PROTOTYPE DEVELOPMENT OF VOIP STEGANOGRAPHY

ABDULALEEM ZAID MOHAMMED AL-OTHMANI

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

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

NOVEMBER 2009

Dedicated to

My beloved parents, my darling supportive wife, my gorgeous daughter, my dearest siblings and to all whom were beside me

ACKNOWLEDGEMENT

First and foremost praise and gratitude be to ALLAH, almighty, without whose gracious help it would have been impossible to accomplish this work.

I was extraordinarily fortunate in having Prof. Dr. Azizah Bt. Abd Manaf as my supervisor in UTM. I would like to express my gratitude and appreciation to her, who has supported me throughout my project with her patience and knowledge whilst allowing me the room to work in my own way. I attribute the level of my Masters degree to her encouragement and effort and without her this project, too, would not have been completed or written. One simply could not wish for a better or friendlier supervisor.

Many thanks to each lecturer in UTM-CASE, they were my guidance to achieve my goals, they gave me all the support I need and were always kind. My entire study in this honorable institute was an everyday opportunity to acquire fine knowledge.

Furthermore, my special thanks go to my friend and colleague Saeed AlQahtani for his indispensable advices, valuable assistance and sincere companionship.

Finally and most importantly, words fail me to express my appreciation to my wife whose dedication, love and persistent confidence in me, has taken the load off my shoulder. I owe her for being unselfishly let her intelligence, passions, and ambitions collide with mine. I am deeply and forever indebted to my parents for their inseparable support, love and prayers throughout my entire life. I am also very grateful to all my brothers and sisters.

ABSTRACT

Information Security has evolved significantly over the last decade and even more quickly over the last few years. Most organizations recognize that one of their most important assets is their data. Steganography is an effective means of hiding secret data, thereby protecting the data from unauthorized or unwanted viewing. Indeed, along with encryption, steganography is one of the fundamental ways by which data can be kept confidential. Hiding the desired secret information in seemingly innocent multimedia files or medium will avoid the need to secure communication channel when sending secret messages. The biggest challenge to steganography is how to increase the amount of information to be embedded in the host channel without affecting the properties of that channel while keeping this secret transmission invisible to unauthorized parties. To face this challenge, many methods, media, techniques and algorithms are being introduced. One of the new and promising communication medium that can be used as a host for steganography is Voice over Internet Protocol. VoIP is a form of communication that allows people to make phone calls over an internet connection instead of typical analogue telephone lines. VoIP characteristics, such as, real-time transmission, bi-directional nature and vast amount of data make it very appropriate medium to hide secret data. Few recent researches were conducted to elucidate the steganography techniques and theories that can be applied on VoIP. This project concerns available steganographic techniques that can be used for creating covert channels for VoIP streams. Based on that, the proposed prototype is configured to apply some of these techniques in lab environment. Consequently, some suggested improvements and techniques are introduced in this project report to enhance VoIP steganography.

ABSTRAK

Keselamatan maklumat telah berevolusi pesat selama sedekad lalu, lebih-lebih lagi beberapa tahun kebelakangan ini. Kebanyakan organisasi sedia maklum bahawa salah satu aset terpenting mereka ialah data. “Steganography” ialah salah satu asset cara berkesan untuk menyembunyikan data sulit dan melindunginya dari dilihat oleh pihak yang tidak berkenaan. Bersama “encryption”, “steganography” adalah salah satu langkah asas agar data kekal sulit. Dengan menyembunyikan data sulit di dalam fail multimedia biasa atau medium yang normal, saluran komunikasi tidak perlu dikawal ketat apabila menghantar mesej rahsia. Cabaran terbesar untuk “steganography” ialah bagaimana untuk menambah saiz informasi yang boleh dimasukkan ke dalam “host channel” dan pada masa yang sama mengekalkan ciri-ciri saluran tersebut supaya ia tidak dapat dilihat oleh pihak yang tidak berkenaan. Pelbagai cara, media, teknik dan algoritma sedang diperkenalkan untuk menghadapi cabaran ini. Salah satu daripada medium komunikasi yang baru dan berpotensi untuk digunakan sebagai perumah untuk “steganography” ialah “Voice over Internet Protocol”. VoIP ialah satu bentuk komunikasi “online” di mana pengguna boleh membuat panggilan telefon menggunakan Internet. Ciri-ciri VoIP iaitu “real-time transmission”, “bi-directional nature” dan jumlah data yang banyak membuatkan ia medium yang sesuai untuk menyembunyikan data sulit. Beberapa kajian terbaru telah dijalankan untuk menerangkan teori dan teknik “steganography” yang boleh digunakan untuk VoIP. Projek ini ialah berkenaan teknik “steganography” sedia ada yang boleh digunakan untuk mencipta saluran rahsia untuk VoIP. Berdasarkan teknik ini, satu prototaip cadangan telah dibina untuk mempraktikkan beberapa teknik tersebut di dalam “lab environment”. Seterusnya, beberapa cadangan pengubahsuaian dan teknik diperkenalkan dalam laporan projek ini untuk memperbaiki VoIP “steganography”.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview

Steganography is the process of hiding secret data inside other, normally transmitted data. In other words, as defined by [40] steganography means hiding of a secret message within an ordinary message during sending or transmission phases and its extraction at the destination point. Ideally, anyone scanning this information will fail to know whether it contains covert data or not.

Steganography applications conceal information in other, seemingly innocent media. Steganographic results may masquerade as other file for data types, be concealed within various media, or even hidden in network traffic or disk space. We are only limited by our imagination in the many ways information and data can be exploited to conceal additional information [49].

