UDC 004.223.2

# CLIENT-SERVER WEB APPLICATION ON ENCRYPTION MESSAGES IN THE CHAT NETWORK ON THE BASIS OF HMAC-SHA256 AND AES ALGORITHMS

*VLADISLAV PETYUKEVICH, DMITRY PASTUKHOV*
Polotsk State University, Belarus

*This article discusses the design of the secure data transfer scheme between users using peer-to-peer scheme, as well as the protection of this data. The analysis of technology most suitable for the development of this scheme has been done.*

Some means of transferring information between users, such as Viber and Telegram, use message encryption, but transmit messages through their own servers. Thus, it turns out that all user messages can be stored on the server and transmitted to someone.

This problem can be solved using a peer-to-peer connection.

A peer-to-peer network is an overlaying computer network based on equal rights of participants. There are often no dedicated servers in such a network, and each node (peer) is both a client and acts as a server. Unlike the client-server architecture, such an organization allows the network to remain operable with any number and any combination of available nodes. Members of the network are peers. [1]

Benefits from using peer-to-peer:

1. Protection against server data leakage;
2. Reducing the load on the application server, because the server will cease to participate in the process of sending messages.

None of the popular messaging tools use message protection at the highest possible level. Viber and Telegram use end-to-end encryption, but their common problem is control of the entire message passing process by the servers of these services.

End-to-end encryption is a data transfer method in which only users participating in communication have access to messages. Thus, the use of pass-through encryption does not allow access to the cryptographic keys by third parties. [2]

The topic of combining end-to-end encryption and peer-to-peer connections is not well developed. Only one article in English was found on the Internet. But only theoretical issues were considered in this article without considering the options of the technologies used.

This article deals only with the case of the text data transfer. However, the technologies used in this scheme can be applied to transfer other types of data.

End-to-end encryption in the peer-to-peer network will avoid the problem of intercepting the data being sent. This application should also work in the browser so that the user does not have to install anything.

In connection with the requirements to install peer-to-peer connections between clients using WebRTC:

WebRTC is an open source project designed to transfer streaming data between browsers or other applications supporting it using peer-to-peer technology. [3]

At the API level, technology is standardized by the W3C consortium, and at the protocol level - by the IETF community. Its inclusion in the W3C recommendations is supported by Google Chrome (and others based on it), Mozilla, and Opera.

Technology benefits:

1. Conducting a conference in a browser greatly simplifies the process of holding a conference — the user does not need to install separate applications for this;
2. Used codecs provide good quality of communication;
3. The ability to implement any interface elements using HTML5 and JavaScript;
4. Open source gives you more options.

The technology defines only the general standard of data transmission (video and sound), but individual solutions of different browsers regarding the subscribers addressing and other control processes are not compatible with each other. Therefore, even calls between a pair of different browsers present a separate complexity.

For end-to-end encryption, Diffie – Hellman protocol is used.

Diffie – Hellman protocol is a cryptographic protocol that allows two or more parties to obtain a shared secret key using an unprotected communication channel. The resulting key is used to encrypt further exchange using symmetric encryption algorithms. [4]

Description of the message transmission scheme:

1. According to the Diffie-Hellman protocol clients generate their public / private key pair during authorization and send the public key to the server;
2. Before sending messages clients receive each other's public keys through the server and exchange messages to establish peer-to-peer connections via WebRTC. To reduce server load, setup messages for peer-to-peer connections are transmitted via the WebSocket protocol;
3. As a result of receiving public keys customers can generate a common key using the Diffie-Hellman protocol;
4. After establishing peer-to-peer connections, clients can exchange encrypted shared key messages.

Algorithms used in this scheme:

1. To create a public / private key pair the Diffie-Hellman protocol is used;
2. To generate the private key the HMAC-SHA256 algorithm is used with a block size of 64 bits. The HMAC-SHA256 algorithm hashed the user name and a random number. It is done for the purpose of making different key for each new session;
3. The AES algorithm with a key (length of 256 bits and a block size of 64 bits) is used for messages encryption. The key for encrypting / decrypting messages is the shared key of two users, which is obtained using the Diffie-Hellman protocol.

Establishing a peer-to-peer connection between two clients:

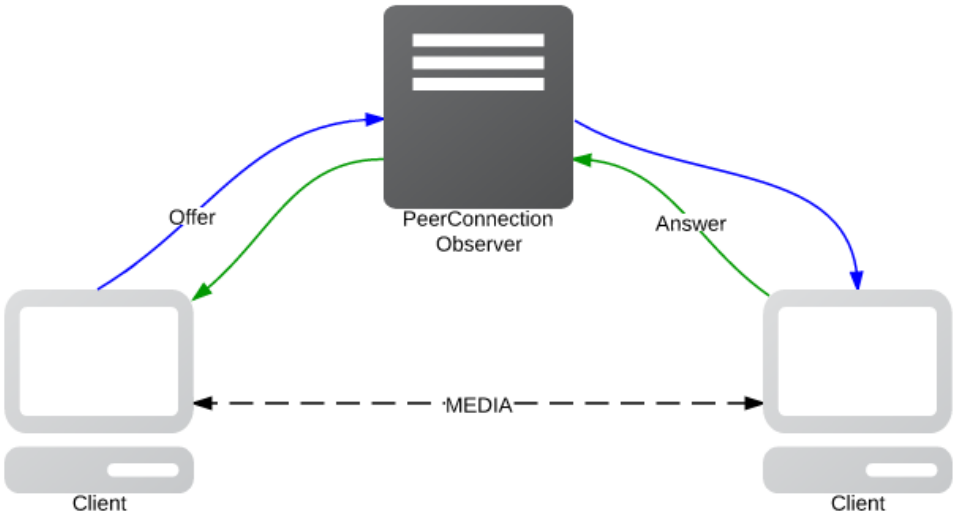


Figure 1. – A peer-to-peer connection between two clients

Simplified connection steps between two clients:

1. The first client sends the so-called Offer to the second client via server;
2. The second client sends a response through the server to the first client;
3. A peer-to-peer connection is established between clients.

For quick transfer of messages to the server, the WebSocket protocol is used. WebSocket is a full-duplex protocol over TCP connection designed for real-time messaging between a browser and a web server. [5] Compared to HTTP, WebSocket sends much less service information with each request.

The scheme for secure data transfer between users using end-to-end encryption in a peer-to-peer network was designed in the course of this study. End-to-end encryption was implemented using Diffie-Hellman protocol using the HMAC-SHA256 and AES algorithms. WebRTC was used to set up peer-to-peer connections in the browser. The developed scheme leaves the possibility for the refinement and introduction of additional remedies.

REFERENCES

1. Одноранговая сеть [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Одноранговая_сеть. – Дата доступа: 20.09.2018.
2. Бутакова, Н.Г. Криптографическая защита информации: учеб. пособие для вузов / Н.Г. Бутакова, В.А. Семененко, Н.В. Федоров. – М. : МГИУ, 2011. – С. 91–102.

3. WebRTC [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/WebRTC. – Дата доступа: 20.09.2018.
4. Протокол Диффи-Хеллмана [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Протокол_Диффи_—_Хеллмана. – Дата доступа: 20.09.2018.
5. WebSocket [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/WebSocket. – Дата доступа: 20.09.2018.