Asian Journal of Information Technology 15 (24): 5120-5125, 2016
ISSN: 1682-3915

Development of Secure and Reliable Communications System for Corporate Sector Over Mobile Telecom Networks

[1]Aleksei Makhovikov and [2]Sergei Kryltcov
[1]Department of Informatics and Computer Technology, Saint-Petersburg Mining University, 199106 St. Petersburg, Russia
[2]Department of General Electrical Engineering, Saint-Petersburg Mining University, 199106 St. Petersburg, Russia

Abstract: The study addresses the issues of development and functioning of the software and hardware system intended to provide secure and reliable communications for remote corporate subscribers over the networks with cellular or wireless internet access. The system requirements necessary to maintain secure connection of end users are indicated and discussed. Based on the analysis of existing solutions, the structure of novel software and hardware system which fulfills indicated requirements was proposed, implemented and tested in several Russian and Canadian companies. Results showed that developed system allows secure and high quality voice and data transmission between subscribers over the 3, 4G and Wi-Fi mobile telecom standards.

Key words: Unified communications, VoIP, data protection, encryption, Russia

INTRODUCTION

The ensuring of private and reliable conversations of remote subscribers has become the subject of a great concern nowadays, when information tends to become one of the most valuable resources. This trend is the most noticeable in the corporate segment that is caused by several factors (Machovikov, 2015). Currently companies of any size all over the world tend to become distributed to achieve the most efficient way of providing their services and delivering of products to the end customers which is fair for wide area of businesses-from mineral complexes to consulting companies. Business efficiency in such circumstances strongly depends on providing reliable communication between the company branches as well as between individual employees. In competitive conditions, a large portion of information exchanged inside the company becomes a trade secret which exposure to third parties may lead to severe losses for company that is especially fair for the countries with market economy (Machovikov *et al*., 2011).

Historically, traditional telephony was the only way for subscribers to communicate and in many companies this remains the main communication way. However, nowadays users communicate via the vast variety of technologies, such as cell phones, internet-messaging, e-mail, etc. Achieving of full usage of corporate communication technologies that are based on different principles of information transfer increases the overhead costs of the enterprise. In this case, the world's leading pro-producers of hardware and software such as the Microsoft and Cisco for about ten years developing the concept of unified communications which implies the use of corporate communication for the organization of the existing network infrastructure. In such systems, all the necessary information (voice, video and data) is transmitted in the real time over IP-network. Using unified communications significantly reduces the cost of ownership and creates a communication system and outputs the business communication to a new level.

MATERIALS AND METHODS

Development of reliable and secure communication system: To build and/or maintain unified communications system it is necessary to indicate requirements for such system intended to provide communications over the cellular and wireless networks. The first requirement is the provision of security for communications which is a complex task (Machovikov, 2011). The security of communications is achieved by use of encryption algorithms on the end user devices, so exchanged information will travel across the network only in the encrypted form. There are two basic types of such algorithms: symmetric-and asymmetric-key algorithms. The symmetric-key algorithms use the same (or relatively

Corresponding Author: Aleksei Makhovikov, Department of Informatics and Computer Technology, Saint-Petersburg Mining University, 199106 St. Petersburg, Russia

easy transformed) keys for both encryption and decryption of information which usually means that both parties must have the access to the shared secret which is a drawback of such systems. The asymmetric-key algorithms use public key to encrypt the information while decryption of information in finite time is only possible with the receiver's private key. There is availability of strong realizations of both types of encryption algorithms and the key lengths as well as encryption method required to maintain secure connection are usually described in the particular country standards. So it can be said that strong encryption become a de-facto standard for a wide variety of messaging and voice communication applications now a days.

However, the voice and text conferencing require multiple concurrent opened sessions between the subscribers and such applications are usually realized according to client-server model. The majority of such applications, available on the market is either the closed source code of client-and/or server-side applications or hosting the server only at third parties site. Both scenarios lead to inability to fully control the encryption and session establishment processes for the customer. Therefore, to ensure exchange of private information for business customers it is necessary to gain full control over every node of the communication system.

Several open-source applications are intended to work around that issue, however, there is no existing solid solution among them which would include both the client and server software, allowing to establish communications between end-user smartphones (Flanagan, 2012). That leads to another complex requirement to communication system-ease of use, preferably for both users and administrators. In the presence of different platforms available to host applications on laptop, desktop/server workstation or smartphones, ease-of-use requirement also claims another issue-the communication system software should be platform independent to achieve the comfortable use on the most company's and users' devices. The management point of view is another issue of the ease-of-use term. The communication network should be managed easily and all changes in the network structure should be obvious for the administrator that will lead in turn to increased security and reliability of the whole system.

