Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.424 – 431

RESEARCH ARTICLE

A Proposed Security Framework for VoIP

Mandeep Singh[1], Neetu Sharma[2]

[1]Research Scholar, Department of Computer Science and Engineering, Ganga Institute of Technology & Management, Kablana

Email ID: mandeep.may91@gmail.com

[2]HOD, Department of Computer Science and Engineering, Ganga Institute of Technology & Management, Kablana

Email ID: neetush75@gmail.com

Abstract: VoIP stands for Voice over Internet Protocol and is a way to carry voice traffic over computer networks like the Internet. Over the last decade VoIP has become increasingly popular, gaining millions of subscribers every year (e.g. LINE and WECHAT provide voicecall facilities) and has certainly caught the eye of telecommunication service providers all over the world. The driving factor for the success of VoIP is cost reduction, both for users and providers. But VoIP doesn't only bring reduced costs it also brings threats and vulnerabilities since it is IP based it's susceptible to large number of threats. The threats include spoofing or identity theft and call redirection, making data integrity a major risk. Therefore authentication and encryption techniques can be used to design a framework which can survive the possible threats. In this security framework authentication is implemented first to authenticate the true user and then cryptography techniques is used to safely transmit the information stream over the network. The authentication part will be implemented using biometrics because it is not possible to theft anyone's physical features.

Keywords: VoIP, SIP, RTP, PSTN, DoS

1. INTRODUCTION

Voice over Internet Protocol (VoIP) is a protocol optimized for the transmission of voice through the Internet or other packet switched networks. VoIP is often used abstractly to refer to the actual transmission of voice. VoIP is also known as IP Telephony, Internet telephony, Broadband telephony, Broadband Phone and Voice over Broadband. Voice over Internet Protocol (VoIP) is one of the rising voice communication technologies over packet-switched networks, such as the Internet and other IP networks. It uses the internet technologies and web linked environment in a highly efficient way to offer much more versatile services with reduced or no costs. Additionally combined with the embedded technology, Voice over IP allows a wide range of hand-held devices to have their real-time access to voice communication on the Internet, making a new era to the future internet technologies. Wireless LAN systems providing broadband wireless access in hand held devices have become more popular in recent years. There has been growing interest on Internet telephony, mainly on hand held devices running applications such as web browsing and email. Internet telephony allows the Users to make voice and video calls over the internet. The main advantage of IP telephony over a wireless network is that it allows mobility of the people while they are talking.

We may consider a VoIP call as a three−phase process:

Establishment

Conversation

Termination

The first and the third phases typically make use of a signalling protocol, such as the Session Initiation Protocol (SIP), while the second utilizes the Real−Time Protocol (RTP) to transport the media data. Therefore, this project handles the signalling protocol security and the data transport protocol security independently. The main goal of this document is the description of a suitable solution to achieve this security without effecting the performance of the model.

Mobility aspects of the model are not explicitly considered in this project, although this paper may be one of the bases for future work in this area, since the proposed solution is based on the use of mobile devices operating in wireless environments.

Regarding practical work and tests of the model, this project in mainly focused on the security for the media stream (by using the Secure Real−Time Protocol, SRTP). However, thorough theoretical work has also been performed, which includes other aspects as said above, such as the establishment and termination of the call (using the Session Initiation Protocol, SIP) and the key−management protocol to be used.

Security Attacks

A security attack is defined as an assault on system security that derives from an intelligent threat (which might exploit a vulnerability), and compromises the security of information owned by an organization. Security Attacks are divided into two main groups: Passive Attacks and Active Attacks.

Passive Attacks: Those whose goal is to obtain information that is being transmitted. Passive Attacks are divided into two main groups:

- Release of message contents: Interception of the content (possibly sensitive) of a message.
- Traffic Analysis: Interception for observing the patterns of the messages to guess the nature of a communication.

