Bekala Katazhyna
5th-year student, faculty Cybersecurity, computer and software engineering
National Aviation University
Kyiv, Ukraine

A METHOD OF PROTECTION OF INFORMATION IN IP-TELEPHONY NETWORKS AGAINST UNAUTHORIZED ACCESS BASED ON ASTERISK PBX

Annotation: The article is devoted to the consideration of the problem of increasing the level of security of the IP-telephony network and access to confidential information within this network. The paper proposes a method for delimiting access to telephony by blocking unauthorized IP addresses and entering a blacklist of permitted, suspicious operations. The example of such operations may be password, which was incorrectly entered several times. And also the way to determine the burglary, if the above checks were successfully passed. The algorithm and block diagram of the blocking system operation of a unique network address that implements the proposed method are considered in the paper.

Keywords: network protection, IP telephony, VoIP, cybersecurity, network access, protection against unauthorized access, protection of information in networks, system vulnerabilities, system protection.

I. INTRODUTION

The 21st century is characterized by the dynamic development of the information technology industry. It is impossible to imagine an enterprise or a person, who does not use achievements of this industry. The more technology is used, the more cybercriminals are interested in it.

VoIP is based on IP technology and uses the Internet, it also imitates all their vulnerabilities. In addition to imitators, IP telephony has vulnerabilities that arise from the features of VoIP network architecture. All of these vulnerabilities create the need for enhanced security and thorough network analysis. The consequences of IP telephony attacks can be: theft of calls, server crashes, as well as theft of personal data and subsequent actions with them. To date, one of the most important tasks of IP-telephony are to protect the network, improve existing ones, or implement new methods of counter-attack.

When using a global network in a security system, it is based on the use of access control and authorization systems, i.e. it contains the following tasks:

- Identification is the procedure for recognizing a user on a system, that is, establishing a correspondence between a subscriber who connects via a remote access channel to another IP telephony client or clients. Customers are identified by their username and IP address.
- Authentication – action the confirms a subscriber's authority to use the customer ID he / she entered. That is, the check or caller is really who he/she pretends to be. Authorization is the granting of rights to a user to access resources and to perform certain actions, as well as the process of verifying and confirming these rights when attempting to perform these actions.
- Discharge integrity control is a complex of measures that makes it impossible to change or withhold an order when transmitting from a subscriber to the system via a remote access channel.
- Confidentiality is the prevention of the transmitted data via a remote access channel to a third party.

Thus, the urgency of the task of ensuring the security of IP-telephony networks is associated with widespread use in various organizations, enterprises and institutions, and the great interest of the attackers in this field. So that is one of the more important tasks of IP-telephony is to secure the network, improve existing ones or implement new methods of counter-attack.

II. FORMULATION OF THE PROBLEM

The great interest of cyber-criminals in IP-telephony networks is growing at a fast pace, in parallel with an increase in the number of users. Such kind of interest usually causes attacks on the network. The consequences of attacks can be as following: theft of calls, server failure, as well as theft of personal data and further actions with them.

The complication and number of attacks on VoIP servers continue to increase. Automatic port scanning and security sensing are used many times a day. Each new attack attempt is from another IP, and potential hackers use the botnet. This makes it more difficult to block them by firewall. Another difficulty in blocking attacks is that the source address is intentionally tampered. Such actions make it difficult to identify the true sender address, which is disguised as "noise" generated random addresses.

IP Telephony (VoIP) is a set of communication protocols, technologies and methods that provide traditional two-way voice messaging for telephony, as well as video messaging over the Internet or other IP networks. Today, most businesses use VoIP for both external and internal communications. The use of IP-telephony systems allows companies to significantly reduce the cost of calls, especially international ones, and integrate telephony with Internet services and provide intelligent services.

Thus there is a need to improve existence or to develop a new method of combating attacks that can circumvent these problems. Especially important is the creation of subsidiary or firewall applications replacing to block suspicious random IP-addresses.

III. FORMULATION OF PURPOSE AND TASKS

The purpose of the work is creation algorithm of method of protection of information in ip-telephony networks against unauthorized access based on Asterisk PBX.

According to the purpose of the work it is necessary to solve the following tasks:

- To explore IP telephony network;
- To analyze IP telephony vulnerability;
- To develop an application to block unwanted IPs.

The scientific novelty of the research is the following: the algorithm of blocking of intruders and definition of other necessary components of system of protection are developed and implemented. The algorithm helps to protect the network more carefully, and is able to prevent repeated attacks.

