

NEWS

OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN

SERIES OF GEOLOGY AND TECHNICAL SCIENCES

ISSN 2224-5278

Volume 1, Number 421 (2017), 149 – 156

UDC 654.028

¹M.Z. Yakubova, ²T.G. Serikov, ³A.K. Muratova¹Almaty University of Power Engineering & Telecommunications, Kazakhstan,²Kazakh National Technical University, Almaty, Kazakhstan,³Karaganda State Technical University, Kazakhstan.

E-mail: Mubor149@rambler.ru, Tansaule_s@mail.ru, Aiza_yo@mail.ru

**PROTECTION OF IP-TELEFONY NETWORKS
ON THE BASIS OF ASTERISK FROM INTERCEPTION OF DATA**

Abstract. Nowadays the new round of technologies development on voice transfer, and IP-telephony is observed. In a type of the growing levels of demand and popularity of IP-telephony as bases of corporate communication infrastructure creation there is a question of ensuring at most a level of its safety. As the server of IP-telephony has direct access to the network the Internet, and authentication of subscribers happens to IP addresses. In this article the issue of safety of telephony on the basis of Asterisk from interception of these clients is resolved. As the network analyzer the software of Wireshark is used. As soft phone and client base laptops, computers, and gadgets which pass tests are considered. Communication of clients with the server passes through a wireless point of WiFi access. The attacking device is the laptop on which the software package of CommView for WiFi is established. By the result of carried out test the analysis of network's vulnerability was made. Recommendations about a measure of protection from unauthorized access are made. The optimum option of network protection is offered.

Keywords: IP-telephony, protocol, address, wireless attacks, server, Asterisk.

Introduction. For the development of information technology of telecommunication systems', chair of Karaganda state technical university established laboratory and had tested the implementation of protection which was carried out from malicious to a IP-telephony network for definition of weak spots in a network. And the results were taken on its protection. Generally information gets huge value, and modern technologies allow bringing in every spot on the globe very quickly and without use of the expensive machinery and equipment. In fact, the mankind is entering into the information century. Therefore questions transfer and information reception moves to the forefront.

Transition from traditional telephone networks to networks of IP-telephony is noted. The main difference of new networks is the applied principle of switching, namely application of packages' switching. Telephony turns from complex structure with a huge number of the equipment and personnel into one of data's services transmission networks. Application of IP-telephony gives to the client a set of opportunities and minimum price for services. They provide services of a speech transfer and video traffic to any subscriber connected to network (for example, the Internet) [1].

One of the most widespread systems of IP-telephony is the system of IP-telephony Asterisk. This system allows to work with different protocols of IP-telephony, provides a broad set of services [2].

The most popular protocol of IP-telephony is SIP (Session Initiation Protocol). This protocol differs in simplicity (and proximity to the HTTP protocol (HyperText Transfer Protocol)), independence of transport protocols, integration with a stack of protocols of TCP/IP, a possibility of work with other protocols. Asterisk supports the SIP protocol and this protocol is applied on that most often. For this reason in this article the protocol of telephony is considered.

With increase of the information price, the need for its protection increases. There is a set of information's interception ways against the fight for ensuring confidentiality of subscribers. To show vulnerability of the user data, we will use providing program Wireshark [3].

Wireshark is one of the most popular and powerful modern network analyzers. It is capable to carry out interception of a traffic, the analysis of shots headings, packages, etc. and to carry out viewing of directly transmitted data. The program is capable to analyze a traffic on many signs. In particular, it is capable to distinguish and give streams of audio and video. The built-in tools allow to allocate data flows and to present them in a convenient format (for audio, it is possible to keep video as the block of data and to format) [4, 5].

The purpose of the research is to resolve the issue of safety of telephony on the basis of Asterisk from interception of these clients by taking as the server of IP-telephony has direct access to the Internet, and authentication of subscribers happens to IP addresses and as the network analyzer the software of Wireshark is used as soft phone and client base laptops, computers, and gadgets which passes test are considered. Communication of clients with the server passes through a wireless point of WiFi access [6, 7].

Let's review an example of such interception. The call between two users of Asterisk without enciphering has been carried out for this purpose. Wireshark established on IP-telephony server carries out interception of data [8].