However, the system's reliability depends on many factors and should be provided on each stage of the establishing of communication between subscribers. The hardware reliability as well as reliability of the program implementation for particular platform are out of scope of the study. In communication applications, especially in its implementation on cellular networks, the reliability becomes a huge issue as reliability of packet transmissions in cellular networks highly depends on the strength of station signal, canal bandwidth, station overload, et cetera. In such circumstances, the presence of reliable algorithm for data transmission over the cellular networks is an essential feature of the communications system. Based upon above, several methods of achieving the secure and reliable communications between corporal subscribers can be summed up:

- Strong and reliable end-to-end encryption algorithm
- Cross-platform (including mobile platforms) software availability
- Customer's ownership of all system nodes involved in data manipulation (not transmission)
- Ease of use for both users and administrators
- Reliable data transmission protocols designed for cellular and wireless networks

There are different systems for unified communications available today. Most well-known of them are as follows: Microsoft Unified Lync, Cisco Unified Communications, Avaya Aura, HP Unified Communications, Istra and more (Flanagan, 2012). While most of these systems offer great user and management experience, they are also characterized by high cost and the need for them to deploy and maintain highly qualified professionals, specially trained. IP-telephony systems are also often organized by installation of the own SIP-server, often Asterisk but the installation and configuration of these servers also requires highly qualified specialists in IP-telephony systems. In addition as consumer devices for such communications systems are commonly using stationary IP-phones and clients for smartphones, they do not provide high-quality communications.

In turn, users of smart phones to make calls and send short text messages and files are widely used three global communications: Skype, Viber and WhatsApp. These systems, of course, easy to use, provide good call quality and their clients are easy to install and set up but their use in the corporate sector is limited. The reason for this is that third parties own the server that stores the personal data of subscribers and transmits data.

Thus, the development of an inexpensive, easy to install, easy to use and provides a guaranteed closure of the entire unified communications transmitted information which as the subscriber units are the modern smart phones is an important and urgent task.

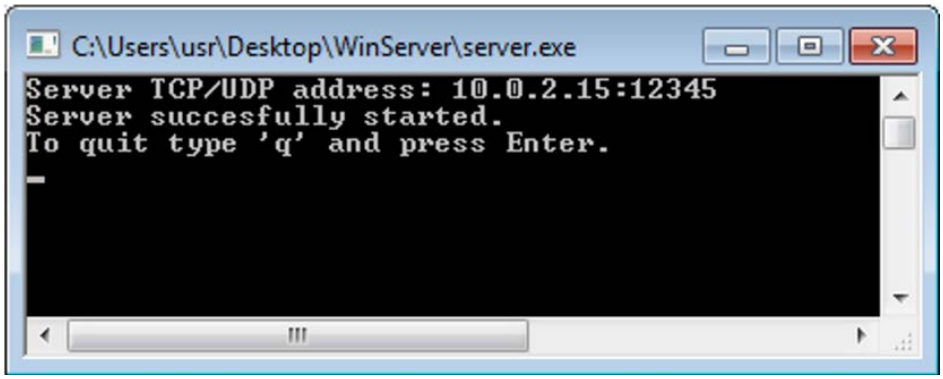

Fig. 1: Server command line interface in MS Windows 7

Proposed solution: The overall structure of the proposed systems which is well suited to maintain indicated features, includes:

- Server application
- Proxy server application
- Administrative application
- Client application

Server application: Server is an application for the desktop or server system based on Linux/Windows distributions. Currently server is applicable for the following Linux OS: Ubuntu (both Server/Desktop) 12.04-15.10, Debian 6.0-8, CentOS 7. The server application works also on the following Microsoft OS: Windows 7, 8, 8.1, 10. The server applications maintain following major functions:

- Storing the IP-address and proxy port
- Storing basic keys
- Storing subscribers and their smartphones data
- Ensuring customer authorization
- Synchronization of contacts between the server and the subscribers
- Generation of session keys
- Establishing and breaking the connection between the clients

A static public IP-address must be assigned to the server networking interface. The server is the central element in the system and it maintains communication with all system elements via secure communication channels. The server command-line interface on the Microsoft Windows OS is shown in Fig. 1.

