Ensuring information security in corporate communication systems

K.V. Matrokhina[1], A.B. Makhovikov[1], E.N. Trofimets[2]

[1]Saint Petersburg Mining University, 199106, 2-, 21st Line, St Petersburg, Russia
[3]Saint- Petersburg University of State Fire Service of the EMERCON of Russia, Saint-Petersburg, Russia

Abstract: The paper considers a secure information transfer protocol for corporate IP-telephony system. In the article are analized the advantages and disadvantages of the known protocols. A description of the process of establishing a connection, sending text messages and voice communication in the developed protocol is given. Its practical significance and expediency of use are described.

1 Introduction

One of the fundamental principles of modern communication systems is the provision of servers that ensures the functioning of the system, “somewhere on the Internet”. This is convenient for users, since to connect to the system, you only need to download the client application from the store and perform the minimum steps to configure it. However, the non-admittance of access to the server by third parties is guaranteed only by the words of the owner of the communication system. In particular, if we consider the Viber system, then the development of its client-side is carried out in Belarus, but the server-side is in Israel, and Belarussian programmers do not have access to the server-side codes. This can be a threat to privacy.

Another basic principle is the use of asymmetric encryption algorithms, i.e. algorithms using public and private keys. Naturally, this is done for the users’convenience who do not need to obtain a key to encrypt messages in a specific way, but can simply get the public key over the network. But it should be bear in mind that asymmetric algorithms, in addition to large computational costs compared to symmetric ones, and achieving the same cryptographic strength with a longer key length, have weak resistance to man-in-the-middle attacks.

It should be noted that messengers that are considered secure use "end-to-end" encryption, in fact, it is not the case. The process is such that modern mobile operators use symmetric translation of network addresses, which excludes the possibility of direct exchange of information between clients, that the process of generating a common key requires data transmission [1].

Thus, none of the conversations using VoIP and IM can guarantee the confidentiality of the exchange of voice and text information over the Internet.

Thus, the topical task is to develop a system that implements the idea of using standard client applications, applications on smartphones, with technological processing of

transmitted information on its own corporate server. One of the main elements of such a system is the data transfer protocol, which must provide guaranteed protection of possible confidential information.

2 Review of literature

Ensuring the security of transmitted information is one of the most important tasks of any modern communication technology, including IP-telephony. These technologies implement methods aimed at preventing a number of threats [2] that arise during data transmission over communication channels: sniffing, interception and manipulation of data, substitution, and hacking of user data, restriction of availability. The works [3] are devoted to the discussion of these problems [4,5] and other authors.

IP networks can be considered in a broader sense as part of the future digital enterprise network [3,6] or a wide-purpose self-driving IoT complex management system [7].

Hence the need to study IP-telephony and its security in general, especially when solving the problems of creating and operating integrated information systems [8-12].

Currently, in the corporate sector, SIP servers are usually used to organize IP-telephony, video and audio conferencing, and instant messaging (see Figure 1). It should be noted that for the organization of IP-telephony, instead of standard applications for smartphones, IP-phones are used.