As a result of the intercepted data's observations the following facts have been elicited.

Firstly, it is possible to watch frames of the SIP protocol and to look through them (including the user data). The password is ciphered by MD5 (Message Digest 5) algorithm and therefore it can't be read in opened, but there is a possibility of activity observation of users [9, 10].

Secondly, there is a possibility of a talk interception. After the end of a call to Wireshark the choice of the Telephony menu, and in its subparagraphs of "RTP" (Real-time Transport Protocol) and "Show all streams" is carried out. The program displays streams (figure 1):

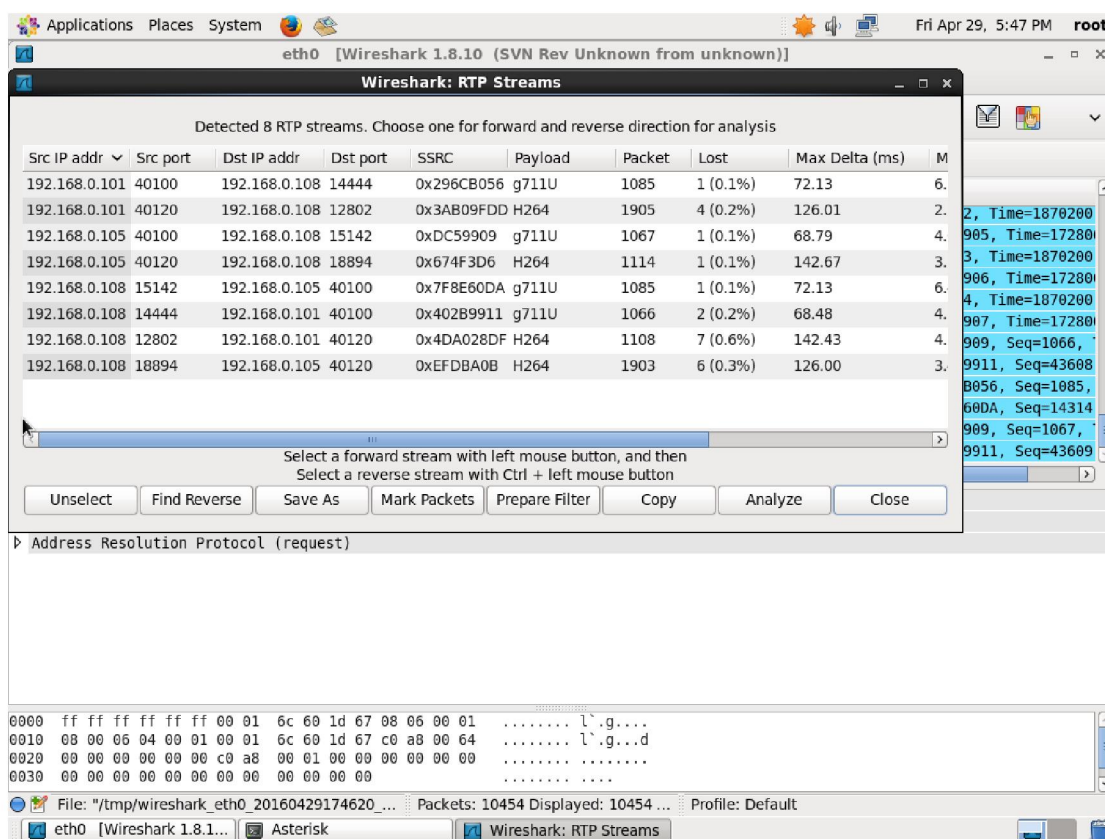


Figure 1 – RTP streams, captured by Wireshark

By pressing of the Analyze button Wireshark provides the analysis of the chosen stream on shots. At the same time there is a possibility of stream preservation (the Save payload button.). The stream can be kept in a format of uncompressed data (.raw) or in an audioformat (.au) (the last is right for the G.711 audiocodec).

Follows from the aforesaid that additional measures are necessary for protection of the user traffic. Mechanisms of a traffic protection of telephony against interception are provided in Asterisk. The linking of the TLS (Transport Layer Security) and SRTP (Secure Real-time Transport) protocols is used for this purpose [11].

TLS – the protocol of the fifth session level of the OSI model providing information security by its transfer through package networks by establishment of the protected connection.

