Enhancement Of AES Algorithm For IAX Protocol

OMAR ABDUL MOUTI MOLKI

A project report submitted in partly fulfillment of the
requirements for the award of the degree of
Master of (Computer Science)

Faculty of Computer Science & Information Systems
Universiti Teknologi Malaysia

APRIL 2009

ABSTRACT

Voice over IP (VoIP) is transforming the telecommunication industry. It offers multiple opportunities such as lower call fees, convergence of voice and data networks, simplification of deployment, and greater integration with multiple applications that offer enhanced multimedia functionality. However, notwithstanding all these technological and economic opportunities, VoIP also brings up new challenges. Among them, security is perhaps the most compelling. Security for Voice over IP (VoIP) can be achieved in different ways. In this project new encryption algorithm has been proposed and implemented on IAX protocol with focusing on the performance for the secure media session. But VoIP has a very special characteristic: it is “time critical”. Time has a tremendous impact on this technology’s ability to performance, and to transmit meaningful information as well. Consequently, security considerations for VoIP must take additional steps to fulfill specific quality demands. First, the technology requires a very low latency less than 150ms. Second, packet loss cannot exceed the mark of 3%. Third, the technology is highly sensitive to “unquantifiable disrupting factors such as jitter”. All these factors converge and constitute the most critical of all VoIP security vulnerabilities to ensure the secure stream of VoIP service and provide satisfactory performance.

ABSTRAK

Suara Latar IP (VoIP) adalah berubah industri telekomunikasi. Ia menawarkan peluang-peluang berbilang seperti panggilan lebih rendah yuran, penumpuan rangkaian-rangkaian suara dan data, pemudahan penggunaan. dan integrasi lebih besar dengan pelbagai aplikasi tawaran itu meningkatkan multimedia kefungsian. Bagaimanapun, walaupun semua ini teknologi dan peluang-peluang ekonomi, VoIP juga membesarkan cabaran baru. Antaranya, keselamatan boleh jadi yang terbanyak menambat perhatian. Keselamatan Untuk Suara Latar IP (VoIP) boleh dicapai dalam cara-cara berbeza. Dalam projek ini algoritma penyulitan baru telah dicadangkan dan melaksanakan pada protokol IAX dengan menumpukan atas prestasi untuk sesi media yang selamat. Tetapi VoIP mempunyai satu ciri khas sebenar: ia “masa kritikal". Masa mempunyai satu kesan dahsyat pada keupayaan teknologi kepada prestasi, dan untuk menghantar maklumat yang bermakna juga. Akibatnya, pertimbangan keselamatan untuk VoIP mesti mengambil langkah-langkah yang tambahan untuk memenuhi sifat khas tuntutan-tuntutan. Pertama, memerlukan teknologi kependaman rendah sebenar kurang daripada 150ms. Kedua, kehilangan bingkisan tidak boleh melebihi tanda 3%. Ketiga, teknologi adalah amat sensitif untuk “unquantifiable menggendalakan faktor seperti ketar". Semua faktor-faktor ini bertumpu dan membentuk paling gawat semua keselamatan VoIP kelemahan-kelemahan bagi memastikan sungai selamat bagi perkhidmatan VoIP dan menyediakan prestasi yang memuaskan.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.0 Introduction

Voice over Internet Protocol (VoIP) is the most popular in telecommunication technology. Nowadays, three million users use VoIP. It is estimated that the number will increase to twenty-seven million by the end of 2009 (Richardson, 2005). Furthermore, big companies and small enterprises are trying to reduce costs and improve productivity in all areas of the business. That means VoIP continues to grow in popularity and remains a promising telecommunication technology that will gradually replace traditional PSTN phone systems.

As it knows in this millennium, VoIP technology continues to touch upon every aspect of our life including the way we interact. Traditional conferences are not to be left out of the digital revolution. With the technology tools, it seems very feasible that a new “electronic conference” model can emerge, allowing us to be there wherever the conference event may be. Recently, after the VoIP has been invented, then the next challenge for the researchers is the security of voice service.

Moreover, the sensitivity of information that frequents in such a system is very critical. Therefore, the security is an essential to the VoIP.