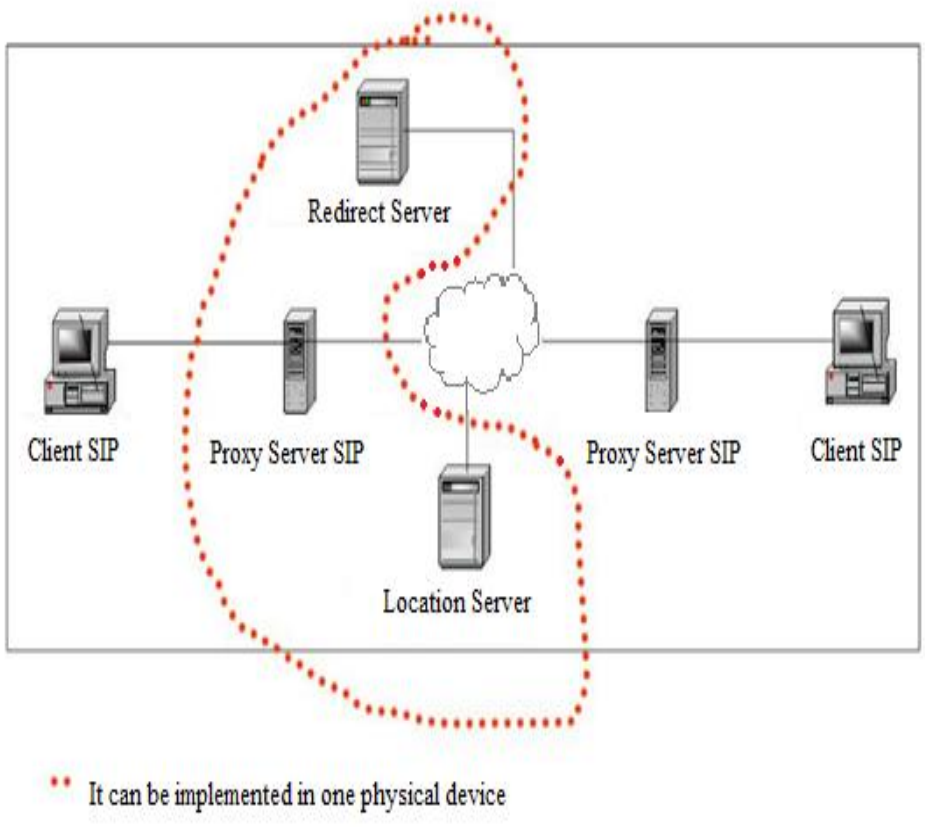

Fig. 1. An example of the organization of a corporate system SIP communications.

To ensure the protection of information during its transmission in the considered network, three types of protocols are used:

- Media protection protocols (SRTP);
- Protocols for generating/distributing keys for media protection protocols (ZRTP);
- Signaling protection protocols (SIP) [13].

Unfortunately, the aforementioned protocols have drawbacks, which means they cannot guarantee comprehensive protection of information. TLS uses the same set of keys (public and private) for server authentication and SRTP key exchange (*Keys, Ciphers, Messages: How TLS Works*).

ZRTP uses non-cryptographic keys for encryption.

SRTP and ZRTP are two evolutions of the RTP protocol for real-time data transmission. The fundamental difference between them is that the key exchange for SRTP occurs in the signal phase, and for ZRTP - at the beginning of the voice phase by the Diffie-Hellman method.

Unfortunately, the use of these protocols does not provide guaranteed information closure in IP telephony systems. TLS has many vulnerabilities [14] and cannot reliably exchange the keys required for SRTP. And the Diffie-Hellman method used to generate the key system in the ZRTP protocol is not immune to a man-in-the-middle attack. For authentication in ZRTP, a short authentication string (SAS) must be used, which is an abbreviated representation of the cryptographic hash of the received keys [15]. SAS calculates the values on each side of the connection and the subscribers transmit them to each other by voice for verification, which is not involved in messages.

In this regard, for the corporate IP-telephony system being created, it was decided to develop its own protocol for secure information transfer.

3 Methodology

The system includes a server application for CentOS or MS Windows operating systems, an application for MS Windows for system administration, and client applications for smartphones running on the Google Android and Apple iOS operating systems, located in Google Play and AppStore, respectively. The basic system is shown in Figure 2.

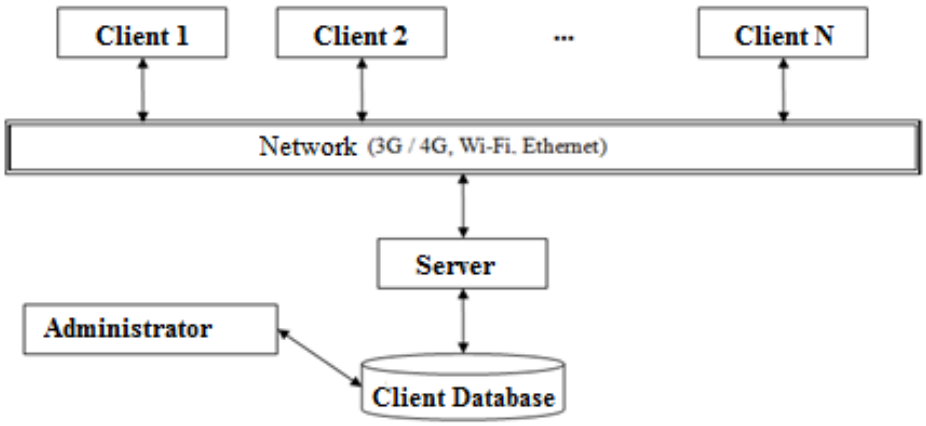

Fig 2. System block diagram.