The protocol works as follows. The client sends inquiry for connection establishment to the server, and also sends data on available protocols of enciphering. The server having received these data determines parameters of the protected connection (in fact, makes the choice of the best algorithm). After that it sends to the client the certificate with an open key. The client ciphers the casual sequence of data an open key and sends it on the server. The server decodes the sequence, and, in case of lack of mistakes and failures, there is an establishment of the protected connection [12, 13].

The protocol applies asymmetric enciphering. It means that only the party possessing the closed key can decipher the data ciphered by an open key. In this case such part is the server.

Secure Real-time Transport Protocol – the protocol of transport level intended for enciphering, protection against substitution of data and preservation of the data integrity transferred by the RTP protocol. Codes of AES (Advanced Encryption Standard) are used. Application of the TLS protocol is necessary to protect process of a secure channel establishment of SRTP [14].

Asterisk allows to use these protocols at the expense of special modules, in particular, of the `res_srtp.so` module. This module has already built in some distribution kits (for example, AsteriskNOW) and has already been ready to use. In case Asterisk has been separately installed, it is necessary to receive this module and to rebuild Asterisk with this module.

For generation of certificates `ast_tls_cert` script is provided. First of all it is necessary to download a script, it is carried out by the `wget` http://svn.asterisk.org/svn/asterisk/branches/11/contrib/scripts/ast_tls_cert team. That allows to load a script from svn-storage of data Asterisk. It should be noted that the script is loaded into that folder in which the entrance before command execution has been carried out [15, 16].

After downloading of a script we pass to his use. From the folder where the script has been loaded, we start team. `/ ast_tls_cert - C 192.168.0.106 - O kontora - d/etc/asterisk/keys`. Certificates for the server with the address 192.168.0.106, the name of the kontora organization in `directory/etc/asterisk/keys` is being generated.

Further it is necessary to generate certificates for clients. We start command. `/ ast_tls_cert - m client - with / etc/asterisk/keys/ca.crt - k/etc/asterisk/keys/ca.key - O kontora - d/etc/asterisk/keys - o 5002`. We receive the key for the client 5002 generated for the certificate of `ca.crt` and a key of `ca.key` of the kontora organization.

In folder `etc/asterisk/keys` there will be following files: `asterisk.key`, `asterisk.csr`, `asterisk.crt`, `asterisk.pem`, `5002.pem`, `5002.key`, `5002.csr`, `5002.crt`, `ca.key`, `ca.crt`, `ca.cfg`, `tmp.cfg`.

Further we configure the server. All changes are made to the `sip.conf` file. Section general:

```
[general]
tlsenable=yes
tlsbindaddr=0.0.0.0:5061
tlscertfile=/etc/asterisk/keys/asterisk.pem
tlscafile=/etc/asterisk/keys/ca.crt
tlscipher=ALL
tlsclientmethod=tlsv1
tlsdontverifyserver=yes
bindaddr=192.168.0.106
externaddr=192.168.0.106
videosupport=yes
```

Here we set TLS support, we set the address and port, files of the certificate and a key, we include enciphering and in addition we enter a number of teams for Asterisk [17].

It is possible to check TLS work the openssls_client team - connect 127.0.0.1:5061. Has to be are provided withdrawal of team with enciphering parameters, the certificate, a key.

We set up clients:

```
[5002]
type=friend
secret=12345
host=dynamic
context=local
disallow=all
allow=ulaw
allow=h264
transport=tls
encryption=yes
```

Here we set use of TLS and enciphering (we include SRTP).

The following stage is the control of clients. Clients have to support TLS and obligatory inclusion of SRTP. We consider the control of clients.