The practical value of the work is that the method, applied in the system, provides reliable protection against possible threats and creates a strong counter attack against attackers. This ensures the stable operation of the network and the protection of personal data of users from leakage, as well as the secrecy of telephone conversations.

IV. MAIN PART

The method is developed to determine the user IP address authenticity when logging in to the network and filtering addresses with a block of false or suspicious actions when trying to access valid addresses. This method avoids attacks that pretend being undetected. The application of this protection option can be used in all closed IP-networks. Solving the problem of the networks protection is thus possible by registering at the IP address of the address for further authorization. The algorithm is able to reduce the frequency of false authentication attempts. The method shown in this work is great for protecting the system against DDOS, called denial-of-service attacks and brute-force attacks, making it impossible to change numbers (prevents IP addresses from being tampered with).

The first part of the method is the IP address filtering. Since IP telephony is a private network, there is a specific list of users who have access to the system. That is, the first step is to check if there is an address trying to access the filter range. If there is an address, access is granted, if not, it is blocked.

The second part of the method is that the program scans log files and forbids IP addresses that detect signs of harmful activity. Such signs include a large number of password crashes, searches for exploits. Addresses marked with such features are blocked at a specified time using the iptables management interface. The method is a security policy that can also set conditions for usernames and passwords, which allows you to prevent from a weak authentication problem. The second step allows you to prevent a deliberate change of address and interference to the network through any access to the computer.

The third part gives an opportunity to determine the substitution of CallerID, through the analysis of the SIP package contents, which causes the real end user to be identified. This helps to protect the system from indirect hacking (when a cyberattack is performed on a user of the system who has passed all stages of verification).

In a set of three stages, the method gives a powerful deflection to attacks, especially attacks such as "denial of service and break the password by the method of full scan. The method works independently of other Asterisk protocols, so its operation cannot damage its own communication work.

This method of protection also includes the following components of the IP network protection system: complex password policy, disabling the response to the wrong password and blocking access after unsuccessful attempts to register. In addition, this approach perfectly complements other components. Such as the use of firewalls, encryption of telephone conversations and the actual use of VPN.

In addition, the connection and voice session of the identified clients is secure. The basis of any secure connection is cryptography. Cryptography is called the technology of addition, that is, encryption, and decryption of encrypted messages. In addition, cryptography is an important component in ensuring integrity, confidentiality, and authentication. Authentication is a mechanism for verifying, verifying the identity of the sender or recipient of the information. Integrity assumes that the data was not subject to change during the transfer, and confidentiality provides conditions under which no data will be understood by anyone except the sender and the recipient to whom it was addressed. Typically, the mechanisms of cryptography appear in the form of an algorithm, namely a mathematical function, and a secret value, that is, a secret key. The algorithms used are widely known, so only cryptographic keys should be kept secret. The reliability of a key depends on its size, that is, the more bits in such a secret key, the less vulnerable it is.

Unlike existing some analogs, this method has a number of advantages. Firstly, it is used particularly in Asterisk, that is, there is no need to set anything. Secondly, it can run without a firewall, in opposition to an analog that only complements the firewall. Thirdly, the method can be used as a security policy for network logon, while the analog cannot affect weak authentication. Fourthly, the method does not provide constant monitoring of the system.

The block diagram of the algorithm is used for protecting the IP-telephony network from unauthorized access by the method of blocking IP-addresses is shown in Fig. 1. When attempting to connect to the network, authorization is initiated at the IP address initially (each address may have its own specific rights). At the same time, defining the rights, it checks if there is this IP address within the filter. If the authorization fails, the address immediately falls into the ban, and only administrator can unblock it. If it is successful - check the authorization (determine whether the specified login and password is valid). If authentication fails (5 attempts), lock at the given time. You can unblock both the administrator and the system automatically after the coincidence of the specified time. If it is successful - the user can use his authority on the network.