The server is the central element of the complex and in the course of its functioning, it interacts with all other elements through secure communication channels. Base and session keys are generated when installing or reinstalling the server.

The server is an application for CentOS or MS Windows operating systems.

The main functions of the server are:

- Storage of main keys;
- Storing information about company employees and their smartphones;
- Ensuring the authorization of clients;
- Providing clients with contact lists;
- Establishment and termination of connections between clients;
- Generation of basic and session keys.

The structural diagram of the server is shown in Figure 3.

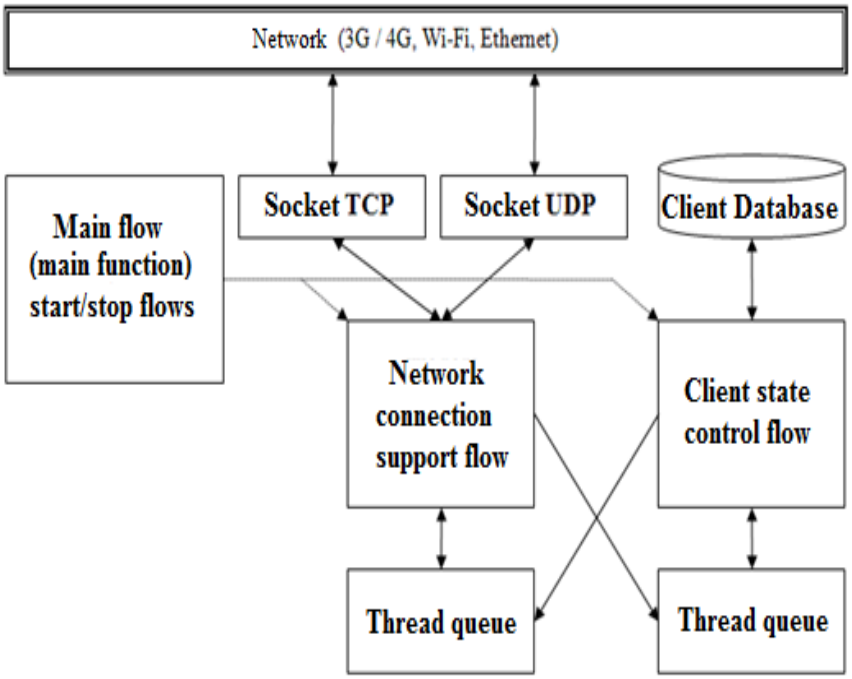

Fig. 3. Server block diagram.

The client is an application for smartphones running Google Android, Apple iOS operating systems. The core of the system for Google Android is written in Java Native Interface and C, for Apple iOS in Object C and C.

The main functions of the client are:

- Making calls;
- Sending text messages;
- File exchange between network subscribers.

The structural diagram of the client is shown in Figure 4.

