Viktor GNATYUK[1], Nadiia DYKA[2], Vasyl KINZERYAVYY[3],
Sergii GNATIUK[4]

Opiekun naukowy: Roman ODARCHENKO[5]

METODA ZWIĘKSZENIA CYBERBEZPIECZEŃSTWA TELEFONII INTERNETOWEJ

Streszczenie: Zastosowanie telefonii internetowej (IP) w różnych sferach aktywności ludzkiej pozwala zwykłym obywatelom na ułatwienie sobie życia. Stosowana jest ona m.in.: aby realizować zadania biznesowe, takie jak zwiększenie sprzedaży, poprawę pracy zatrudnionych, podniesienie jakości usług dla klientów, automatyzację procesu pracy, dostarczania informacji koniecznych dla kierownictwa firmy i wiele innych. Używając telefonii internetowej jest ważne aby zapewnić konieczny poziom bezpieczeństwa informacji. Natomiast w przypadku braku tegoż aspektu, firma może narazić się na wielkie straty finansowe i wizerunkowe. Dlatego celem niniejszej pracy jest uniemożliwienie włamania się osób postronnych, czyli uniemożliwienie cyberataków w telefonii internetowej. Aby osiągnąć ten cel, opracowano metodę poprawienia cyberbezpieczeństwa telefonii internetowej poprzez identyfikację typów wrażliwości telefonii komórkowej. Dokonano tego poprzez identyfikację ciągu kroków, które dokonuje włamywacz (intruz) aby przeprowadzić cyberatak na telefonię komórkową. Umożliwia to identyfikację cyberataków oraz przeprowadzenie akcji prewencyjnych zwiększających poziom bezpieczeństwa. Opracowana metoda oraz narzędzia (z niej wynikające) będą użyteczne dla administratorów systemów, dla specjalistów z zakresu bezpieczeństwa informacji w odniesieniu do „CERT / CSIRT cyber incidents" (cyberataków) co ma istotne znaczenie dla zabezpieczania systemów informatycznych w przedsiębiorstwach i organizacjach.

Keywords: telefonia internetowa (IP), wydarzenie w sieci, Asterisk, SIP, ATS

[1] National Aviation University, Institute of Air Navigation, Electronics and Telecommunictions, Department of Telecommunication Systems, PhD, associate professor, victorgnatyuk@ukr.net
[2] National Aviation University, Institute of Air Navigation, Electronics and Telecommunictions, Department of Telecommunication Systems, PhD student, Nadin_dyka@ukr.net
[3] National Aviation University, Institute of Information and Diagnostic Systems, PhD, associate professor, v.kinzeryavyy@gmail.com
[4] State Service of Special Communication and Information Protection of Ukraine, Deparment of Electronics Communications Development, PhD, associate professor, gnatyuk-2@i.ua
[5] National Aviation University, Institute of Air Navigation, Electronics and Telecommunictions, Department of Telecommunication Systems, PhD, associate professor, odarchenko.r.s@ukr.net

METHOD OF INCREASING OF CYBER SECURITY IN IP-TELEPHONY

Abstract: Implementation of IP telephony in various spheres of human activity allows ordinary citizens to simplify their lives, to realize the main aspects of business: increasing sales, improving employee performance, improving customer service quality, automating work processes, providing the necessary information for management, and more. Using IP telephony is important to ensure that the necessary level of information security, because failure to implement this aspect can be a major financial and image loss. Therefore, the purpose of this work is to disable the implementation of intruders of cyber incidents in IP telephony. To achieve this, a method for improving the cyber security of an IP-telephony was developed, which, by identifying the types of vulnerabilities for IP telephony, identifying the sequence of steps that an intruder committed to implementing cyberattack on IP telephony and raising the level of information security of IP telephony. This allows identifying the possible types of vulnerabilities for IP telephony, investigating the sequence of steps for implementing cyberattack on IP telephony, and conducting preventive actions to increase the level of information security of IP telephony. The developed method and the tools formed on it will be useful for system administrators, for information security specialists in the response teams for CERT / CSIRT cyber incidents, which are assigned responsibilities for the protection of ITS within enterprises and organizations.