Active Attacks: Those which involve some modification or alteration of the data stream, or the creation of a false stream. Active Attacks are in turn divided into four groups:

- Masquerade: It implies one entity pretending to be a different entity.
- Replay Attack: It consists of the capture of sensitive data, and its subsequent retransmission to produce an unauthorized effect.
- Modification of messages: It implies the alteration, deletion, delay, or reordering of some portion of a message, producing an unauthorized effect.
- Denial of Service (DoS) Attack: DoS attack prevents or inhibits the normal use or management of communication facilities by disabling or overloading them.

Passive Attacks are difficult to detect, since they do not imply alteration of the data. Thus, the solution is the prevention of these attacks, and the mechanism used is encryption.

On the other hand, Active Attacks are difficult to prevent, since that would imply the physical protection of resources and paths. Therefore, the solution is to detect and recover from these attacks.

Processes Involved

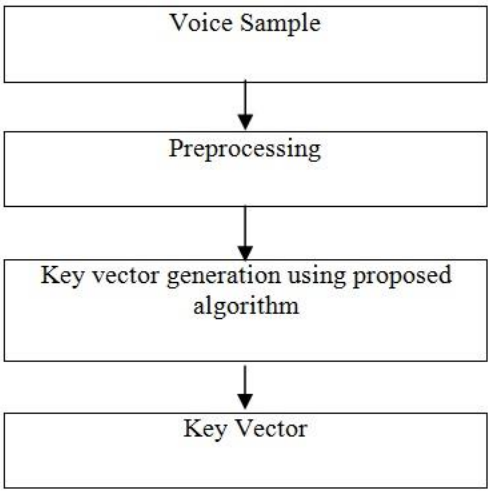
Authentication Process: This section describes the authentication process by means of the establishment of a call. The mentioned process outlines the situation where the goals of the implementation are already met. Systems that communicate try to initiate a call on the request of one of the EPs that are registered to it. The communication between the two devices is part of the call signaling to establish a call.

Biometric Cryptosystem: Cryptography provides the secure manner of information transmission over the insecure channel. It authenticates messages based on the key but not on the user. It requires a lengthy key to encrypt and decrypt the sending and receiving the messages, respectively . But these keys can be guessed or cracked. Moreover, Maintaining and sharing lengthy, random keys in enciphering and deciphering process is the critical problem in the cryptography system. The above mentioned problem is solved by a Biometric cryptosystems. Biometric cryptosystems combine cryptography and biometrics to benefit from the strengths of both fields. In such systems, while cryptography provides high and adjustable security levels,

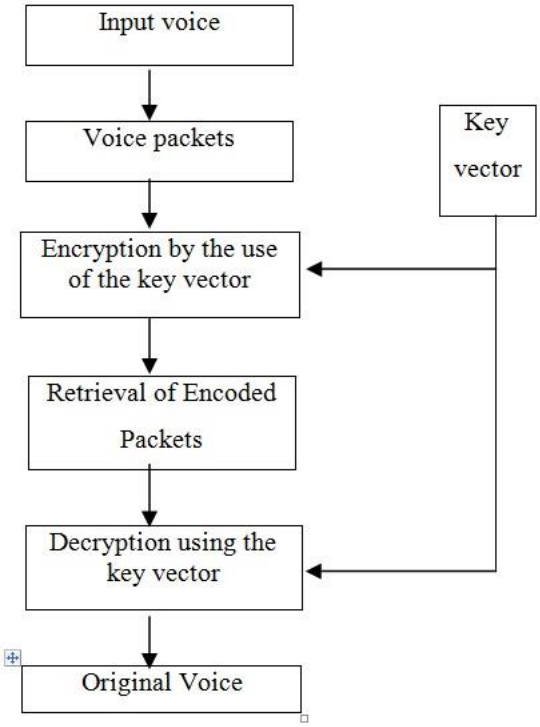
biometrics brings in non-repudiation and eliminates the need to remember passwords or to carry tokens etc. In biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication.

2. MODEL USED

Cryptography provides high and adjustable security levels, biometrics brings in non-repudiation and eliminates the need to remember passwords or to carry tokens etc. In biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication.