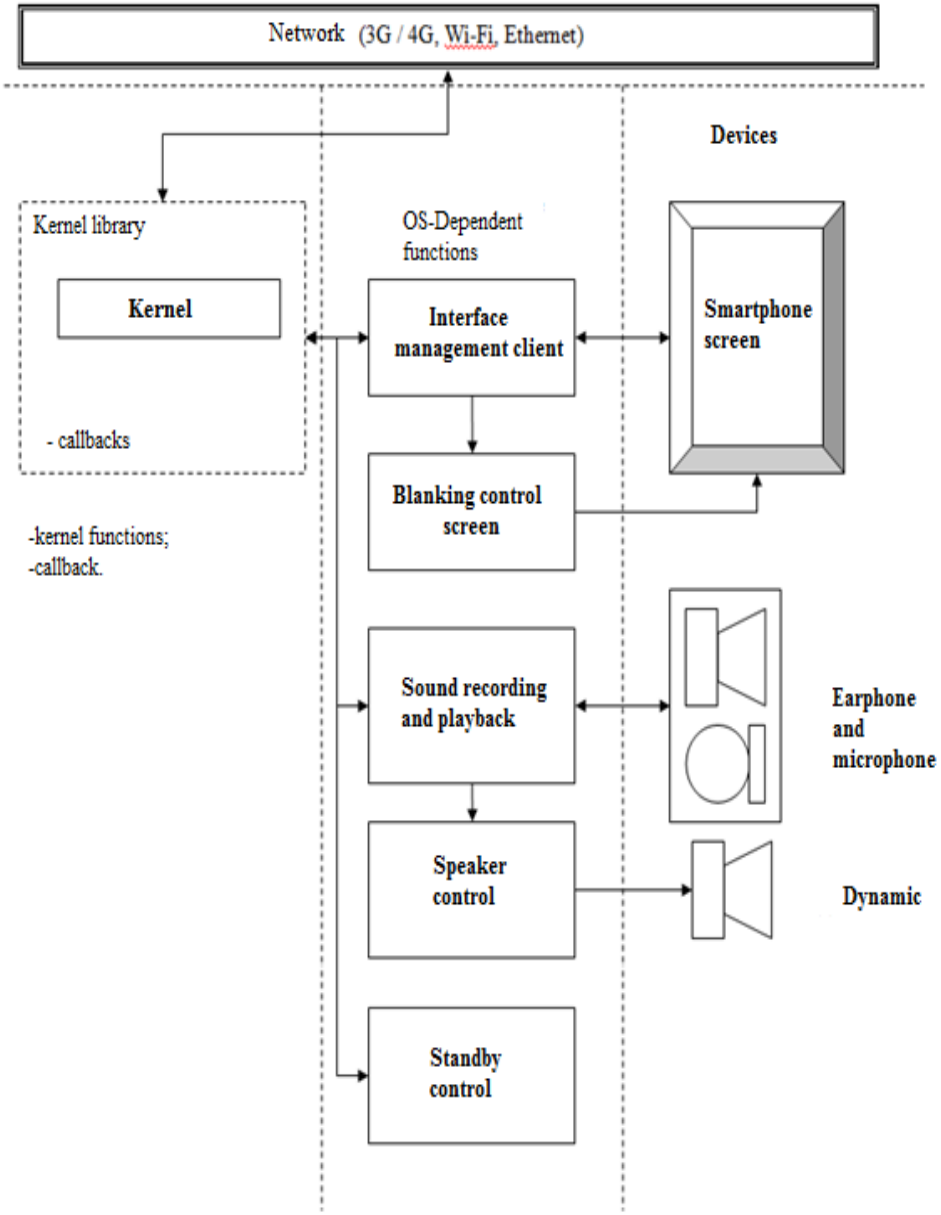

Fig. 4. Client structural diagram.

Since the developed communication system is corporate, there is a fundamental possibility of setting up subscriber smartphones directly at the company's office. During this setup, the basic encryption keys are injected into the client applications and thus do not need to be transmitted over the communication channels. This provides the possibility of using only symmetric encryption algorithms, which, in comparison with asymmetric algorithms, are distinguished by greater cryptographic strength with a shorter key length and lower computational costs. One of the best such algorithms is the Russian GOST 28147-89 "Information Processing Systems. Cryptographic protection. Algorithm for cryptographic transformation" (*GOST 28147-89*).

The following describes the processes that are carried out on the basis of the developed protocol, based on GOST 28147-89 in the developed system. It is important to note that the protocol was developed before the notice on the procedure for using the block cipher algorithm GOST 28147-89 dated 01.07.2019 appeared (*Notice about the order of using the block encryption algorithm GOST 28147-89*). The updated version is planned to take into account the new requirements.

