BUSITEMA UNIVERSITY

FACULTY OF ENGINEERING

DEPARTMENT OF COMPUTEBR ENGINEERING

SECRET CODE BASED COMMUNICATION SYSTEM OVER LOCAL NETWORK

BY

MUSABE ROBERT

BU/UG/2011/1177

EMAIL: robertmusabe@gmail.com

+256781758217

SUPERVISOR: MS OWOMUGISHA GODLIVER

A Project Report Submitted to the Department of Computer Engineering in Partial Fulfillment of the Requirement for the Award of the Degree of Computer Engineering of Busitema University

MAY 2017

DECLARATION

I, MUSABE ROBERT REGNO: BU/UG/2011/1177 hereby declare that this project report is my original work except where explicit citation has been made and it is not presented to any institution of higher learning for any academic award.

SIGNED………………………………..

MUSABE ROBERT

BU/UG/2011/1177

Date----------------------------------

APPROVAL

I certify that the project entitled “**secret code based communication system over Local network"** has been done with my supervision and is now ready for Examination.

SIGNED…………………………………

MS. OWOMUGISHA GODLIVER

Department of Computer Engineering

Date…………………………………………………..………………………………………

DEDICATION

I wish to dedicate this final project report to my beloved parents Mr. and Mrs. Rwomubanyoro Julius, to all my brothers, sisters and friends

ACKNOWLEDGEMENT

First and foremost, I extend my sincere and inexplicable gratitude to the almighty God who has enabled me to contrive through all the challenges up to this time. I would also like to acknowledge and appreciate my supervisor; Ms. Owomugisha Godliver, for her whole-heartedly support and guidance especially toward the accomplishment of my project and research. To all my lecturers am very grateful for the unwavering support rendered. To my classmates and friends who sacrificed their time and knowledge and engaged in discussions as regards to the successful development of my project proposal work; I also extend my thanks to my lovely parents who have always financed me in different endeavors as regards my Education is concerned.

Table of Contents

LIST OF FIGURES

LIST OF ACRONYMS

GSM- Global system for mobile communication

TDMA- time division multiple access

LAN- Local area network

WAP-Wireless access protocol

GPRS-General packet radio system

Mbps- Megabits per second

WWW-world wide web

PC- personal computer

AES- Advanced encryption standards

SMS- Short messaging system

TCP- Transmission control protocol

IP – Internet protocol

HTML- Hypertext markup languange

RDBMS- Rational database management system

DDA- Database architecture

SQL- Structured query language

GUI- Graphical user interface

AES- Advanced encryption standard

DES- Data encryption standard

ABSTRACT

A secret code based communication system over a local network is the subject system. This is a communication system that relies on the algorithms to encrypt and decrypt that is able to work with any type of message and files exchanged amongst computers connected on a local area network. The message and files are encrypted using secret keys that are selected by the sender and this secret key is made known via SMS to the receiver on his/her phone number. At the receiving end the message is retrieved upon entering the correct key similar to the one used to encrypt. In gathering requirements, consultation, interviews and document review concerning the existing security systems and their weakness were used. It was from the analysis of the gathered information that the development of secret code based communication system over a local network system kicked off. I designed the system in visual basic studio and wrote the code in C# which provided me with the basic picture on how the system would work and be integrated from it's constituent subsystems. The subparts of the system were tested prior to the system testing after which they were integrated. The functionality of the system was under the control of the algorithm/code that was written in C#. The system was finally subjected to system testing to verify and validate it is working.

CHAPTER ONE: INTRODUCTION.

1.0 Background

Internet and mobile communication have become vital part of our lives in the recent decade, but almost all of it is exposed to criminals [1]. Wireless networks have significantly impacted the world, since their initial deployment. These networks have continued to develop and their uses have significantly grown.

In network communication systems, exchange of information mostly occurs on networked computers, mobile phones and other internet based electronic gadgets. Unsecured data that travels through different networks are open to many types of attack and can be read, altered or forged by anyone who has access to that data [2].

The concept of saving sensitive information, keeping them secure is parallel to it [2]. Many techniques are introduced to safely transfer data over internet and these use encryption and decryption methods however, new methods are also coming into practice day by day.

These essential requirements of secure communication over computer networks are ensured through cryptographic protection. Encryption is what provides communication with confidentiality, the assurance that transmitted information is only read by the recipient and not by an eavesdropper [3]. Authentication of users and data is provided by message authentication codes and digital signatures. The security of these functions relies on the fact that a legitimate user knows some secret information, a key unknown to attackers. If attackers somehow figure out this key, they can fully breach the systems security [3].

1.1 Problem statement

In any organization, secrecy and privacy are of paramount importance especially when more confidential and sensitive information is stored on computers and transmitted over the Internet, and there is a need to ensure information security and safety

However, the available security mechanisms for instance the use of passwords and firewalls are highly vulnerable to security threats any time such as interception and modification making these files and messages accessed by unintended parties or altered [4].

References

[1] AtulChaturvedi, ShyamSundar, *A Secure Key Agreement Protocol Using Braid Groups Department of Mathematics*, Internationnal Journal of Advanced Networking and Applications (IJANA), vol. 01, issue 05, 2012

[2] AT and T Bell."A cryptography file system for Unix".*presented at first ACM conference on communication and computing security. Fairfox, November 3-5 1993.*

[3] Prakash GL, Dr.Manish Prateek and Dr. Under Singh." *Data Encryption and decryption algorithm using key rotation for data security in cloud computing*". International journal for engineering and computer science, volume3, issue 4, April 2014.

[4] Thomas Willinger, Jorge Guajard and Christ of Paar. "A cryptography in embedded systems". *Presented at embedded world 2003 exhibition and conference. Nuremberg, Germany, February 18-20, 2003.*

[5] Sakinah Ali pitchay and Farida Ridzuarn" *proposed system concept on enhancing encryption and decryption method for cloud computing*". *Presented at the international conference on modelling and simulation.* AMSS, UK, January, 17, 2015.

[6] EMilly Shen and Brent Waters. " predicate privacy in encryption systems". *Presented at homeland security conference under grant award,* Homeland, USA, November 17, 2006.

[7] Mahdi AL-qdah."*Simple encryption/decryption Application*". International journal of computer science and security, volume 1, issue1.

[8] J.G. Proakis, *Digital Communications*. 3rd Ed. New York: McGraw-Hill, 1995.

[9] Heshem A. El Zouka, *providing end-to-end secure communications in gsm networks*, International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.4, July 2015

[10] *Transmission Systems for Communications*, 4th ed., Western Electric Co., Winston-Salem, NC, 1995, pp. 44–60.

[11] Don Coppersmith, ShaiHalevi, and CharanjitJutla. Cryptanalysis of stream ciphers with linear masking

[12] *Paul Zandbergen.(2017 Feb 02)* Systems Security: Firewalls, Encryption, Passwords & Biometrics [on line]. Available: http://WWW.study.com

[13] In Moti Yung, editor, Advances in Cryptology CRYPTO 2012, volume 2442 of Lecture Notes in Computer Science, pages 515-532. Springer Berlin Heidelberg, 2012.