International Journal of Wireless Communications and Mobile Computing
2016; 4(3): 56-61
http://www.sciencepublishinggroup.com/j/wcmc
doi: 10.11648/j.wcmc.20160403.11
ISSN: 2330-1007 (Print); ISSN: 2330-1015 (Online)

Commentary

Study SIP Protocol on Asterisk Phone System and Offer Solutions to Its Security

Hadi Abdolmaleki, Masoud Masomi, Mohamad Noroozi, Fatemeh Mirzaei

Telecommunication Department of Non-profit Institution of Higher Education, ABA University, Abyek, Qazvin, Iran

Email address:

Hadi.voip@gmail.com (H. Abdolmaleki), massoud_masoumi@yahoo.com (M. Masomi), noroozi.62@gmail.com (M. Noroozi), fmirzaei_91@yahoo.com (F. mirzaei)

To cite this article:

Hadi Abdolmaleki, Masoud Masomi, Mohamad Noroozi, Fatemeh Mirzaei. Study SIP Protocol on Asterisk Phone System and Offer Solutions to Its Security. *International Journal of Wireless Communications and Mobile Computing.* Vol. 4, No. 3, 2016, pp. 56-61.
doi: 10.11648/j.wcmc.20160403.11

Received: May 31, 2016; **Accepted**: June 13, 2016; **Published**: June 23, 2016

Abstract: Undoubted every organization's heart is it's phone system. The old phone systems couldn't perform any method to make phone center and voice transmission intelligent on network and they had determinate abilities. Meantime Voice over Internet Protocol (VoIP) introduced itself to the world and performed a lot of abilities for clients like voice transmission on network. Many companies Investment on voip systems and implemented their methods on software and hardware packages. But between them a different production had designed and Performanced by Mark Spenser from Digium Company in 1992 which named Asterisk. Asterisk's increasing popularity's reason was its open code programs and its flexibility. VoIP systems such as Asterisk use voice transmission protocols to transfer voice over network. One of the voice transmission protocols is Session Initiation Protocol (SIP), which is one of the Asterisk's voice transmission protocols. The first and the most important point in voice transmission over network is security. Security can be divided to two parts as inscrutability of invaders to network and coding transmitted voices over network to prevention of illegal listening. In this project at first we tried to introduce Asterisk phone system's structure and Session Initiation Protocol (SIP) and then scrutiny method of Invader's dominance to this protocol and Performance modern methods to prevent hacker's dominance and also coding voice packages to Obscure them in transmission way.

Keywords: Asterisk, Phone System, Security

1. Introduction

Today, telecommunications play a significant role in every large and small business. The need for that arose when staff in an organization had to go to visit each other for any conversation.

Companies tried to provide telephone lines to avoid comings and goings and facilitate establishing relationship with their employees for customers and corporate insiders.

The high cost of telephone lines and inability to control users made companies tend towards internal telephone systems. A large number of companies began to build analogue phone centers and provide facilities like the independence from using telephone lines for doing communications inside organization and they conducted incoming calls by an operator.

Such companies made their own systems more advanced by improving their efficiency and adding more facilities like controlling the incoming and outcome calls and answering menu of the organization to direct the incoming calls efficiently.

The demands of the companies increased so that conventional phone centers were no longer able to satisfy them and offer newer services.

At that time VOIP technology (voice over internet protocol) introduced telecommunications over internet and offered facilities beyond what conventional telecommunications offered- facilities offered by telecommunications over internet include voice transmission over internet and the removal of any constraint about telephone cabling.

These telecommunications required only a stable network

for voice transmission so that they can establish a telecommunication. This network may be a very simple one inside the organization or a national (internet) or even an international one.

So the first step VOIP technology took was the elimination of any constraint of location from telecommunications inside organization.

Due to the emergence of VOIP technology, various companies started to establish telecommunications over internet and produced different hardware and software products and the most famous ones among them include Sisco, Avaya, Mytel, Asterisk phone centers and so on. In addition to the advantage of voice transmission, there are other extraordinary benefits in these products including the recording and controlling conversations, increasing the efficiency by making telecommunications intelligent, visual connection, etc.

