильного коммьютера без поддержки браузера посредствам Bluetooth. – Холодильна техніка і технологія, № 4, Апрель 2015

7. New Collision Attack Lowers Cost of Breaking SHA1 http://www.securityweek.com/new-collision-attack-lowers-cost-breaking-sha1

С. С. Сурков, А. Н. Мартынюк

Исследование и разработка структуры, безопасности и защищенности протокола умного дома

Данная работа описывает коммуникацию, безопасность и защищенность компонентов умного дома, таких как центральный сервер и умный модуль. Основой исследования и разработки является протокол, который необходим быть надежным и защищенным от сетевых атак. Модель коммуникации нашего Smart Home решения основана на базе WiFi микроконтроллеров и центрального сервера.

Ключевые слова: *микроконтроллеры, буферы протокола, умный дом, двоичный протокол, Web-Sockets.*