J. Basic. Appl. Sci. Res., 1(12)3143-3148, 2011

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Security Key Generation Algorithm for User Identification in Voice over IP (VOIP) Networks

Sheeraz Arif, Rashid Hussain, Syed Wasif Ali Shah, Ahmed Sikander

Faculty of Engineering Science and Technology, Hamdard University, Karachi 74600, (PAKISTAN)

ABSTRACT

The introduction of new services and technologies in the internet have captured all the headlines in magazines, one of them is the voice over IP (VoIP). It is the voice transmission over data Network t in which the voice call can be made via internet, but internet is very unstable and unsecure network, the VoIP calls remain essentially unsecured, subject to security breaches. To secure any network there must be some methods or procedures to ensure the user authorization and encryption of data speech. In this paper a simple and easy secret key generation method of desired key length has been proposed against the traditional user authorization model. This can be helpful to reduce the security risk. This key generation method is very simple but very effective.

KEY WORDS: VoIP, Key Generation, Algorithm, XOR operators, encryption, decryption, cryptography, spoofing, identity theft.

1. INTRODUCTION

With the advancement of new technologies and the high speed network deployment, the VoIP is considered as a potential killer application for internet [5]. Most of the Telecom companies have moved there telephony communication to their data network. The VoIP solution offers a cheaper and clearer option in comparison to the conventional PSTN phone lines, because in PSTN each voice call uses a portion of dedicated 64Kbps unique connection but most of its part is consumed due to silent moment or lapses in speech [11]. VoIP deployment capitalize on the inefficiency of this design because the analogue signal is digitized, compressed, chunked into packets and sent over the data Network, so the less bandwidth is consumed. The larger a system, the higher are the security risks and lapses. VoIP is the part of internet so there are numerous threats to it, which include spoofing or identity theft, call redirection, traffic analysis, replay messages, tapping, data integrity and dictionary attack on the password file of a UNIX system. To prevent such attacks, encryption technique is the best way, but sometimes it becomes more complex and introduces the overhead and delays, because encryption of each packet sometimes consumes all of the allotted bandwidth. Due to these security threats and problems, we propose a secret key generation algorithm, which is very simple and effective and can be easily implemented to the present VoIP model. In the traditional VoIP models, the user must be authorized before making a call; users have to send the password to the server for user verification. There might be a possibility of a attack on the password file maintained by server. In this paper, a method has been given to generate a secret key, which will be helpful to encrypt our password and reduce the security threats. Different protocols for VoIP such as H.323 and SIP (session initiation protocol can also support this algorithm. The rest of the paper is organized as follows. Section 2 discusses the architecture of telephony over internet. Section 3 discusses the user authorization model in traditional VoIP network. Section 4 presents the secret key generation algorithm. Section 5 discusses the obtained results. Section 6 concludes the paper.

2. VOICE OVER INTERNET PROTOCOL

Voice over Internet Protocol (Voice over IP, VoIP) is a family of technologies, methodologies, communication protocols, and transmission techniques for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Even though IP Telephony and VoIP are terms that are used interchangeably, they are actually different; IP telephony has to do with digital telephony systems that use

***Corresponding Author:** Sheeraz Arif, Faculty of Engineering Science and Technology, Hamdard University, Karachi , 74600, (PAKISTAN). Email: sheeraz.arif@hamdard.edu.pk Ph.: +92-346-2896374

IP protocols for voice communication while VoIP is actually a subset of IP Telephony. VoIP is a technology used by IP telephony as a means of transporting phone calls [13].

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. The codec used is varied between different implementations of VoIP (and often a range of codecs are used); some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs.

There are three types of VoIP tools that are commonly used; IP Phones, Software VoIP and Mobile and Integrated VoIP. The IP Phones are the most institutionally established but still the least obvious of the VoIP tools. The use of software VoIP has increased during the global recession of 2008-2010, as many persons, looking for ways to cut costs have turned to these tools for free or inexpensive calling or video conferencing applications. Software VoIP can be further broken down into three classes or subcategories; Web Calling, Voice and Video Instant Messaging and Web Conferencing. Mobile and Integrated VoIP is just another example of the adaptability of VoIP. VoIP is available on many smart phones and internet devices so even the users of portable devices that are not phones can still make calls or send SMS text messages over 3G or Wi-Fi.

2.2 VoIP PROTOCOLS

Some of the VoIP protocols implemented in the market

- H.323
- IP Multimedia Subsystem (IMS)
- Media Gateway Control Protocol (MGCP)
- Session Initiation Protocol (SIP)
- Real-time Transport Protocol (RTP)
- Session Description Protocol (SDP)
- Inter-Asterisk eXchange (IAX)

H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.[1]

It is widely implemented by voice and videoconferencing equipment manufacturers, is used within various Internet real-time applications such as GnuGK and NetMeeting and is widely deployed worldwide by service providers and enterprises for both voice and video services over IP networks. It is a part of the ITU-T H.32x series of protocols, which also address multimedia communications over ISDN, the PSTN or SS7, and 3G mobile networks [12].