For control of the mobile client for Zoiper it is necessary to make basic settings of the client, to include SRTP (at the same time the program will request inclusion of the TLS protocol what it is necessary to agree with). Besides, the address of the server needs to be added with number of port 5061 (after the address through a colon). Screenshots of settings are presented in the figure 2:

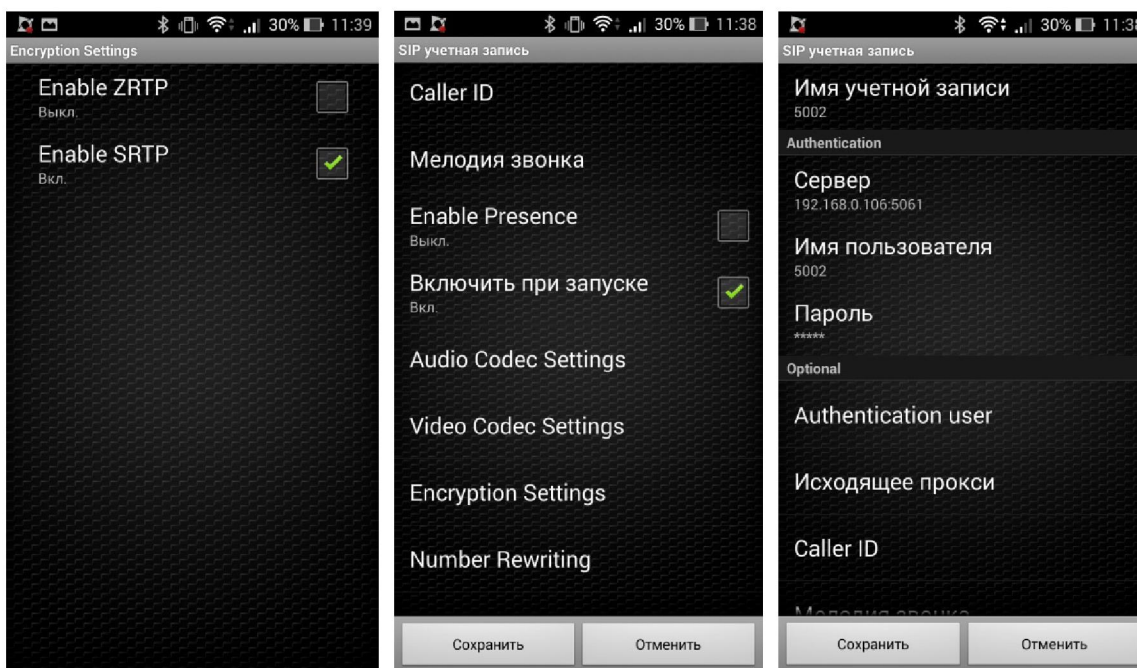


Figure 2 – The VoIP by Antisip settings for TLS and SRTP

After saving of settings the client program has to be registered on the server.

The Blink settings also demand inclusion of TLS and obligatory enciphering. At first obligatory enciphering joins in the Media menu (figure 3):