Keywords: IP-telephony, cyberincident, Asterisk, SIP, ATS

1. Introduction

Today, mankind has received a lot of interesting modern technologies, including IP-telephony, which in various spheres of human activity allows ordinary citizens to simplify their lives, to realize the main aspects of business: increasing sales, improving employee performance, improving customer service quality, automating work processes, providing the necessary information for management, and more. This technology has become a vivid symbiosis of classical telephony and the Internet. It combines all the most important functions of these technologies. The principle of operation of IP-telephony is that the voice of the subscriber is automatically transformed into data packets that are transmitted through the network to a given destination and immediately after that, they are converted to regular language. Telephony of this type directly belongs to broader category which received the name VoIP (Voice Over IP). Last allows to transfer by the same principle not only standard voice messages, and gives the chance to send different video files and similar messages. Such technology allows several times to minimize the load on the network. In parallel with it also the cost of stationary phone call decreases. To take advantage of the IP telephony, it is necessary to get specially developed devices. These are SIP phones and softphones. Not so many enterprises are engaged in production of the equipment of this direction. Particularly great successes were achieved by Grandstream and Cisco SB. Trademarks produce a wide range of devices for IP-telephony, constantly improving the quality of goods. The catalog includes models of IP-telephones with the following design features: with the leading tube, wireless,

LCD display, Wi-Fi, etc. Each such functional special feature enhances the user-friendliness of the device for this purpose.

2. Analysis of solutions and problem statement

Today, the market is represented by a large number of solutions for the construction of IP-telephony, but the undisputed leader is the free solution of computer telephony (including VoIP) with the open source Asterisk from Digium. Asterisk system architecture (Figure 1) includes: network, hardware, local operating system and components [1].

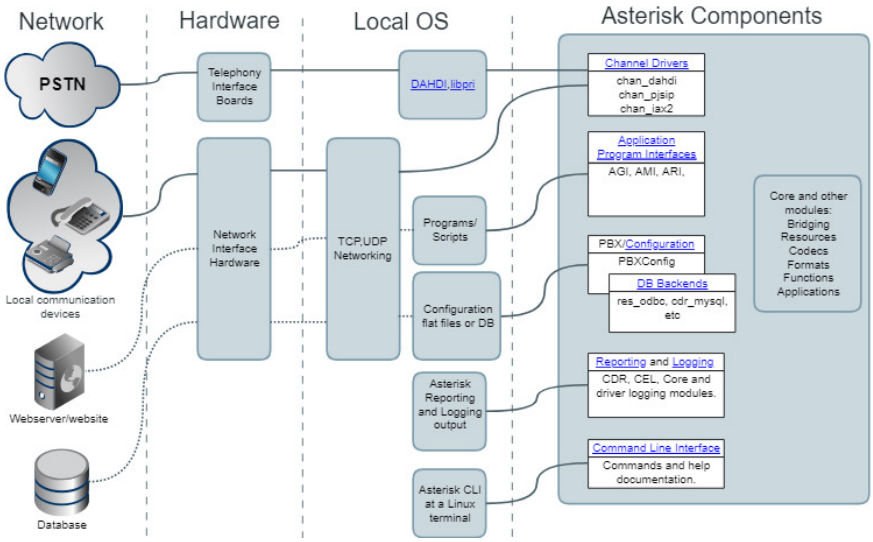

Figure 1. Asterisk system architecture

Asterisk in combination with the necessary equipment has all the features of the classic dial central office, supports a multitude of VoIP protocols (SIP, H.323, IAX2, MGCP, SIMPLE, SCCP, XMPP, Unistim) and provides functions for managing calls (voice mail, conference calls, IVR , call center, Call Detail Record), it is also possible to broadcast text and video signals. Support for a wide range of hardware and computer protocols allows you to organize a huge number of scenarios for network interaction, reception and processing of information. Asterisk can work with both analogue lines (FXO / FXS modules) and digital (ISDN, BRI and PRI T1 / E1 streams). By means of certain computer boards of Asterisk it is possible to connect to high-conducting the T1/E1 lines, that allow you to work in parallel with dozens of telephone connections.The complete list of equipment for connection to the telephone network of general use is determined by the support of equipment in the kernel modules.The typical diagram of the IP telephony Asterisk is shown in Figure 2.