Key generation using voice samples



Encryption and Decryption using the key

2.1 Tool Used: MATLAB

MATLAB (Matrix Laboratory), a product of Mathworks, is a scientific software package designed to provide integrated numeric computation and graphics visualization in high-level programming language. MATLAB program consists of standard and specialized toolboxes allowing users to take advantage of the matrix algorithm based on LINPACK1 and EISPACK2 projects. MATLAB offers interactive features allowing the users great flexibility in the manipulation of data and in the form of matrix arrays for computation and visualization. MATLAB inputs can be entered at the "command line" or from "mfiles", which contains a programming-like set of instructions to be executed by MATLAB. In the aspect of programming, MATLAB works differently from FORTRAN, C, or Basic, e.g. no dimensioning required for matrix arrays and no object code file generated. MATLAB offers some standard toolboxes and many optional toolboxes (at extra cost), such as financial toolbox and statistics toolbox. Users may create their own toolboxes consisted of "mfiles" written for specific applications. The original version of MATLAB was written in FORTRAN but later was rewritten in C. MATLAB consists of a collection of toolboxes. These toolboxes contain library files called M-Files, which are also functions or command names, executable from the Command window.

3. Review of Literature

In Year 2003, Israel M. Abad Caballero presented a solution to secure every link of the Mobile VoIP , from the establishment to the termination, giving the model, the necessary security services and minimizing the effect of this security services and their mechanisms on the performance. His work was focussed on the security of the media stream. However, a thorough investigation work had also been performed concerning the SIP security and the key management.

In Year 2007, Pawel Lawecki investigated Security of Voice over IP in public networks problem. In order to perform a security analysis many background and initial research had to be carried out. VoIP general properties were studied, including VoIP's role in Next Generation Networks and comparison with the traditional PSTN services. Different issues like cost, switching, quality or mobility were analyzed. Structure of public IP network was also examined. Consequences of open and combined architecture on VoIP were studied in detail. Differences between access and service provider and their impact on security of public network were also investigated. Impact of access network properties, like mobility or shared medium (shared local access network) was studied on three examples of access scenarios - DSL, Cable and WiMAX. Internal architecture of service provider network was also analyzed in general and on example of SIP protocol architecture.

In Year 2008, Johann Thalhammer yielded the result that all interfaces require the security services authentication and data integrity. The interface between a GK and the BES additionally demands privacy because of the sensitivity

of the transmitted data. The result for the proposals of the security framework must be seen for each interface or connection separately. The RAS protocol between EP-GK was already equipped with authentication and data integrity. If the use of pregranted ARQ is inhibited, this method already provides a certain level of security.

In Year 2009, P.Arul had proposed a method of securing VoIP communication using encryption and a novel approach for fingerprint based cryptography system. The crypto keys had been generated using fingerprint patterns, which is stable through out person's lifetime. This approach has reduced the complicated sequence of the operation to generate crypto keys as in the traditional cryptography system. It can generate more complex keys with minimum amount of time complexity, which is aptly suited for any real time cryptography.

In Year 2010, Christian Schridde proposed the development of the Secure Session Framework. It consists of two main parts: first, a key agreement scheme with extensions to multiple independent key generators, and second, a corresponding multi-signature scheme. The key agreement is based on well known assumptions and is efficient in the terms of communication and computational cost. It fulfills all necessary requirements for a secure and authenticated key agreement protocol. The Φ-Hiding assumption was addressed and it was shown that this assumption can be broken with an average advantage probability of 1/4 if the setup was chosen in a certain way.

In Year 2011, Alireza Heravi evaluated the users' awareness and attitudes towards privacy and security issues in VoIP communications. For this reason, an on-line questionnaire was designed to collect information, and to analyze the collected data quantitative-statistical techniques were employed. The findings of this study revealed that the majority of participants are neither concerned about VoIP privacy (eavesdropping) or VoIP security. They also do not expect to have the best facilities and privacy features when using VoIP since VoIP providers generally offer low-cost services. Also, the findings indicate that participants are most concerned about lower cost and least concerned about security when making international calls. However, most respondents who make international calls (either using VoIP or traditional telephony, and either by phone or via computer) are at some level concerned about privacy (eavesdropping). The same trend applies to domestic and interstate calls as well.