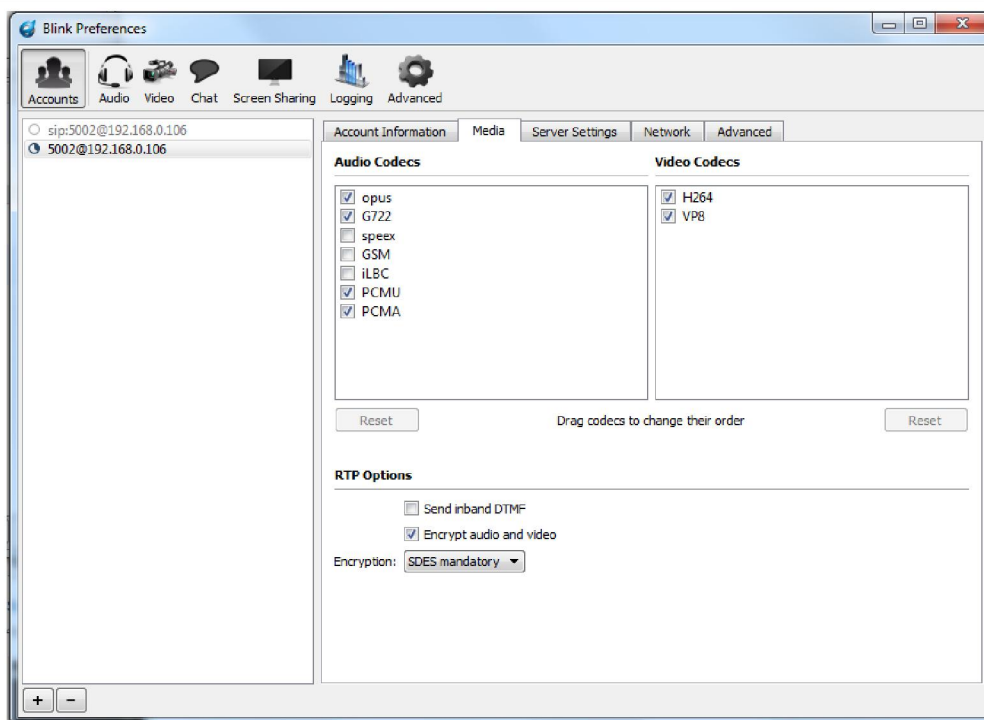


Figure 3 – Turning on the enciphering in Blink

Next in menu «ServerSettings» we enter address of the server, port number and choice of the TLS transport (figure 4):

SIP Proxy

Always use my proxy for outgoing sessions

Outbound Proxy: Port: Transport:

Auth Username:

Figure 4 – Settings of the server

In the Network menu the choice of TLS is also made, and the way to the file of the client certificate (figure 5) registers in the Advanced menu on the line "Certificate File":

TLS Settings

Certificate File:

Verify server

Figure 5 – Choice of certification

In the Advanced menu of the program (the previous settings were made in the menu of accounts) it is left included only in the TLS protocol with the necessary port and the certificate is chosen.

And now at implementation of a call the organization of the protected session by means of the TLS protocol is carried out, and data are ciphered by SRTP. The intercepted stream is represented as UDP (User Datagram Protocol) stream. Now instead of the Wireshark Window with the intercepted packages are presented in the figure 6. In this case Wireshark doesn't identify streams of RTP and can't analyse them, data are ciphered. Protection of the user data against malefactors has been carried out [18].

Support of TLS and SRTP is declared practically in all modern client applications of IP-telephony. For this reason the linking of these protocols is widely applied to a traffic protection of telephony. It is especially urgent in complex compound networks in which is more difficult to trace and prevent interception of data. These technologies ensure safety of information, at the same time their application doesn't demand introduction of new hardware and is carried out at the program level.

Treat advantages of IP-telephony: its low cost, reliability, high speed of communication and simplicity of use. It uses the most advanced technology of compression of our voice signals, and completely uses the capacity of telephone lines. Therefore packages of data from different inquiries, and even their various types, can move on the same line to one and too time the Internet, but also in other networks of data transmission with package switching (local, corporate) [19].

As a result of the conducted researches it is revealed that at expansion of corporate networks there is a sense to introduce program IP PBX instead of electronic and digital automatic telephone exchanges, the prize turns out not only at cost, but also on acquisition of technologies which electronic and digital automatic telephone exchanges don't provide.

The carried-out calculations show that in a point of access to a network with Asterisk the multimedia stream thus is hard enough to have an access point the speed of transfer of 54 Mgb providing for a multimedia traffic and a pass-band 2 GHz [20].

The scheme of wireless attack of a network the client - the server is developed and experiment on attack of a network the client the server is made.