Among the mentioned products, Asterisk which is supplied by Digium Company was the most popular one compared to the others and this was due to high facilities provided by this phone center open text of its software.

In all phone centers over internet, voice transmission is done by its protocols. In order to use the products developed by the manufacturers of VOIP devices, a single protocol was considered and changed into a standard one in this area to create a common language and that was SIP (Session Initiation Protocol).

One of the used protocols for transmitting voice over internet is SIP.

Despite the advances of technology and changing conventional phone centers to VOIP, these centers have been threatened more than the conventional phone centers and this was because of establishing connection in the form of data packages over internet. It can be said that as long as a network used for a telecommunication has no contact with the outside world, those threats are not tangible and even they may not exist. However, you encounter major threats when you use internet for telecommunications and some hackers may access to your system and this incurs high costs and thereby, hackers would misuse exchanged information over your phone system.

To prevent this, we need to enhance the security of our system and encode vocal data so that hackers cannot listen to them.

2. Materials and Methods

VOIP is the abbreviation for “voice over internet protocol” which means transmitting voice over internet.

A set of laws which determine the way of exchanging information are called “protocol”. You can consider it as the common language between two systems. Protocol which is run to transfer data over internet is called Internet Protocol (IP).

To digitize voice, binary numbers are changed into digital format and allow for data transfer based on available IP. Process which is done for sending voice traffic over IP is called “VOIP” (voice over IP-VOIP).

In this technology, voice transmission is carried out in a digital format based on sending and receiving data packages.

To transfer data, we need a suitable network and this can be either intranet or internet.

Human voice is an analogue signal. Therefore, at the source a transducer is used for transforming analogue signal to digital one. Since voice must be changed into data packages in order to be transmitted through IP, voice signal needs to be digitized.

Fig. 1. *Process of data transfer.*

2.1. Asterisk

Fig. 2. *Asterisk.*

Asterisk was founded by Mark Spenser, the CEO of Digium company, in the format of GNU/GPL in 1999. Asterisk is a step towards generalizing different communication methods based on computer networks for telecommunications, visual connections and relevant applications such as IM, call/contact center… With the growth of communications based on IP based computer networks, Asterisk gained a high popularity. Being free compared to the high costs of current brands in the market, potential facilities with appropriate quality, standard protocols and independence from a special hardware, ease of use and installation, wide range of information society and more importantly, the integration of voice services (including telephone and chat), visual services and data caused Asterisk as a Soft Switch to be regarded as one of the effective components in modern communications world of next generation. Asterisk is based on programming language C and it is loaded on various operating systems such as Linux, Net BSD, Solaris and Unix. Moreover, we can make Asterisk services operational using computers and conventional servers and calculating the system power (CPU/RAM) according to the number of users. However, the popularity of Asterisk and diversity of the services it offers encouraged many manufacturers to utilize a combined platform provided by Linux and Asterisk for making unified communications at different scales.

In practice, it is easy to produce simple, inexpensive and efficient tools on the one hand and complicated designs with high number of users in Enterprise setting on the other hand because the relevant software tools are available and we can facilitate system management by designing an appropriate interface over Web. In more complicated modules, it is possible to change codes due to open text of Linux and Asterisk for better performance. As multi objective software which is designed based on information networks, proper design of network, Redundancy, QOS Traffic, management & planning and proper use of its software especially in Enterprise settings are inevitable. Thus, Asterisk is a good option for both simple applications such as phone center (IPBX) and complicated ones like video conferencing, Call/Contact center and integration with software such as

administrative automation, ERP, etc. and it must have all these prerequisites. Asterisk and mainly Soft Switch viewpoint and voice, telephone and image interchanges based on software tools over internet are not only consistent with the conventional ideas of telecommunications but also complementary to that. Although a structure like Asterisk is described based on popularity and expansion of computer network based communications (video conferencing, IP Telephony, VOIP), it has never forgotten compliance with conventional structures such as TDM. Although initiating Asterisk according to IP based devices is simpler and cheaper, compliance with traditional technologies has always been considered. The defenders of Soft Switch viewpoint and more traditional ideas have always discussed about two issues, security and reliability in Soft Switch and Asterisk systems compared to conventional systems.