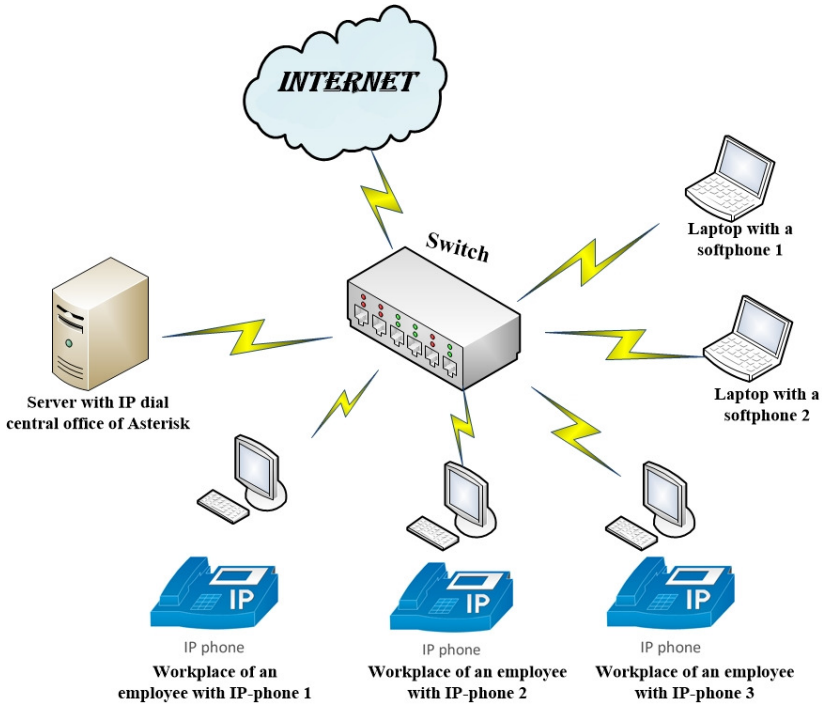

Figure 2. The scheme of the IP telephony Asterisk organization

By using the IP - dial central office of Asterisk, it is important to ensure that the necessary level of information security is ensured, since failure to implement this aspect can lead to significant financial and image losses. As a rule, "crack", realize cyber incidents [2], Asterisk from other countries and begin to make international calls, after such "cracking", to the organizations come accounts to scores for tens and even hundreds of thousands of dollars. What's interesting, the victim may become both like a large organization (which is not a fact), and so small. Basically, these are small organizations where the minimum attention is paid to the safety of Asterisk. Scanning of the Internet in search of the next victim continues constantly. By accessing Asterisk, malefactors can connect the purposes of the organization on the account of the victim and make international calls at their expense. Therefore, the purpose of this work is in making impossible implementation by malefactors of cyber incidents in IP-telephony, to achieve which, we will develop a method of increase in cyber security of IP-telephony, which, by identifying the types of vulnerabilities of IP-telephony, determination of the sequence of steps, that the attacker does to implementation of cyber attack on IP telephony and raising the level of information security of IP telephony, allows identifying possible types of vulnerabilities of IP-telephony, investigating the sequence of steps for implementing a cyber attack on an IP-telephony nity and performing preventive action to increase the level of information security IP-telephony. The developed method consists of the following stages.

Stage 1. Determination of types of vulnerabilities for the IP telephony. For implementation of this stage we will set a variety of types of vulnerabilities, which exist when functioning the IP telephony:

$$\mathbf{V} = \{\bigcup_{i=1}^{n} \mathbf{V}_i\} = \{\mathbf{V}_1, \mathbf{V}_2, ..., \mathbf{V}_n\}, \quad (i = \overline{1, n}), \tag{1}$$

where n – the number of possible types of vulnerabilities.

For example, as a result of carrying out the analysis of the existing types of vulnerabilities during functioning of the IP telephony [3-11] we will create the table for IP dial central office of Asterisk of tab. 1.