Steganographic techniques for hiding messages have been around for as long as cryptography and have evolved with technology. One of major advantages of steganography over simply scrambling messages using cryptographic techniques is that probable eavesdroppers don't know what to listen to and whether there is a hidden data or not [23]. A covert channel is one of the most popular steganographic techniques that can be applied in the networks.

The covert channel offers an opportunity to manipulate certain properties of the communications medium in an unanticipated, unconventional, or unforeseen way, in order to transmit information through the medium without detection by anyone other than the entities operating the covert channel [40].

Voice over Internet Protocol (VoIP), or IP telephony, is defined by [1] as a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks".

At the present time, VoIP is one of the most popular services in the Internet. It was introduced to the telecommunication market and since then, changed it completely and gradually. As it is used worldwide more freely, the traffic volume that it generates is still increasing. Because of its popularity, it is becoming a natural target for steganography. That is why VoIP is appropriate to enable hidden communication throughout IP networks [40]. This new area and medium of steganography is going to be one of the most popular media to be used to hide data over internet networking due to the relatively huge amount of data that could be hidden, the real time nature of VoIP calls and the bi-directional capability that is provided by such transmission.

1.2 Background of the Problem

No real-world steganographic method is perfect: no matter what the method is, the hidden information can be potentially revealed. Generally, the more hidden information is inserted into the normally transmitted data, the greater the chance it will be detected [43].

Because the number of steganographic methods and mechanisms which are applicable on VoIP streaming is large, steganography in VoIP should be considered

as an excellent, secure and efficient way to hide data over IP networking. Moreover, the fact that until now there is no single method to detect hidden data within VoIP streaming, VoIP steganography should be considered safe and invulnerable for more few years ahead.

Like conventional steganography, VoIP steganography techniques can be unsafe to organizations because of the risk of confidential information leakage [28]. These are also the reasons that make some researchers suggested that VoIP steganography should be treated as a threat to public security. It is thus important to understand the essential nature of various steganographic methods and, in effect, be able to construct effective steganalysis solutions.

Nevertheless, for good purposes, it is very useful to identify and find out better steganographic techniques and approach or to improve the existing ones to make hiding data within VoIP streams more secure, efficient and practical.

1.3 Problem Statement

Mazurczyk and Szczypiorski [44] stated that securing Internet Telephony is a complex process. This not only means the ability to make secure conversation between two communicating parties, but also the security of signaling messages used to make this call possible at all. It may also means the security of the steganographic or watermarking channels that may be used within the VoIP streaming signals.

Providing methods and techniques to hide data in a very popular medium like VoIP is a challenging goal. It is obvious that there are limitations on the amount of secret data that should be buried in VoIP streaming without affecting the overall voice stream during VoIP call. The fact that there are limitations on the rate of covert data makes it harder to introduce secure and practical techniques which provide

larger rate of impeded data. In addition, [16] stated that if covert data rate is too high it may cause voice quality deterioration and increased risk of detection.

The problem that this project is proposed to solve is how to provide or suggest efficient VoIP steganography techniques or improvements to increase the rate of the impeded secret data within VoIP stream without effecting the overall conversation process of the VoIP calls? How VoIP steganography system that applies one or more of these enhanced techniques could be implemented, keeping in mind that, to my best knowledge, until now, there is no known such system?

1.4 Project Aim

While the overall idea of using steganography to implement covert communications is not new, burying hidden message in internet phone calls represents the latest evolution of steganography [23].

The main aim of this project is to implement a simple prototype by utilizing some steganography techniques on VoIP streaming in order to investigate how to increase the overall rate of covert data without affecting the voice quality and with less rate of detection.

These investigations will be done in accordance with what have been found by other researchers in this field, even though it is still a very new area of research and there is only very small number of researches on this subject.

1.5 Project Objectives

The objectives of this project are:

1. To study VoIP steganography, analyze its current techniques and discuss their performance in terms of capacity.
2. To develop a simple lab-based system that performs VoIP steganography using one or more LSB techniques to illustrate the VoIP steganography process.
3. To suggest effective ways to improve the capacity of covert data in VoIP steganography.

1.6 Project Scope

VoIP steganography covers a wide range of information hiding techniques; including popular techniques based on IP or TCP and others protocols. The main idea is to use free, redundant or unused fields of these protocols [43].

There are many techniques that could be used to hide communications in various layers of VoIP traffic. One of them is by taking advantage of unused or rarely used data fields.

In this research, I will study available covert channels that may be utilized for hidden communication for SIP protocol used as a signaling protocol for VoIP service. Moreover, new steganographic methods that were introduced very recently will be studied in this project. For each of these methods, this research will estimate potential bandwidth to later evaluate how much information may be transferred in a typical IP telephony call. I will study also the ability to use the payload of the voice packets in VoIP real-time steganography process.

As mentioned before, this project program will be designed and implemented to work in a lab-based environment. This means, the VoIP call will be limited to two hosts using point-to-point connection with static IP addresses. This is different from the real life VoIP applications which use client-server calls. As a result, the system

will be based on LAN network which provides an environment with almost zero noise. This will greatly help to get better VoIP steganography performance and correctness. Due to the complexity of VoIP steganography, only specific basic types of visual and statistical measures will be considered.

The most important success factors of this project are keeping the overall changes of the VoIP stream very small so that they can be hardly noticed while embedding a large amount of covert data and providing maximum extraction of the hidden information.

1.7 Summary

In this chapter, an introduction to this project is provided as well as the aim, and objectives of this project. The underlying background of the problem was explained as the reason to choose this topic of the project. The scope of this project was identified and the problem statement was declared.