IP Multimedia Subsystem or **IP Multimedia Core Network Subsystem** (**IMS**) is an architectural framework for delivering Internet Protocol (IP) multimedia services. It was originally designed by the wireless standards body 3rd Generation Partnership Project (3GPP), as a part of the vision for evolving mobile networks beyond GSM. Its original formulation (3GPP Rel-5) represented an approach to delivering "Internet services" over GPRS. This vision was later updated by 3GPP, 3GPP2 and ETSI TISPAN by requiring support of networks other than GPRS, such as Wireless LAN, CDMA2000 and fixed line [12].

MGCP is a signaling and call control protocol used within Voice over IP (VoIP) systems that typically interoperate with the public switched telephone network (PSTN). As such it implements a PSTN-over-IP model with the power of the network residing in a call control center (soft switch, similar to the central office of the PSTN) and the endpoints being "low-intelligence" devices, mostly simply executing control commands. The protocol represents a decomposition of other VoIP models, such as H.323, in which the media gateways (e.g., H.323's gatekeeper) have higher levels of signaling intelligence [12].

The **SIP** protocol is an Application Layer protocol designed to be independent of the underlying Transport Layer; it can run on Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or Stream Control Transmission Protocol (SCTP). It is a text-based protocol, incorporating many elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP) [14].

The **Real-time Transport Protocol** (**RTP**) defines a standardized packet format for delivering audio and video over IP networks. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web-based push-to-talk features [12].

The **Session Description Protocol** (**SDP**) is a format for describing streaming media initialization parameters. The IETF published the original specification as an IETF Proposed Standard in April 1998 [15].

IAX is the **Inter-Asterisk eXchange** protocol native to Asterisk PBX and supported by a number of other soft switches and PBXs. It is used for enabling VoIP connections between servers beside client–server communication [12].

2.3 ARCHITECTURE OF INTERNET TELEPHONY

By using the VoIP service, we can send different kind of data such as voice, fax, images and other information over the dedicated circuit switched connection of the Public Switched Telephone Network (PSTN) [6]. Usually VoIP has two basic methods for internet access1-Dialup Access and 2-Direct Access, as shown in figure.1. In dialup access The ISP's network access device actually consists of a series of rack-mounted modems linked to communication servers. The server stand for one of several devices connected to the local LAN, with a router to the LAN, and router serial port offer the high speed communication connection from the ISP to an internet network service provider called NSP. Direct or Dedicated access is usually linked with the group of subscribers placed within a building or university campus. Under this access technique, subscribers are connected to a community LAN and the local area network is in turn linked via the use of a router and leased line to an ISP. As an alternative of the line come to an end at an ISP's communications server the leased line end at a multi-port router connected to a LAN every subscriber PC normally run a browser on top of a TCP /IP protocol.

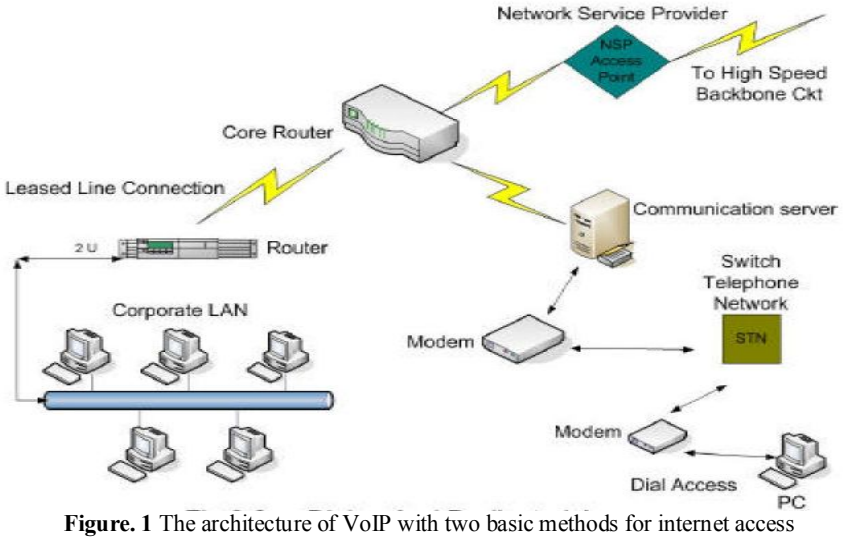

Figure. 1 The architecture of VoIP with two basic methods for internet access

3. AUTHORIZATION MODEL IN TRADITIONAL VoIP

In order to secure VoIP network, the identity of both user and device must be verified and after the user identification, the device can be easily be filtered by MAC address list. This authorized trust is between caller and host Network. The steps of authorization in traditional VoIP are as follows:

1- The user sends one or more requests to Network attached storage (NAS) for access the Network.
2- The NAS passes the message to the authentication server.
3- Server requests the credentials of the user and specifies the type of credentials required to confirm the user's identity.
4- The user sends its credentials (password) to the Server.
5- Upon validating the user's password, the authentication server transmits a success/failure message to NAS.
6- If success is granted, the NAS opens the port to all traffic.
7- Now the user is able to access the Network resources.