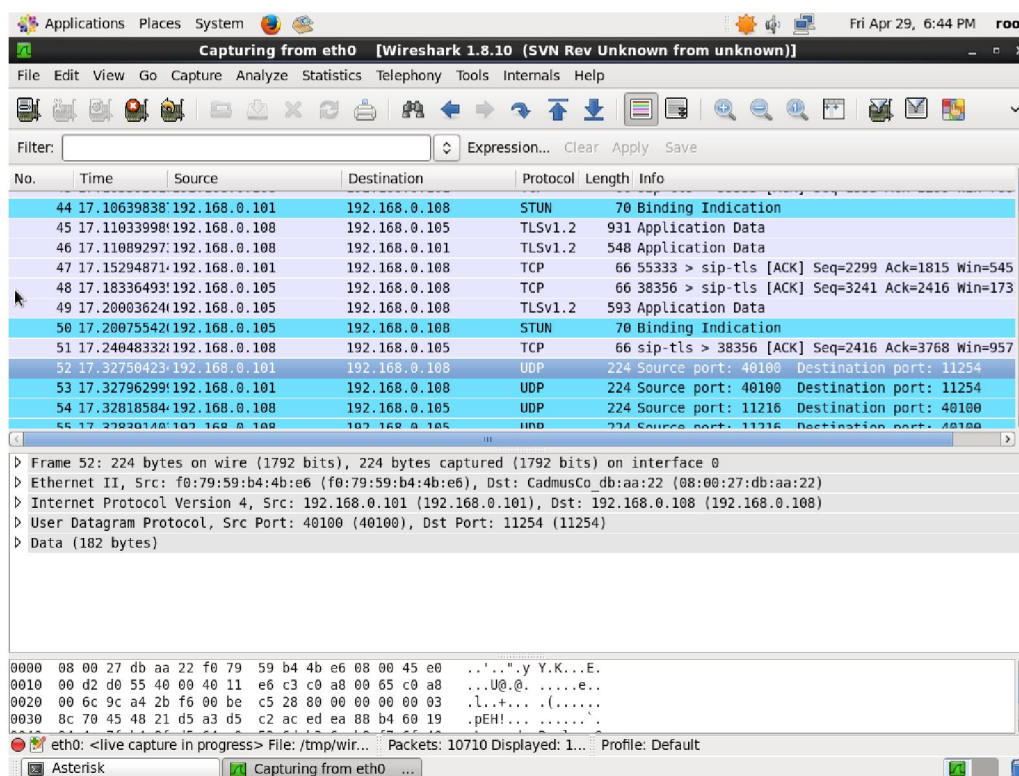


Figure 6 – The traffic protected from interception

On the developed scheme of a network on chair test on carrying out attack for the first time is carried out from the malefactor on a network for definition of weak spots to networks and offers of taking measures to its protection, problems are for this purpose solved on:

- To studying and development of the program instrument of modeling of attacks in the CommView for WiFi network.
- Experiments in the developed network of attack of the malefactor are made and results in drawings and tables of screenshots are given.

- On the basis of research of results of attack offers on taking measures of protection of a LAN (Local Area Network) are also developed.

REFERENCES

- [1] Nazarov I.A. (2013) Monthly electronic online the Security systems magazine 6:69-73 (in Rus.).
- [2] Goldstein B.C., Pinchuk A.V. (2001) IP-telephony. Radio and communication, Russian. ISBN: 5-256-01585-0.
- [3] Yakubova M.Z. (2013) POISK International scientific magazine-application of RK 2: 9-12 (in Rus.).
- [4] Goldstein B.S., Sokolov N.A., Yanovsky G.G. (2010) Communication networks. BHV, Russian. ISBN: 978-5- 9775-0474-4.
- [5] Yakubova M.Z. (2013) POISK International scientific magazine-application of RK 2: 28-30 (in Rus.).
- [6] Meggelen J., Madsen L., Smith J. (2007) Asterisk. The future of technology. O'Reilly Media, USA. ISBN: 978-0-596-51048-0.
- [7] Carpenter C., Duffet D., Middleton N., Plain I. (2009) Asterisk 1.4: Professional guide. PACKT, UK. ISBN: 978-847194-38-1.
- [8] Robar A. (2009) FreePBX 2.5: Powerful telephony solutions. PACKT, UK. ISBN: 978-1-847194-72-5.
- [9] Todd J. (2003) Asterisk: A Bare-Bones VoIP Example. O'Reilly Media, USA. ISBN: 978-0062417343.
- [10] Spencer M., Allison M., Rhodes Ch. (2003) The Asterisk Handbook: Version 2. Digium Inc. USA. ISBN: 0-47-98622-4.
- [11] Hellstrom G., Jones P.E. (2006) RTP Payload for text in an audio stream. Cisco systems Inc., USA. RFC 4351.
- [12] Goldstein B.S., Frankman V.A. (2002) Call-centers and computer telephony. BHV, Russian. ISBN: 5-8206-0105-X.
- [13] Baskakov I.V., Proletarskiy A.V., etc. (2008) IP-telephony in computer network. Intuit, Russia. ISBN: 978-5-94774-978-6.
- [14] Stallng W. (2001) Cryptography and Network Security: Principles and Practice. Prentice Hall, USA. ISBN: 978-0138690175.
- [15] McClure S., Scambray J., Kurtz G. (2004) Hacking Exposed: Network Security Secrets & Solutions. Osborne Media, USA. ISBN: 978-0072121278.
- [16] Sheglov A.Yu. (2004) Protection of computer information against unauthorized access. Science and technic, Russia. ISBN: 5-276-00641-5.
- [17] Mayvold E. (2016) Safety of networks. INTUIT, Russia. ISBN: 5-9570-0046-9.
- [18] Birukov A.A. (2012) Information security. Protection and attack. Press, Russia. ISBN: 978-5-94074-647-8.
- [19] Goldstein B.C., Goldstein A.B. (2006) Softswitch. BHV, Russian. ISBN: 5-8206-0117-3.
- [20] Raake A. (2006) Speech quality of VoIP: Assesment and prediction. Wiley, UK. ISBN: 978-0470030608.