Starting from encrypt sender the voice, then sending that encrypted voice through the network, terminating by decryption back the packet at the receiver side, many algorithms and techniques were occurred in that long path. On the other hand, we need to improve certain techniques for encrypt the voice, in the same time to enhance the AES encryption algorithm.

This proposal will compare the most popular VoIP protocols to choose the suitable protocol and apply the propose algorithm, aiming to improve the security of voice to reduce the hacker and snoop during transmitting the data through the network used.

1.1 Problem Background

The telecommunications industry spans over 100 years, and Asterisk server the most famous VoIP's server has integrates most of the major technologies that it has made use of over the last century. To make the most out of Asterisk, you need not be a professional in all areas, but understanding the differences between the various protocols will give you a greater appreciation and understanding of the system as a whole (Frank, 2006). They are so many numbers of protocols for VoIP. Some of them popular and standard, while the other still under development. Each one of those protocols has different properties and its own specification. So we should understand each of them and the differences between them to know which one we should choose or which part we should develop.

The key to the success of any VoIP session is to provide similar features that are derived from real-time conferencing environments; the most basic one of which

is live audio broadcast. The following goals are required to achieve more secure algorithms:

1. Apply all the security rules such as key exchange, and encryption.
2. A fast and efficient system to be applicable to large groups or clients with access to only a small amount of computing power.
3. To provide real-time communication among conference members with high level of security
4. To design a general system to be applicable in different environments such as in companies or universities

Encryption Methods exist to provide a secured data transported on IP networks, these methods can be employed for voice services. However, early security methods were designed for securing data transport and not so much with real-time communication in mind. Therefore, many current security methods are appropriate for small scale communication systems but for large scale systems they might incur a considerable overhead, which could make them unusable. With the adoption of VoIP for large scale systems, a need has emerged for new security mechanisms which are specifically designed for real-time applications.

Voice of Internet Protocol is the next generation telecommunications method. It allows phone calls to be routed over a data network thus saving money and offering increased features and productivity. All these benefits come at a price, vulnerability. It is easier to attack and exploit a voice and data network. VoIP will need extra security measures beyond the standard security that is typically implemented for a computer network. Many issues need to be addressed such as type of attacks, security, quality of service and VoIP protocols.

1.2 Problem Statement

There are many VoIP protocols in the market. Some are proprietary while others are open standards. The three most popular open protocols are H.323, SIP and IAX. They were designed by many different organizations and operate slightly differently. All of them have problems with the use of random ports problems with NAT translations and firewalls.

Encryption helps protect your privacy and authenticates the message. Transport Layer Security and IPsec are the two main encryption methods. IP security is used to encrypt call setup and control messages. TLS is an alternative to IPsec and is based off the SSL protocol. It is used is used to provided a secure call setup. Many different algorithms can be used such as DES, 3DES, AES, RC4, and RC5 (Roberts, 2005). The simpler encryption results in better performance (NIST, 2005). It is an effective measure against eavesdropping and protects sensitive information.

1.3 Project Objectives

This research aims to study the methodology that can be used to test the security of voice by different tools to determine which algorithm is better to be used, this algorithm will be much better, much easier, and high performance of quality. All those are based on studying the results from previous published works. Beside that the researcher will rearrange some of the previous work and also might combine different previous works to get his own methodology.

The main objectives of this project are stated in the following points:

1. To investigate and compare VoIP protocols through the security point of view.
2. To propose security algorithm based on enhance AES algorithm to secure VoIP encryption, and
3. To test the delay time of the proposed algorithm among the original algorithm within acceptable time frame.

1.4 Project Scope

The objectives of this study were stated in the previous section. In order to achieve the study objectives, it is important to highlight the study area and its boundaries, which are stated in the following points:

1. The propose algorithm will be applied on a chosen protocol after comparison done.
2. IAX platform using Microsoft Express C# will used to simulate the parameters of voice encryption.
3. Virtual VoIP IP PBX software will used as a server to manage the IAX call.

1.5 Project Justification

The primary measurement of success of VoIP security is to perform high security algorithm of voice measured from users' satisfaction. Any project has its own problems, from this point determining the project success or fail comes from how this project can manage and control the problems.