Table 1. Types of vulnerabilities for IP dial central office of Asterisk

№	Code	Description
1	NCF	Asterisk, for some reason, has a dedicated IP address and is displayed on the Internet (for example, this Asterisk server is the same as the Internet-distributing server, so that the wire with the Internet and the dedicated white IP is inserted directly into this server). At the same time, on the Asterisk server does not have a firewall configured, and this Asterisk is vulnerable on the network side.
2	DP	SSH and SIP have default ports.
3	SP	Simple passwords for SIP of clients are used.
4	BSF	The protection function is not enabled for scanning existing SIP clients.
5	FSD	The protection function at the Dial plan level is not implemented.
6	FSA	The access function only from the local network is not implemented.
7	SA	SSH is allowed to access root user.
8	LE	In Linux unnecessary services with holes doesn't are disconnected.
9	AV	The system with the PBX interface, for example Elastix which has additional vulnerabilities is used.
10	ICA	At the SIP provider's level, international calls are allowed (when they are not required).
11	LF	At the level of SIP provider restriction function isn't realized (call as many as you like, but at the end of the month you will receive an invoice).

Consequently, using expression (1) and data from Table 1, at n = 1 we obtain:

$$\begin{aligned} \mathbf{V}_A &= \{\bigcup_{i=1}^{n} \mathbf{V}_i\} = \{\mathbf{V}_1, \mathbf{V}_2, \mathbf{V}_3, \mathbf{V}_4, \mathbf{V}_5, \mathbf{V}_6, \mathbf{V}_7, \mathbf{V}_8, \mathbf{V}_9, \mathbf{V}_{10}, \mathbf{V}_{11}\} = \\ &= \{\mathbf{V}_{\text{NCF}}, \mathbf{V}_{DP}, \mathbf{V}_{SP}, \mathbf{V}_{BSF}, \mathbf{V}_{FSD}, \mathbf{V}_{FSA}, \mathbf{V}_{SA}, \mathbf{V}_{LE}, \mathbf{V}_{AV}, \mathbf{V}_{ICA}, \mathbf{V}_{LF}\} = \\ &= \{NCF, DP, SP, BSF, FSD, FSA, SA, LE, AV, ICA, LF\}, \end{aligned} \tag{2}$$

where $\mathbf{V}_1 = \mathbf{V}_{\text{NCF}} = NCF$, $\mathbf{V}_2 = \mathbf{V}_{DP} = DP$,…, $\mathbf{V}_{11} = \mathbf{V}_{LF} = LF$ – types of vulnerabilities for IP dial central office of Asterisk.

Stage 2. Determining the sequence of steps to implement cyberattack on IP telephony. To realize this stage, we will set a host of steps for implementing a cyberattack on IP telephony:

$$\{\bigcup_{i=1}^{n}\mathbf{S}_i\}=\{\mathbf{S}_1,\mathbf{S}_2,...,\mathbf{S}_n\}, \tag{3}$$

where $\mathbf{S}_i \subseteq \mathbf{S}$, $(i=\overline{1,n})$, n – quantity of steps of the malefactor.

For example, we will consider the sequence of steps for implementation of cyber attack to the IP dial central office of Asterisk (tab. 2).

Table 2. Description of steps to implement a cyber attack on the IP dial central office of Asterisk

№	Code	Description
1	**SC**	Scanning of the Internet on existence of systems with open port 5060 (clients of SIP traditionally use port 5060 TCP and UDP for connection of servers and other SIP elements, mainly SIP is used to set up and disconnect voice and video calls).
2	**SL**	Asterisk is found, search of the available SIP of clients to whom it is possible to be connected. Sending requests until you come to the answer that such an SIP client exists. As a result, the malefactor receives the list of a look: [1000] [1001] [1002] - these are SIP clients.
3	**BF**	Launch of " brute force" - programs for selecting a password for SIP clients.
4	**SR**	Having found the password, the malefactor launches a softphone on his computer and registers it on the received data - the external IP address (which he found by scanning the open 5060 ports, the login (which is the same as the number of the SIP client he found) and the password that he picked up as a result of the " brute force ".
5	**MC**	The attacker can make international calls, and so on.