The advantages of the algorithm include high performance, protection against the imposition of false data (generation of an imitation insert), the same encryption cycle on four GOST algorithms, and a large key length. The use of other known algorithms in this system can create a security risk. So, symmetric algorithms DES (56) and 3DES (112 or 168) have a small key length according to modern standards. Since these algorithms are highly computationally powerful, they are insecure. Despite the key length of 256 bits, the AES algorithm is susceptible to side-channel attacks. The BLOWFISH algorithm has a sufficiently high cryptographic strength and a key length of up to 448, but at the same time consumes a lot of RAM.

4 Results

Authorization. After starting, the Client enters the "connecting" state and establishes a TCP connection with the Server using the known IP address and port. In case of a successful connection, the Server switches to the "awaiting authorization" state, and the Client switches to the "authorize" state and sends a packet with its identifier and two generated numbers, which are half of the session ID and session key. The package is encrypted using the Client's base key. If the first half of the session identifier and the session key match, then the authorization is considered successful.

After successful authorization, the client begins to periodically "ping" the server. Each encrypted ping packet, as well as all packets transmitted from the client, contains a unique connection identifier that was used for authorization. The client's IP address and port are remembered by the server. If ping packets do not arrive within a certain time interval, then the authorization of this client is lost. Additionally, client disconnection is possible by sending a special message. As soon as the Server receives a packet with a message about successful authorization, it sends a list of subscribers to the Client.

Channel maintenance. To keep the channel active, the Client sends "ping packets" to the Server at regular intervals. The Server responds to them and determines the time when the last packet arrived. If the allowed timeout has exceeded, the Server terminates the connection.

The Client also continuously measures the time elapsed since the last ping packet arrived from the Server and, if its permissible value is exceeded (i.e., if the Server is "silent"), terminates the connection and attempts to authorize again. Attempts to authorize are made by the Client at regular intervals in an endless cycle. In this case, the Subscriber has the opportunity to terminate the work of the Client at any time.

Sending text messages. To exchange text messages, the Sender Client creates an SMS Session - a data structure containing the Addressee Client identifier, Session type ("sms"), and information about the sent and received messages, including text, time of sending, lifetime, status ("sent ", " Delivered", "read") and the time of the last status change. The Sender-Client scans the Session at a specified frequency and deletes from it messages that have expired.

To send a message, the Sender-Client generates an SMS packet, which includes the identifiers of the Sender-Client, the Addressee Client, messages, message content, lifetime and time of its creation. This packet is encrypted with the session key and sent to the Server. The message status is set equal to "sent" and the time of sending is entered into the

Session. The Server decrypts the packet, removes the Addressee Client identifier from there, re-encrypts the packet with its session key and sends it to it.

The Addressee-Client decrypts the packet and, if it has not yet exchanged messages with this Sender Client, it creates a Session containing the Sender Client identifier and the Session type ("sms"). The content of the message, the lifetime and the time of its creation, the message ID, are recorded in the Session. The message status is set equal to “delivered”, the time of the status change is equal to the current time, and a “SMS confirmation” packet is sent to the Server, containing the identifiers of the Addressee Client, Sender Client, message, its “delivered” status and delivery time. After the Subscriber reads the message, the status changes to “viewed” and a packet is sent to the Server with the “viewed” status and viewing time. "SMS confirmation" packets are encrypted with the session key of the Addressee Client.

The Server decrypts the packet, removes the Sender Client's identifier from there, re-encrypts the packet with its session key, and sends it to it.

Upon receipt of the “SMS confirmation” package, the Sender Client enters the message status and the time of the status change into the session.

Call. The Initiator-Client organizes a Call Session (by calling a subscriber) - a data structure containing the Addressee-Client identifier, the Session type (“call”), the Session state (“waiting for an answer”), and the Initiator-Client Session identifier. It also generates a session key.

Next, the Initiator-Client sends to the Server a "start" packet containing the Session type ("call"), the Session identifiers of the Initiator Client, Initiator-Client, Destination-Client, and the session key. This packet is encrypted with a session key.

Upon receipt of the start package, the Server initiates a Call Session using the information from it. Moreover, the Server generates the Session ID of the Destination-Client. Then it sends the “start” packet to the Addressee Client, containing the Session type (“call”), Client Session identifiers, and a session key.