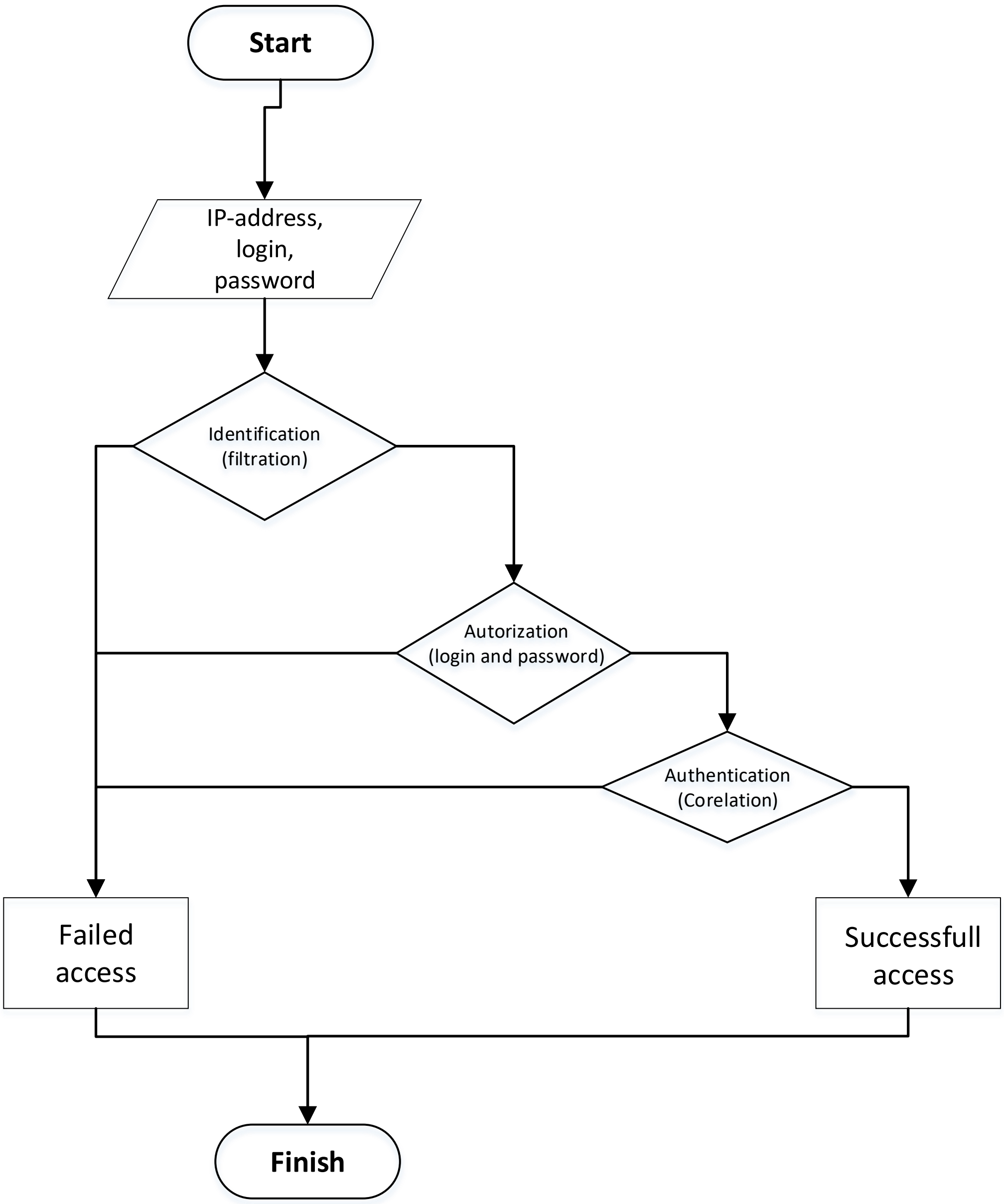

Fig.1. Block diagram of the method algorithm method of blocking IP-addresses

The method demonstrated in the article will provide better protection for the IP-telephony system when using a network security system. Such system includes appropriate settings of VoIP server, use of firewalls, encryption of telephone calls. For example, use a combination of TLS and SRTP protocols to encrypt voice data on a network and transmit voice data between remote users through an encrypted tunnel, namely IPsec. The application of the created algorithm of blocking of IP-addresses will allow to improve the security system. Using all of the above methods in combination will provide improved security of information within the network and with remote users.

Also ensuring safe operation of IP systems requires the client to follow the following common guidelines:

- keeping secrets and not passing on to third parties their own passwords, one-time code tables, cryptographic key carriers and other means of network access;

- use of computers and other communications technologies whose software is fully controlled by the client for use on systems;

- Immediately lock your account in case of loss of passwords, one-time code tables, cryptographic key carriers or other means of accessing the IP telephony network, and when access to a third party network is detected.