So, using expression (3) and data from Table 2, at n = 5 we obtain:

$$\mathbf{S}_A=\{\bigcup_{i=1}^{5}\mathbf{S}_i\}=\{\mathbf{S}_1,\mathbf{S}_2,\mathbf{S}_3,\mathbf{S}_4,\mathbf{S}_5\}=$$
$$=\{\mathbf{S}_{SC},\mathbf{S}_{SL},\mathbf{S}_{BF},\mathbf{S}_{SR},\mathbf{S}_{MC}\}=\{SC,SL,BF,SR,MC\}, \tag{4}$$

where $\mathbf{S}_1=\mathbf{S}_{SC}=SC$, $\mathbf{S}_2=\mathbf{S}_{SL}=SL$, $\mathbf{S}_3=\mathbf{S}_{BF}=BF$, $\mathbf{S}_4=\mathbf{S}_{SR}=SR$, $\mathbf{S}_5=\mathbf{S}_{MC}=MC$ – he malefactor's steps for cyber attack realization on the IP dial central office of Asterisk.

Stage 3. Increasing the level of information security of IP-telephony.

To realize this stage, we will set a host of actions to increase the level of information security IP-telephony:

$$\mathbf{A} = \{\bigcup_{i=1}^{n} \mathbf{A}_i\} = \{\mathbf{A}_1, \mathbf{A}_2, ..., \mathbf{A}_n\}, \quad (5)$$

where $\mathbf{A}_i \subseteq \mathbf{A}$, $(i = \overline{1,n})$, n – a number of actions to increase the level of information security IP-telephony:

For example, consider actions to increase the level of information security for the IP dial central office of Asterisk table 3.

Table 3. .Actions to increase the level of information security for the IP dial central office of Asterisk

№	Code	Description
1	CS	Change of SIP port (bindport = 3348;)

2	SL	The prohibition SIP of connections outside a local area network (deny = 0.0.0.0 / 0.0.0.0;
		permit = 192.168.0.1 / 24;
		allowguest = no;
		call-limit = 2;)

3	SS	Protection of the server against search according to numbers (Alwaysauthreject = yes)
4	IC	Establishment of difficult passwords for SIP clients (you can use a password generator, a password with office signs and numbers)
5	SI	Blocking international calls at the level of Dial's plan (exten => _3809X.,1,System(echo «To» ${EXTEN} «Ext» ${CALLERID(num)} | mail -s «8-10 ALARM» test@gmail.com); exten => _3809X.,n,Hangup();)
6	CF	Configure iptables embedded firewall (editing configuration file iptables)
7	CP	Change of SSH port, interdiction to the user "to log in" as root through SSH, we add the new user (useradd username, passwd username; AllowUsers username, PermitRootLogin no; Port 1265)
8	DA	Turn off Apache from startup and change its port (chkconfig httpd off, IP_адрес_сервера: 7623)
9	DM	Disable Unnecessary Modules and Protocols of Asterisk (noload => chan_jingle.so noload => chan_skinny.so noload => chan_iax2.so noload => chan_console.so noload => chan_mgcp.so noload => chan_gtalk.so)
10	CM	Change the Asterisk control port (AMI) (port = 8374)

11	SF	Customize the system fail2ban (the protection program of servers from the attack «Brute force»).
12	SD	Protection against DOS attacks (we modify iptables): (-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445 -m recent --set --name dos-attack -A INPUT -p tcp -m multiport --dports 1265, 7623,3348,137,138,139,445 -m recent --update --seconds 2 --hitcount 20 --name dos-attack -j DROP) Also, iptables can be linked to the fail2ban system in such a way that packets from the DOS attack are not discarded, and their messages are logged in the iptables log file. File2ban is based on the template, looks at log / var / log / messages and if it sees such a message in this log, it simply blocks the IP address that sends these messages and informs us by email that the DOS attack was carried out.
13	SSP	protection from port scanning (iptables - xtables-addons)
14	SSH	SSH certification. SSH certification. There is an opportunity to do so that you can connect to SSH (for example, through Putty) only if the computer that connects to the Linux server has a certificate installed. The general procedure is as follows: 1) Generating keys. 2) The generated key is entered into the authorized_keys file. 3) Generated key is extracted from Linux in Windows. 4) The extracted generated key using the puttygen program is converted. 5) The resulting converted file is connected to Putty. 6) Set up service SSH in Linux. 7) Check of working capacity.
15	ES	Disconnection of samba (; Path; chkconfig smb off)
16	DP	At the level of provider it is also possible: the prohibition of international calls, establishment of limits, restriction of the maximum cost of calls.
17	OE	Establishment of the protected VPN connection, establishment of difficult passwords to web interfaces of the hardware phones, change of HTTP port.