By encoding the information, security of transferring voice information is guaranteed. In addition to conventional practices, we can create specific protocols to encode information. This is achieved by the capabilities of Linux operating system and in general, we can use either conventional encoding practices or specific protocols to provide security between the components of Asterisk based system.

In addition, Linux is an appropriate firewall per se which can guarantee high security in gaining access to Asterisk service providers. A lot of important features of Asterisk system have been derived from capabilities of Linux operating system. Capabilities like clustering and High Availability (HA) involve reliability of Asterisk based Soft Switch. Redundancy facilities such as feed resources besides redundancy facilities of computer networks in the format of links, devices or tools and protocols caused Asterisk to be aligned with TD Based systems. With such descriptions, Asterisk is a way to offer modern communications of next generation at varying scales. Innovation in offering a wide range of voice, image and data services made this software popular.

2.2. Communication Techniques of Asterisk with the Outside World

The first technique is using analogue lines and we can establish their connection with phone (call) center in two ways:

(1) Transducer cards of urban analogue lines (if we use real servers, we can use this technique but we cannot use it in virtual machines).

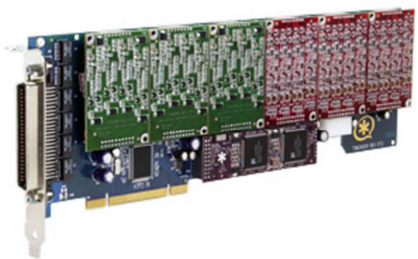

Fig. 3. *Analogue card FXO.*

(2) Analogue External Gateway (here we can use both real and virtual servers)

Fig. 4. *Analogue Gateway FXO.*

The second technique is using digital urban lines. This technique is suitable for large offices.

(1) Transducer cards of digital urban lines (if we use real servers, we can use this technique but we cannot use it in virtual machines)

Fig. 5. *Digital cards E^1, T^1, J^1.*

(2) Digital External Gateway (here we can use both real and virtual services)

Fig. 6. *Digital Gateway E^1, T^1, J^1.*

The third technique is using VOIP service providers. In this technique, we can establish a SIP trunk by traffic service providers and conduct the output on this trunk without any hardware.

The fourth technique is using communication lines of another server and the connection between them is established by trunk.

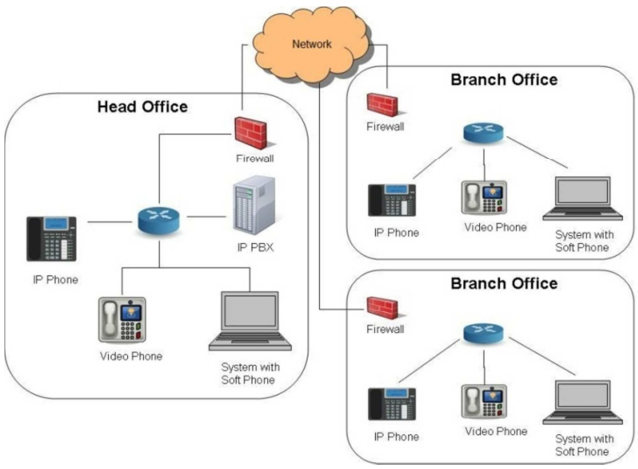

Fig. 7. *Outline of Asterisk phone system.*

With the ongoing development of telecommunications and phone systems, security in VOIP has become a matter of the greatest importance. Asterisk as one of the open text contact management software tools uses different methods and technologies to provide security. Two techniques, proactive and defensive, are used to provide security. In proactive technique, different kinds of encoding practices are used to prevent listening to SIP & RTP, while in defensive technique, Asterisk uses the other open text tools simultaneously, e. g. Fail Ban to identify and block suspicious traffics from unknown sources.