The server application is a portable executable file which can be installed (copied to the system) by any method of distribution, chosen by the company-from USB/flash stick, directly downloaded from the website, etc. However, server application may require some additional software to be installed on the target system, for example, pkill tool for Linux. Server application is ready to work after the initial configuration is done on the target system which includes assigning server IP address and port. The basic keys and keys, required to encrypt connection with the admin application, are to be generated during first configuration of the server application. Copy of generated keys then should be securely transmitted to the workstation with the admin application. All data required by the server is stored in securely encrypted containers. To fulfill requirements to the communications security, it is recommended to store the server workstation at the secured area (Fig. 1).

Proxy server application: The proxy server is a portable executable application for Linux and Microsoft Windows OS and is tested for the same list of OS as server application. The main function of the proxy server is to provide data exchange between subscribers' client applications during the session. Proxy server application can be installed on any computer that has a static public IP-address and a dedicated connection to the Internet at a speed of 100 Mbit sec^{-1}. It is possible and advisable to install proxy server on a virtual machine in public areas. It does not generate, transfer or store any private information. Any unauthorized access to the workstation with proxy server does not lead to the discrediting of the system and its elements.

Administrative application: Administrative application is a portable executable file for the Microsoft Windows. The application provides following administrative functions:

- Addition and removal of the IP-addresses and proxy ports
- Activation of the basic keys on the server

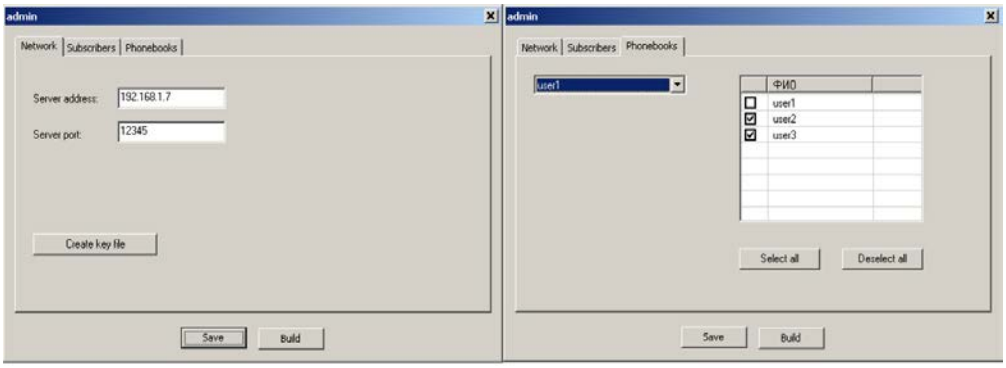

Fig. 2: Administrative application guided user interface in MS Windows 7

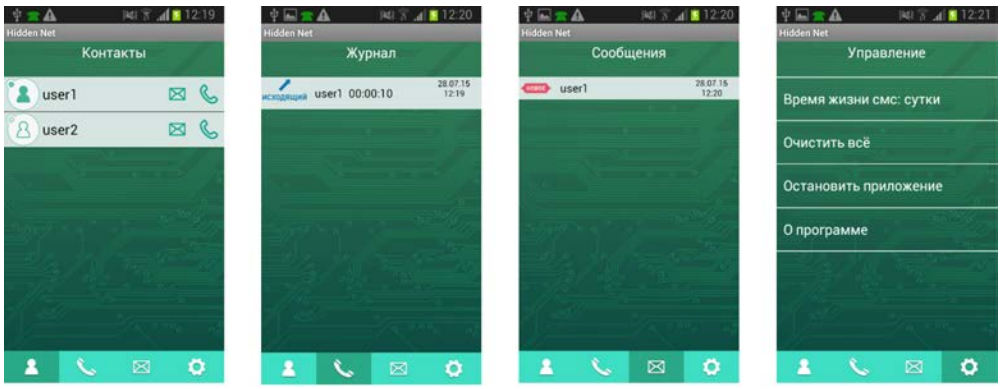

Fig. 3: Client application user interface

- Addition and removal of network subscriber data (unique ID, name, department, position) and their smartphones (manufacturer, model, operating system, IMEI and IMSI)
- Installation and configuration of client applications
- Blocking and removal of client applications

Administrative application files can be obtained by any distribution method chosen by company and installed on any PC/laptop with Microsoft Windows OS 7, 8, 8.1, 10. During the initial configuration, the administrator specifies the IP-address and port of the server, the password to unlock the application and bit encryption order of the audio codec parameters. The guided user interface of the developed administrative application is shown in Fig. 2.

The administrative application opens connection to the server, encrypted with the key generated on the server and securely transmitted to the administrative workstation via any secured channel allowed by the company policy (encrypted flash drive, dedicated encrypted connection, etc). When all settings are tuned, the client application executable files can be generated by the administrative application.