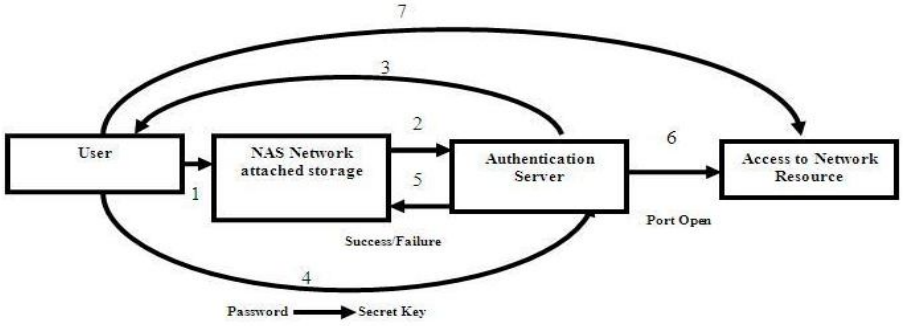

Figure 2 .The Authorization Model of VoIP

The above steps described the authentication procedure in simple VoIP networks. Usually in authentication process the password of the user has to be sent as credential but in our paper we have encrypted our password into secret key by using very simple method, so in this way we can put some security to protect our network from the malicious entities.

4. SECRET KEY GENERATION PROCEDURE

To ensure the security we must keep in our mind that only authenticated and trusted users can communicate in the Network. The communicating entities share a password and the secret key is generated dynamically from this password when needed so we can use a secret key shared between a couple of communicating entities in order to get security service. The secret key can be generated from password dynamically and when server requests the credentials of user this secret key can be passed instead of password for user identity as shown in figure 2.this can be very helpful to enhance our security. We can generate secret keys from password by using numerous different techniques.

Suppose the required length of the secret key is n bytes. The key generating mechanism is as follows:

1- If password length = *n* bytes, key = password.
2- If password length < *n* bytes, key = password padded with zeros.
3- If password length > *n* bytes, key = initially assign first n bytes of password to key, then $(n+M)^{th}$ bytes of the password is XoRed with the $(M \bmod (n))^{th}$ byte of the key (for all password bytes beyond *n*).

To understand the procedure let's consider the case where the password is **abcdEF56** and get the secret key for three cases when the preferred key length is 24 bits, 128 bits, 160 bits, Because the H.323 standard uses the Universal Character Set (UCS), or in other words the ISO /IEC 10646 standard.

In this case we'll consider the 16 bit representation of the character in the password called Unicode 16 bit representation.

a= 00000000 01100001; b= 00000000 01100010; c= 00000000 01100011;
d= 00000000 01100100; E= 00000000 01000101; F= 00000000 01000110;
5= 00000000 00110101; 6= 00000000 00110110

At this point it is seen that the password length is 128 bits. The three cases are as follows

CASE A

When the desired key length is 24 bits, the size of the password exceeds the desire key size, hence

	00000000 01100001 00000000
XOR	01100010 00000000 01100011
XOR	00000000 01100100 00000000
XOR	01000101 00000000 01000110
XOR	00000000 00110101 00000000
XOR	00110110

Equals 00010001 00110000 00100101, which is the 24 bits our required key.

CASE B

When the desire key length is 128 bits:

01100001 00000000 01100010 00000000 01100011 00000000
01100100 00000000 01000101 00000000 01000110 00000000
00110101 00000000 00110110.

The size of the password equals the desired key size; hence the key is identical to the Password.

CASE C

When the desired key length is 160 bits, the size of the password is less than the desired key size. Hence the key is merely the password appended with the appropriate number of zeroes, resulting in:

00000000 01100001 00000000 01100010 00000000 01100011
00000000 01100100 00000000 01000101 00000000 01000110
00000000 00110101 00000000 00110110 00000000 00000000
00000000

By using the above mentioned cases we can generate the secret keys of any desired length (32, 56, 64 and 256 bits) in quick time, because there is no any complexity involved in generation of key.

5. RESULTS AND DISCUSSION

When we talk about security of voice over IP the key stages of VoIP security are encryption delay, message delay, and processing power. We can use a secret key shared between a couple of communicating entities in order to get security services for example user authentication and message authentication or Integrity prevention. Because secret key-based mechanisms are quicker than public key-based Mechanisms, they are frequently ideal when message authentication or integrity is Preferred because in this case every message might require to be authenticated or integrity Checked. For this purpose Public key based mechanisms might be too slow and or computationally intensive. The following table shows the statistics with the different key size.