It is of great importance to use Asterisk and those security tools in an operating system.

(3) SIP: This protocol is usable as the most fundamental and common protocol to transmit voice on internet and the majority of VOIP service providers make use of it. Authentication and Authorization are performed through this to control access to VOIP services. One of the signaling protocols is SIP which is standardized by IETF Committee. SIP is a signaling protocol for establishing, altering and terminating sessions in the presence of one or more participants. SIP recalls used for establishing sessions contain some descriptions related to each session and allow participants to reach an agreement on a collection of media. SIP gets help from Proxy server to conduct requests towards current position of user, authorize and implement the call conduction policies. It also provides registration which allows users to transport their own current positions to internet by Proxy servers. The above protocol is able to be run on several transfer protocols.

In SIP, ports 5060 and 5061 are used for establishing communications and 10000 or 20000 RTP ports are used for transmitting voice.

The structure of the protocol consists of two logical units, namely user and server. The user unit is in fact an application which is divided into two parts, user-client and user-server. When a user is going to make a call, he/she uses his/her own user-client element and when somebody calls him/her, he/she uses user-server.

SIP servers consist of Proxy servers, registrar and path modification server. Proxy server receives requests from user element or other servers and then conducts signaling properly after processing message and connecting to the other server entities.

Registrar server is a server that receives registered message and is responsible for identifying user. In the case of approving registrar, user position is updated.

It is worth noting that these components are logical and therefore, we can implement them on a physical element.

SIP messages have two general forms: request and answer. There are six different kinds of requests: INVITE, ACK and CANCEL for initiating session and BYE for terminating it, REGISTER for recording the required information to establish communications and OPTIONS for receiving server applications.

User-server element produces and sends answer message after receiving and translating request. The answer is a sign of proceeding request.

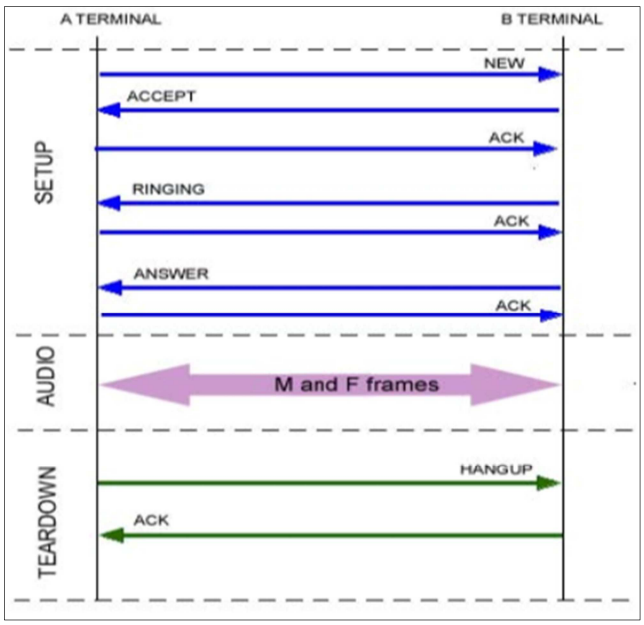

Fig. 8. *SIP communications.*

Security in SIP signaling protocol.

To secure SIP signaling, identification, integrity and privacy are required.

Identification is carried out in both server and user in order that two parties know each other identity. However, doing it by a server is inevitable and thereby server is also dealing with audit and phone calls.

The problem with identification in SIP protocol is not supplying integrity and privacy about calls and this becomes more problematic when the structure of the protocol and its ability are threatened.

In general, threats imposed on ISP protocol are divided into three groups: The first group involves threats from internet about which we discussed previously, e.g. sending fake messages. The second group includes threats from the nature of SIP. For example, a person interferes with call by sending BYE message on behalf of user and by sending REGISTER message he/she destroys users' privacy. The third group involves threats resulting from the complexity of the protocol. For example, hacker fills users' buffers with database commands or awkward messages.