Client application: The client application is an application for smartphones running following operating systems: Google Android, Apple iOS and Microsoft Windows Phone. The main client application features are:

- Implementation of voice calls
- Targeted text messaging
- Exchange of files and data between network users

The client application can be installed on the smartphone by transferring the client application executable files (which are generated for particular OS) to the target device. The interface of the developed client application is shown in Fig. 3.

During the installation of the client app, the user should enter a unique user ID and pin-code which allows the client app to obtain access to remaining part of

information which is generated by the administrative application and required to establish connection to other subscribers.

RESULTS AND DISCUSSION

Description of information exchange processes in the system: The control data is encrypted on the client according to the GOST 28147-89 standard with a 256-bit key which is unique for the client application and is four times larger than key length, usually used in similar applications. Voice information and data are encrypted using the same algorithm and the new key is generated for each communication session. Audio signal compression is performed using a proprietary codec that provides the flow rate of 9600 bits sec^{-1}. If desired (optionally) the codec may use rates up to 26000 bits sec^{-1} which provides a greater naturalness of the reconstructed speech on the end-user device. The use of a proprietary algorithm for audio signal compression and unique method of a bits packaging order for analysis window settings provides additional network security. The control information is transmitted via the server while the session information is transmitted through the one of proxy servers. The solution allows to provide:

- Operation of client applications in any cellular or wireless networks with the Internet without the need for a public static IP-address for the subscriber device
- Fast and easy work of the administrator while adding or excluding users and changing corporate network schemes
- The voice conference and chat organization

The client application is bound to the user device by IMEI and is installed in a smartphone SIM-card via the IMSI. Additional protection is provided against unauthorized use by setting a unique pin-code required to access the application.

The basic keys are generated during the installation and reinstallation the server and are stored in its database in an encrypted form as well as a secure flash drive to be connected to the administrator's workstation. When a client is added to the system on the server establishes link between the subscriber identifier and key entered in the client application when it is installed on the smartphone. This key is used to encrypt the control information transmitted between a client and a server and is not transmitted over the network. With the exclusion of a person from the complex, its basic key is removed. To encrypt information transmitted in a communication session a temporary key is generated which is destroyed after the session is completed.

The proposed novel communication system is currently undergoing a trial operation in a number of small Russian and Canadian companies. At the time of the article publishing, the system achieves very positive reviews. The positive features indicated by the reviewers are as follows: high quality of the voice communication, platform independency, ease of use and installation for both end users and administrators, secure and reliable transmissions. The proposed system is available to try or purchase on the http://hiddennet.mobi website, where the additional information about the system is also available. Tests showed that GPRS and EDGE standards provide high latency of packets delivery which makes it impossible to use mobile communications over the access to the Internet over such standards. 3G and higher telecom standards provide low latency with minor fluctuations and spikes which are effectively compensated with the jitter buffer implemented in software.

CONCLUSION

The study presents key features and methods which are required to build secure and reliable unified communication system for corporate subscribers. The analysis of solutions currently available on the market has shown, that there is no simple solution available for different platforms including mobile phones and providing necessary security and reliable functionality especially for cellular networks.

Therefore, the novel communication application was proposed based on presented methods which offers such features as: end-to-end encryption algorithms with strong keys, availability of client software for different mobile operating systems (iOS android, Windows Phone), availability of server and proxy software for different Microsoft and GNU Linux platforms, easy to use interface on all supported devices for both subscribers and administrators. The study presents structure of proposed system and discusses principles of its operation.

The proposed system was tested in different cellular and wireless networks of Russia and Canada enterprises. Positive reviews and feedback was obtained.

ACKNOWLEDGEMENTS

Aleksei Makhovikov and Sergei Kryltcov conceived and designed the overall proposed system. Aleksei Makhovikov developed the software communication functionality and encryption algorithms. Sergei Kryltcov worked on the server side of project and wrote the study.

REFERENCES

Flanagan, W.A., 2012. VoIP and Unified Communications: Internet Telephony and the Future Voice Network. John Wiley & Sons, New York, USA.,.

Machovikov, A., 2011. The use of online conferencing systems as a way to improve the efficiency of production management. Proc. Min. Inst., 1: 262-266.

Machovikov, A., 2015. Principles of corporate communication systems functioning in mineral complex enterprises. Proc. Min. Inst., 1: 24-28.

Machovikov, A., K. Stoliarov, A. Strelnikova and M. Chernov, 2011. Particular problems solving in the development of Internet conferencing systems. Proc. Min. Inst., 1: 321-325.