Having received the starter package, the Addressee Client notifies the Subscriber about the incoming call.

The session is transferred in the "conversation" state if the incoming call is accepted.

Then the Clients send short UDP packets to the Server. These packets are encrypted with the session key. The role of the Server is to forward packets between the Initiating Client and the Destination Client. As soon as UDP packets are received, the Session goes into a working state and it transmits voice packets to the Server. The packets are encrypted with the session key.

If one of the Clients does not answer the call within a certain time, then the other Client (interacting) sends to the Server an "end of communication" packet. When the Server receives this package, it deletes the working Session.

5 Conclusion

In the modern world, information is one of the most valuable resources, therefore its protection is an important task. Due to the growing popularity of IP-telephony, the issue of ensuring its security, in general, and the confidentiality of conversations in particular, is becoming more acute.

Knowing the main threats to IP -telephony networks, as well as understanding how to eliminate these threats, will help preserve a company's reputation and financial resources.

This article describes the functions of the developed secure protocol and the structural components of the system.

The protocol is applied in the Hidden Net secure corporate communication system, which has been tested at many foreign and Russian companies. As a result, it was

concluded that Hidden Net is a convenient, reliable system that guarantees information confidentiality and data integrity.

References

1. K.V. Matrokhina, A.B. Makhovikov, The development of information protection facilities in corporate mobile VoIP communication systems, *2nd All-Russian Conference Modern educational technologies in training specialists for mineral and raw materials complex, St. Petersburg*, 1184-1190 (2018).
2. E.V. Katuntsov, Analysis of tools for countering threats of information security information transmission network, *Actual problems of info telecommunications in science and education, St. Petersburg*, 96-101 (2016).
3. B.S. Goldstein, A.V. Pinchuk, A.L. Sukhovitskiy, *IP-Telephony*, (BHV-Petersburg, 2014).
4. E.V. Katuntsov, O.V. Kosarev, A.B. Makhovikov, P.S. Tcvetkov, Digital transformation in oil and gas extraction. Innovation-Based Development of the Mineral Resources Sector: Challenges and Prospects - *11th conference of the Russian-German Raw Materials, 2018, Potsdam, Germany,* 531-538 (2018). CRC Press/Balkema.
5. C.A.Van Tilborg, Henk Jajodia Sushil, *Encyclopedia of Cryptography and Security*, 2nd Edition. Springer, 1457 (2011).
6. E.B. Mazakov, Representation and processing of knowledge in information automated systems of intelligent field, *Journal of Mining Institute*, **208**, 256-262 (2014).
7. A.M. Batkovskiy, E.G. Semenova, E.N. Trofimets, V.Ya. Trofimets, A.V. Fomina, Modified method for sensitivity analysis of investment projects efficiency criteria, *Journal of Applied Economic Sciences, Romania: European Research Centre of Managerial Studies in Business Administration,* **4(50)**, 1116-1131 (2017).
8. V.A. Dokuchaev, Information security on corporate VoIP networks, *Electrosvyaz*, **4**, *5-8* (2017).
9. V. I. Doroshenko, Yu.M. Iskanderov, Organization of transport and technological processes based on integrated information systems, *New Economy and the main directions of its formation, St. Petersburg*, 53-62 (2016).
10. V.D. Gaskarov, Yu.M. Iskanderov, S.V. Smolentsev, Development of transport and technological processes based on integrated information systems, *Transport business in Russia*, **5**, 114-117 (2019).
11. Yu.M. Iskanderov, A.G. Nekrasov, B.V. Sokolov, *Information technologies in management (ITU 2018):conference proceedings - St. Petersburg,* 80–89 (2018).
12. A.V. Roslyakov, M.Yu. Samsonov, I.V. Shibaeva, *IP telephony* (2nd ed. - M: Eco-Trends, 252 (2003).
13. A.A. Biryukov, *Information Security: Defense and Attack*, (2nd Edition. - M: DMK Press, 434, (2017).
14. D. Joshua, Implementing SSL/TLS Using Cryptography and PKI, *Wiley*, **696** (2011).
15. P. Thermos, A. Takanen, Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures Addison, Wesley, **384** (2008).