The goal here is to study the security structure of Digest identification and security in TLS.

3. Results

3.1. Digest Identification

Identification in ISP is performed based on identification of HTTP protocol which is briefly called Digest identification. When a REGISTER request reaches server, answer 401 is sent without considering the request and it contains the header of identification. This result contains the method of identification,

Nonce and other parameters. According to SIP standard, Digest method is selected and Nonce is a random number and it is sent so that user can encode its own password. The user selects answer according to user name and password and other parameters like Nonce, Realm, URI and Method and puts it in the header of identifying INVITE request again. Server also does the same thing based on user name and shared password and compares between answers and if they were similar, user signaling would continue by server. As mentioned before, this mechanism may not guarantee the privacy and integrity. However, user password still remains private.

By TLS (Transport Layer security), sending SIP messages is done point by point. Such protocol lies on connective and reliable TCP in transport layer. TLS is consisted of four main phases. The first phase is for making TCP connection and in the second phase, two parties in a communication discuss about encoding and integrity algorithm. In the third phase, based on previous discussions, exchange between general key and identification of two parties is done. Next, each party will consider a basic password and in the fourth phase they will exchange SIP traffic in encoded form by it. After SIP signaling ended, connection continues and if necessary, it is used for continuing communication.

In TLS we can use two forms of encoding, symmetric and asymmetric. In symmetric encoding, two general switches are used by server and client and in this case, encoded content has low security because a common switch between server and client may be hacked by third party, so we use asymmetric form.

In asymmetric encoding, two switches A & B are used, if content is encoded with switch A, it will no longer be decoded. It will be decoded only with switch B corresponding to switch A.

3.2. Security in Voice Encoding in Sip

Now we activate TSL and our signaling will be secure but media is not encoded and RTP conversations are easily audible.

RTP is perhaps the most valuable component in VOIP conversation, so securing this is of great importance. Encoding RTP makes listening to conversation and recording it impossible. There are several ways to secure the content of voice.

All encoding algorithms act in a way that two parties in a conversation reach an agreement on encoding method and algorithm and use it during call. In other words, you cannot use an algorithm in one of two parties which is not accepted by another party. Furthermore, encoding algorithms are based on switch exchange and before starting a telephone conversation, the call should be exchanged between two parties. These switch exchanges are similar to that of passwords between two people except that this is done automatically.

In general, there are two well known methods for encoding multimedia currents and voice which are known as ZRTP and SRTP.

SRTP was developed in 2004 by a small group of IP experts in Cisco and Ericsson. SRTP defines a method for sending and receiving RTP answers and protecting, integrating and identifying message. This method is so designed that it can operate with applications Unicast and Multicast. Since this is an old method and is developed by key actors of IP industry. It is more popular and becomes a standard and is accessible on the world's systems.

ZRTP was developed in 2006 by Zimmermann Phil and it simplifies the process of making a secure call. It is also independent of server oriented encoding so that encoding can be done between servers that are unaware of the RTP content. It is expected that encoding is performed with a high speed since in this method independences are reduced. The success of such method depends on using ZRTP by manufacturer corporations in hardware tools.

In Asterisk, both methods are supported.

3.3. Security in Passwords

One of the most important issues is using hard and complicated passwords.

If you do not consider adequate complexity in choosing passwords and users, hackers may hack your system and steal your private information.

So the final recommendation is considering complexity in passwords.

4. Conclusion

Given the growing development of VOIP technology around the world, security is the most important issue that must be considered.

Asterisk telephone system is able to provide security by supporting the encoding practices of communication protocols, however it cannot support the encoding algorithms by itself and you are required to secure it by adding such facility and prevent threats from hackers.

According to experiments, Asterisk is very vulnerable without using encoding algorithms and everyone can hear people's voice. If this problem is solved after encoding information, you can comfortably use the telephone system. However security is a relative topic and never reaches by 100%.