М. З. Якубова¹, Т. Г. Серіков², А. К. Муратова³

¹Алматы Энергетика және байланыс университеті, Алматы, Қазақстан,

²ҚазақҰлттық техникалық университеті, Алматы, Қазақстан,

³Қарағанды Мемлекеттік техникалық университеті, Қарағанды, Қазақстан

ASTERISK БАЗАСЫНЫҢ НЕГІЗІНДЕ ІР-ТЕЛЕФОНИЯ ЖҮЙЕСІНДЕ ДЕРЕКТЕРДІ ҰСТАП ҚАЛУДАН ҚОРҒАУ

Аннотация. Қазіргі уақытта дауыс жіберу технологиясының дамуының жаңа кезеңін соның ішінде ІР-телефонияның қарқынды қолданыс тапқандығын байқауға болады. Жыл сайын ІР-телефонияға корпоративтік коммуникациялық инфрақұрылымның негізі ретінде сұраныс және қолданыс деңгейі өсіп келе жатуынан оның қауіпсіздігін қамтамасыз ету туралы сұрақ туындайды. ІР-телефонияның интернет желісіне тікелей кірісі болғандықтан абоненттердің аутентификациясы абоненттік ІР-мекенжайлар бойынша жүргізіледі. Мақалада телефонияның қауіпсіздігін Asterisk программасының негізінде клиенттердің деректерін жаулап алудан қамтамасыз ету амалын сипаттайды. Байланыс анализаторы ретінде Wireshark программалық өнім алынған. Программалық телефон және клиенттік база ретінде сынақ жүргізілген ноутбуктар, компьютерлер және гаджеттар алынған. Сынақтар жасалған кезде алынған нәтижелер бойынша желінің төзімділік анализі жасалынған. Рұқсатсыз байланыстан қорғану мақсатында ұсыныстар берілген. Желіні қорғауға арналған ең ұтымды шешім ұсынылды.

Түйін сөздер: ІР-телефония, протокол, мекен-жай, сымсыз шабуылдар, сервер, Asterisk.

М. З. Якубова¹, Т. Г. Сериков², А. К. Мурагова³

¹Алматинский университет энергетики и связи, Алматы, Казахстан,

²Казахский национальный технический университет, Алматы, Казахстан,

³Карагандинский государственный технический университет, Казахстан

ЗАЩИТА СЕТЕЙ IP-ТЕЛЕФОНИИ НА БАЗЕ ASTERISK ОТ ПЕРЕХВАТА ДАННЫХ

Аннотация. В настоящее время наблюдается новый виток развития технологий передачи голоса, а именно IP-телефония. В виду растущих уровней спроса и популярности IP-телефонии как основы построения корпоративной коммуникационной инфраструктуры возникает вопрос обеспечения максимально уровня ее безопасности. Поскольку сервер IP-телефонии имеет прямой выход в сеть Интернет, то и аутентификация абонентов происходит по IP-адресам. В данной статье решается вопрос обеспечения безопасности телефонии на базе Asterisk от перехвата данных клиентов. В качестве сетевого анализатора используется программное обеспечение Wireshark. В качестве софтбонов и клиентской базы рассмотрены ноутбуки, компьютеры и гаджеты, на которых проходит испытание. По результатам проведенных работ произведен анализ уязвимости сети. Даны рекомендации по мере защиты данных клиентов от несанкционированного доступа. В статье нами предложен наиболее оптимальный вариант защиты сети.

Ключевые слова: IP-телефония, протокол, адрес, беспроводные атаки, сервер, Asterisk.