So, using expression (5) and data from Table 3, at n = 17 we obtain:

$$\mathbf{A}_A = \{\bigcup_{i=1}^{17} \mathbf{A}_i\} = \{\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4, \mathbf{A}_5, \mathbf{A}_6, \mathbf{A}_7, \mathbf{A}_8, \mathbf{A}_9, \mathbf{A}_{10}, \mathbf{A}_{11}, \mathbf{A}_{12}, \mathbf{A}_{13}, \mathbf{A}_{14}, \mathbf{A}_{15}, \mathbf{A}_{16}, \mathbf{A}_{17}\} =$$
$$= \{\mathbf{A}_{CS}, \mathbf{A}_{SL}, \mathbf{A}_{SS}, \mathbf{A}_{IC}, \mathbf{A}_{SI}, \mathbf{A}_{CF}, \mathbf{A}_{CP}, \mathbf{A}_{DA}, \mathbf{A}_{DM}, \mathbf{A}_{CM}, \mathbf{A}_{SF}, \mathbf{A}_{SD}, \mathbf{A}_{SSP}, \mathbf{A}_{SSH}, \mathbf{A}_{ES}, \mathbf{A}_{DP}, \mathbf{A}_{OE}\} = \quad (6)$$
$$= \{CS, SL, SS, IC, SI, CF, CP, DA, DM, CM, SF, SD, SSP, SSH, ES, DP, OE\},$$

where $\mathbf{A}_1 = \mathbf{A}_{CS} = CS$, $\mathbf{A}_2 = \mathbf{A}_{SL} = SL$, …, $\mathbf{A}_{17} = \mathbf{A}_{OE} = OE$ – Actions to increase the level of information security for the IP dial central office of Asterisk
Thus, following the steps listed in Table. 3 we will significantly increase the level of information security for the the IP dial central office of Asterisk. For a successful implementation of cyber attacks with such settings a very high level of intruder qualification and significant logistical costs is required.

3. Conclusion

Thus, in this work the method of increasing the cyber security of an IP-telephony is developed, which, by identifying the types of vulnerabilities for IP telephony, , identifying the sequence of steps that an intruder committed to implementing cyberattack on IP telephony and raising the level of information security of IP telephony, allows identification possible types of vulnerabilities for IP telephony, investigate the sequence of steps for the implementation of cyberattack on IP telephony and, as a preventive measure, increase the level of information security of IP telephony.

The developed method and the tools formed on it will be useful for system administrators, for information security specialists in the response teams for CERT / CSIRT cyber incidents, which are assigned responsibilities for the protection of ITS within enterprises and organizations.

REFERENCES

1. Asterisk Architecture: [Electronic resource]. Access mode: *https://wiki.asterisk.org/wiki/display/AST/Asterisk+Architecture%2C+The+Big+Picture*
2. GNATYUK VO: An analysis of the definitions of the concept "incident" and its interpretation in cyberspace. Information security 3(2013)19, 175-180.
3. MAGGELEN J., MADSEN L., SMITH J. ASTERISKTM: The Future of Telephony, 2nd Edition. 2009.
4. PLATOV M.: Asterisk and Linux - mission IP telephony [Text] - M. Platov System administrator (2005)31, 10-38.
5. Knowledge base of Asterisk: [Electronic resource]. Access mode: asterisk.ru/knowledgebase.
6. Knowledge base of Voxlink [Electronic resource]. Access mode: *www.voxlink.ru/kb*.
7. Security in VoIP Networks: [Electronic resource]. Access mode: *habrahabr.ru/post/145206*.

8. ROSLYAKOV AV, SAMSONOV M.YU., SHIBAEVA IV IP telephony. Eco-Trendz, 2003.
9. GOLDSTEIN B.S., PINCHUK A.V., SUKHOVITSKY A.L.: IP telephony. Radio and communication 2001.
10. CITForum IP telephony security - field sketches. A.: [Electronic resource]. *Access mode: citforum.ru/security/articles/ipsec.*
11. 9 rules to protect your Asterisk !: [[Electronic resource]. Access mode: *https://habr.com/company/myasterisk/blog/130325/.*