V. CONCLUSIONS

The article shows the method of information security in IP-telephony networks from unauthorized access based on Asterisk ATS. This method can potentially increase the security level of IP-telephony networks and reduce the possibility of interruption the network and the stealing of personal data as well as the usage of it. It also includes not only ways to prevent intrusion directly into IP telephony, but also a method for recognizing a trusted SIP client. The method of protection against suspected interference presented in the article takes into account the fact that upon access to the system by a third party or a group of persons, all means have been taken to minimize the losses during a successful hacking attempt.

The main problem reffers to IP-telephony security is that they are too open, and violators can attack their components relatively easily. Despite the fact that such attacks are not yet widespread, hackers can optionally carry them out, since attacks on traditional IP networks can be directed almost unchanged to the transmission of digital signal, voice or video. On the other hand, the similarity between conventional IP networks and IP telephony networks also tells us how to protect them. Thanks to the developed system it is possible to prevent attacks on the system of IP-telephony and to minimize losses in case of successful attempt of intervention. Also, in the article the block diagram and the principle of the algorithm of the proposed method are considered.

The proposed method and system can be used when using IP-telephony networks for communication on Unix-like platforms and the usage of the Putty application by Windows software users.

It is important to remember that malicious attacks are applicable to both traditional and IP telephony. The question is that detecting, locating and preventing threats in the IP telephony system is a much simpler and less costly task. In this case, the cost of IP-telephony is significantly lower than analog. The task is to properly implement and debug the IP system and ensure its smooth running with minimal risk aversion. Security features were explored at TIS Telecom.

References:

1. L. Madsen, J. V. Meggelen, J. Smith “Asterisk: The Future of Telephony”, 656, 2015

2. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1. – Харків: Вид. ХНЕУ, 2008. – 352 с.

3. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. Пособие для студ. Высш.учеб. заведений – М.: Издательский центр – Академия, 2005. – 8с.

4. Демпстер Б. Gomillion D. Побудова систем телефонії за допомогою Asterisk – Birmingham: Packet Publishing, 2005. – 176 с.

5. Bekala Katarzyna. Algorithm for protecting access to confidential information in IP-telephony networks // Европейская наука XXI века. – 2018.– с. 55-58.

6. Корниенко Б.Я., Бекала К.И., Галата Л.П. Исследование уязвимостей сетей IP-телефонии // Тенденции современной науки. – 2018. – с. 39-42.

7. Бекала К.И. Алгоритм защиты сетей IP-телефонии от несанционированного доступа // Комп’ютерні системи і мережні технології. – № 11, 2018. – с. 9-10.

Данилов Александр Петрович
Инженер-механик, горный инженер
Автор теории Поглощения энергии,
советник генерального директора
ООО «Компания «Восточный уголь»,
121059, г. Москва ,
Деулин Евгений Алексеевич
,Доктор технических наук,
профессор МГТУ им. Н.Э.Баумана
105005, Москва

УДК 533.5:614.839.54:620.9:661.9:622.235

ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ ВОДОРОДО -СОДЕРЖАЩИХ ОТХОДОВ ПРИ ШАХТНОЙ ДОБЫЧЕ УГЛЯ

Аннотация. В статье говорится, что атомарный водород, являющийся попутным видом топлива при добыче каменного угля появляется в виде раствора атомов водорода в частицах угольной пыли, являющейся продуктом воздействия рабочего органа комбайна или струговой установки на добываемый уголь. Мелкая угольная пыль, появляющаяся во время добычи угля и оседающая на стены и пол выработок шахт и, отдельно, забоев представляет собой «вакуумную взрывчатку», которая представляет собой опасность, с другой стороны она представляет собой уже, обогащенное водородом топливо, которое нам надо научиться утилизировать для получения дополнительной прибыли при угледобыче и на ТЭЦ, что нано-структурированное топливо в 2-3 раза дешевле дизельного топлива и приближается низкой стоимости водоугольного топлива, хотя по теплотворной способности значительно превосходит последнее, приближаясь к дизельному топливу.

Abstract. The article states, that atomic hydrogen, which we consider as a by-product of coal mining appears as a solution of hydrogen atoms in the particles of coal dust, which is the product of the impact of the working body of the combine or plow installation on the extracted coal. Fine coal dust that appears during coal mining and settles on the walls and floor of mine workings and, separately, the faces is a "vacuum explosive", which is a danger, on the other hand, it is already hydrogen-enriched fuel, which must be learned to recycle for additional profit in coal mining and in the mills of thermal power plants, we show that nano-structured fuel is 2-3 times cheaper than diesel fuel and approaching the low cost of coal fuel, although the calorific value is much superior to the latter, approaching the diesel fuel.