Always solving the problems from the beginning is much easier and performs high quality than solving them later. On the other hand, concentrating on the first phase of VoIP lifecycle give us high prediction that the packets will transmit softly with a bit guarantee. Therefore, the data in the first phase during preparing to send it still under control, but after injection the data to the network, it will be out of control, therefore better we prepare it as well as secure. It is like sending e-mail when first the letter should be written from the sender by choosing his own font and color, with VoIP same but the main difference is the voice should be processed in real time.

There are more than ten VoIP protocols, the project tends to select most three common protocols which are more familiar with VoIP, the reason from selecting those techniques are either because the adapted with VoIP protocols or they perform well in arrival time. Most of other protocols are used with special network service, local connection, mobile GSM.

RERENCES

Alias, M. & Ong, L. L. *Performance of Voice over IP (VoIP) over a wireless LAN (WLAN)*. Malaysia: Universiti Teknologi Malaysia, 2006

Anonymous, "Voice *over IP via Virtual Private Networks: An Overview*". AVAYA Communication, 2003

A.Fahmy, M. Shaarawy, K. El-Hadad, G. Salama and K. Hassanain, "A Proposal For A Key-Dependent AES" SETIT 2005, TUNISIA

Bruce Schneier, "*Why VoIP needs crypt*o", 2006.

B. Goode, "*Voice over Internet Protocol (VOIP)*", Proceedings of the IEEE, VOL. 90, NO. 9, 2002.

Cisco, "*Understanding H.323 Gatekeeper*", 2006.

Daemon, J. and Rijmen, V. "The Rijndael Block Cipher: AES Proposal", NIST, Version 2, March 1999

Daemon, J., and Rijmen, V. "The Design of Rijndael: The Wide Trail Strategy Explained." New York, Springer – Verlag, 2000

Daemon, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, 26, 3, March 2001, 137-139.

Daniel-Constantin Mierla, *http://www.isoc.nl/activ/2005-ENUMSIP/2-Mierla-SipTutorial.pdf#search=%22SIP%20tutorial%22, 2005*

Deepak Kumar Dalai, "*On Some Necessary Conditions of Boolean Functions to Resist Algebraic Attacks*", Ph.D Thesis, Applied Statistics Unit, Indian Statistical Institute, Kolkata, India, August, 2006.

Frank W. Miller," *IAX Protocol Description* ", 2006

International Engineering Consortium, "*H.323 tutorial*" 2004

Ixia, *Assessing VoIP Call Quality Using the E-model*. CA 91302. Calabasas: West Agoura Road, 2005

John McCaron, "*A Brief Overview of VoIP Security*".

J. Larson, T. Dawson, M. Evans & J.C. Straley, "*Defending VoIP Networks from DDoS Attacks*", 2004

Jim Dempsey, "*Voice-over-IP: The Future of Communications*", 2003

Joseph Harden, Patrick Fenton, Martin Hehir, Eoin Duggan, "*VoIP and Wireless Networking"*. 2006

Jablon, "*Strong Password-Only Authenticated **Key Exchange***", 1997,

http://www.integritysciences.com/speke97.html

Nadeem Unuth, "*Security Threats In VoIP*". 2005

National Institute of Standards and Technology. "*Security Considerations for Voice over IP Systems ", 2005*

Oliver, C. I, *Converged Network Architectures, Delivering Voice and Data over IP, ATM, and Frame Relay*.1st edition, 2002

Richardson. T, "*US to embrace VoIP*", 2005.

Robert Ensor, "*VoIP: What is it good for?* ", 2005

R.C.W. Phan, "*Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES)*", 2003

Stallings, W. "Cryptography and Network Security: Principles and Practices."

Third Edition, Pearson Education, Inc. 2003.

Stephanie Anderson, University of Miami, "*Privacy/Data Protection Project*", 2006

Steven," *Recommendations of the National Institute of Standards and Technology*" 2005

Thomas Porter, "*H.323 Mediated Voice over IP: Protocols, Vulnerabilities & Remediation*", 2004.

W.C. Hardy, "*QoS Measurement and Evaluation of Telecommunication Quality of Service*", 2003