It should be noted that security voids are not specific to Asterisk technology and they exist in most telephone systems over internet. Of course, we note that VOIP provides a lot of services for users which are not comparable to traditional telephone systems and the world welcomes this technology and its users are increasing rapidly.

On the other hand, hackers also may access to your private system. Your information need to be updated and you must use newest encoding methods to prevent hackers from accessing to your system. Finally, it is concluded that the growing development of technology in telephone systems has caused a lot of problems in security area and if we do not care about them, they may be very problematic.

References

[1] Penton, J., and A. Terzoli. "Asterisk: A converged tdm and packet-based communications system." Proceedings of SATNAC 2003-Next Generation Networks (2003).

[2] Schwarz, Brett. "Asterisk open-source PBX system." Linux Journal 2004. 118 (2004): 6.

[3] M. Spencer, M. Allison, C. Rhodes, The Asterisk Handbook, 2003, Asterisk Documentation Team, Available online at www.asterisk.org.

[4] QoS Routing in Networks with Inaccurate Information: Theory and Algorithms, Roch A. Guerin and Ariel Orda, in proceedings of INFOCOM, 1997.

[5] Improving QoS Routing Performance Under Inaccurate Link State Information, George Apostolopoulos, Roch Guerin, Sanjay Kamat, Satish K. Tripathi, in proceedings of ITC'16, June 1999.

[6] Quality of Service Based Routing: A Performance Perspective, George postolopoulous, Roch Guerin, Sanjay Kamat, Satish K. Tripathi, proceedings of ACM SIGCOMM 1998.

[7] R. Guérin, D. Williams, A. Orda, QoS Routing Mechanisms and OSPF Extensions, proceeding of GLOBECOMM 1997.

[8] G. Apostolopoulos, R. Guérin, S. Kamat, S. K. Tripathi, QoS Routing: A Performance Perspective, proceedings of ACM SIGCOMM. 1998.

[9] Shigang Chen, Klara Nahrstedt, An Overview of Quality-ofervice Routing for the Next Generation High-Speed Networks: Problems and Solutions, IEEE Network Magazine, Special Issue on Transmission and Distribution of Digital Video, Vol. 12, No. 6, November-December 1998, pp 64-79.

[10] Z. Wang, J. Crowcroft, Quality of Service Routing for Supporting Multimedia Applications, IEEE Journal Selected Areas in Communications, 1996.

[11] C. Huitema, Routing in the Internet, Prentice Hall Inc., New Jersey 1995 Mean delay / seconds X. Xiao, T. Telkamp, L, M. Ni," A Practical Approach for Providing QoS in the Internet Backbone", IEEE in Aug. 2001.

[12] B. Moore, E. Ellesson, J. Strassner,"Policy Framework for Multi-protocol Label Switching", Internet draft, draft-ietfmpls framework, txt, 1999.

[13] E. Rosen, A. Viswanathan, R. callon,"Multiprotocol Lable mpls framework. txt, 1999.

[14] D. O Awduche, A. Chiu, A. Elwalid, I. Widjaja, X. Xiao," A Framework for Internet Traffic Engineering", Internet draft, draft-ietf mpls framework-04. txt, work in progress, expires October 2001, June 2000.

[15] T. Kelly, "VoIP for Dummies", Wiley Publishing Inc, 2005.

[16] Johnston, Alan B, "SIP: understanding the Session Initiation Protocol", Artech House Publishers, 2001.

[17] J. Penton, A. Terzoli, CANS: Customizable Alarm Notification System, an H. 323 Signalling Service, South African Telecommunications Networks and Applications Conference, September 2002, Drakensburg.

[18] Z. Chen, S. Guo, K. Zheng, H. Li, "Research on Man-in• the-Middle Denial of Service Attack in SIP VoIP", Networks Security, Wireless Communications and Trusted Computing, 2012. NSWCTC'09.