In Year 2011, Philip J. Starcovic had analyzed existing VOIP applications as a secure technology that has the ability to create true end-to-end security. After testing four VOIP UAs, it was apparent that while communications in transit were secure, how the UA handles data at rest needs to be reevaluated. With the above future areas of research and recommendations, VOIP will create confidentiality and integrity for secure communications throughout the DoD and the world.

In Year 2011, Knutur Birgir Otterstedt analyzed that if Voice over IP is to be a successor to PSTN much work must be done to enhance its security. PSTN has been in place for over a century so clients are used to a certain level of security and reliability. These users expect the same security performance of VoIP. VoIP is susceptible to a larger number of threats than PSTN and these threats are usually more severe for VoIP. All hope is not lost since there are indeed measures that can be taken in order to increase security for both VoIP users and providers. This is however

far from a perfect solution to the problem. Most of these measures require a combination of time, money and IT knowledge to be successfully implemented.

In Year 2012, Karunakar Antham, Chandrashekar Reddy Palle, Ashwin kumar Mantoor proposed that Users with Wi-Fi equipped devices can communicate each other without using access point. This could be useful in the situations where there is no availability of an Access point or network operator such as battle field, disaster situations, undergrounds and communication between cyclists .Voice Communication between the devices will be done after group formation. We studied different approaches to form a group formation between the Wi-Fi devices and established peer to peer voice call without using Internet or network operator. We have presented necessary steps for successfully establish an ad-hoc network of android mobile devices. Finally, we have implemented an application to adopt VoIP to decentralized networks. These factors suggest that battery driven devices will soon become walkie-talkies, allowing users to make free calls.

4. Major Objectives

- The main objective is to design a security framework for secure communication with efficient authentication techniques.
- The objective of work is to develop an environment for confidential transfer of information using internet protocol.
- The objective of work is to minimize the threat in the communication.
- The objective of work is to maintain the secrecy of the information.

5. Conclusion

This paper defines the capability to design a secure framework for communication using VoIP. The work uses biometrics for the authentication of the clients on both sides of the channel. This work uses efficient encryption and decryption techniques for maintaining the confidentiality of the information or data to be transmitted over the channel. The biometrics not only authenticates the clients but also creates a key for using in the encryption of the information.

References

[1]. B. Goode, "Voice Over Internet Protocol (VOIP)". Proceedings of the IEEE, VOL .a. 90, NO. 9, Sept. 2002.

[2]. "Breaking Through IP Telephony "http://www.nwfusion.com/reviews/2004/0524 voipsecurity.html

[3]. J. Ryan. Voice over IP (VoIP). The Applied Technologies Group white paper. 1998.

[4]. R. Barbieri, D. Bruschi, and E Rosti, "Voice over IPsec: Analysis and Solutions". *18th Annual Computer Security Applications Conference (ACSAC)*, 2002.

[5]. B. Goode, "Voice Over Internet Protocol (VoIP)". *Proceedings of the IEEE*, Vol. 90 No. 9, Sept. 2002.

[6]. Baset, S. A., & Schulzrinne, H. (2004, September 15). An Analysis of the Skype Peer-to

[7]. Peer Internet Telephony Protocol. Retrieved from http://arxiv.org/ftp/cs/papers/0412/0412017.pdf

[8]. Chou, W. (2007). VoIP Network Security. *IT Professional magazine*, Vol. 9, Issue 5, pp. 42-46, Sept.- Oct. 2007.

[9]. Higdon, J. (2008). The Top 5 VoIP SecurityThreats of 2008. From VoIP-News website:http://www.voipnews.com/feature/top-security-threats-2008-012408/.

[10]. VOIPSA, Inc.; A portal of VoIP Security Alliance - organization carrying out many VoIP security related projects; *http://www.voipsa.com*, 2006

[11]. Anonymous. (n.d.). *Voice Over IP Information*. Retrieved May 10, 2011, from VoIP Laws and Legal Issues: http://www.voiceoveripinfo.com/voip-laws-legal-issues.php