Table 1 Combinations and time involved for various key spaces

Key Size (bits)	Number of alternative Combination	Time required 1 decryption/µs	Number of XoR operators
24	$2^{24} = 16.7 \times 10^{6}$	$2^{23} \times 10^{-6} = 8.3$ seconds	5
32	$2^{32} = 4.2 \times 10^{9}$	$2^{31} \times 10^{-6} = 35.8$ minutes	3
64	$2^{64} = 1.8 \times 10^{19}$	$2^{63} \times 10^{-6} = 292.4$ years	1
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \times 10^{-6} = 5.3 \times 10^{24}$ years	Nil
160	$2^{160} = 1.4 \times 1.4^{48}$	$2^{159} \times 10^{-6} = 2.3 \times 10^{34}$ years	Nil
192	$2^{192} = 6.2 \times 10^{57}$	$2^{191} \times 10^{-6} = 10 \times 10^{43}$ years	Nil

We can analyze from the table that secret key size less than 32 bits can be broken within very short span of time and key can be revealed with less effort by Bruce force attack.128 bits key is the desirable security key size, because its generation is too easy and less complex and does not require any mathematical operator such as XoR and large processing power is required to get the key.192 bits key is not desirable for real-time call processing because it can offer some encryption delay which is not suitable for any real time call processing.

5. CONCLUSION

The secure authentication allows us to safeguard our Network assets, prevents malicious device from accessing our Network, and enable touch free management of endpoints device. In this paper we have proposed a method of securing VoIP communication, the secret key of our desired length has been generated which is very stable and easy to generate in quick time and there is no complexity involve in its generation. In VoIP there is real time call processing, we can not afford any encryption delay so our proposed key generation method is the ideal one. Keys can be generated and managed inside the secure boundary of the system, so this approach also reduced the complicated sequence of the operation to generate crypto keys as in the traditional system. It can generate more complex key but not in complex manner within minimum amount of time, which aptly suited for any real time cryptography.

REFERENCES

[1]. B.Goode,"Voice over Internet Protocol (VoIP)" proceeding of the IEEE,Vol 90 (2002)

[2]. "Breaking through IP telephony"<http://www.nwfusion.com/reviews/2004/0524voipsecurity.html>

[3]. Shin-Ho Liu,Han-yen YU "A secured Video Streaming" International conference on system science and Engineering 2010.

[4]. T.Subashri "Confidentiality of VoIP using efficient ECDH key exchange Mechanism" Proceedings of the 8th WSEAS International Conference on APPLIED ELECTROMAGNETICS, WIRELESS and OPTICAL COMMUNICATIONS.

[5]. P.Arul "Generate a key for AES using biometric for VoIP Network security,outline of theoritical andapplied information technology 2005-2009.

[6]. P. Mehta and S. Udani, "Overview of Voice over IP". Technical Report MS -CIS-01-31, Department of computer Information Science, University of Pennsylvania, February 2001.

[7]. http://www.cisco.com/warp/public/126/saa.html" R. Sinden", "Comparison of Voice over IP with circuit

switching techniques".Department of electronics and Computer Science

[8]. J. SaiGeetha et. al. / International Journal of Engineering Science and Technology Vol. 2(8), 2010, 3551-3556

[9].Shawn McGann and Douglas C.Sicker "An analysis of security Threats and Tools in SIP-Based VoIP system,University of Colorado.

[10]. Dennis Estacson "potential security problem looms for users of PC-based VoIP products",Queen University,Kingston,ON.

[11]**. "**Multimedia Communication and system (Application, Protocol,Networks,Standards)",By Fred Halsall

[12]. http://en.wikipedia.org/wiki/Voice_over_Internet_Protocol

[13]. www.networkstraining.com , IP Telephony vs VoIP

[14]. Johnston, Alan B. (2004). *SIP: Understanding the Session Initiation Protocol, Second Edition*. Artech House. ISBN 1580531687.

[15] Handley, Mark; Van Jacobson (1998-04). "SDP: Session Description Protocol (RFC 2327)". IETF Retrieved 2008-04-19

From web documents:

Retrieved from http://www.cisco.com/warp/public/126/saa.html" R. Sinden", "Comparison of Voice over IP with circuit switching techniques".Department of electronics and Computer Science on 09 August 2011

Retrieved from http://en.wikipedia.org/wiki/Voice_over_Internet_Protocol on 21 August 2011

Retrieve from www.networkstraining.com , IP Telephony vs VoIP

Retrieved from "Voice over Internet Protocol. Definition and Overview". International Engineering Consortium. 2007 on 2009-04-27.