

قال تعالى

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

اللَّهُ لَا إِلَهَ إِلَّا هُوَ

الْحَيُّ الْقَيُّومُ لَا تَأْخُذُهُ سِنَّةٌ وَلَا نَوْمٌ لَهُ مَا فِي السَّمَوَاتِ وَمَا

فِي الْأَرْضِ مَنْ ذَا الَّذِي يَشْفَعُ عِنْدَهُ إِلَّا بِإِذْنِهِ يَعْلَمُ مَا بَيْنَ

أَيْدِيهِمْ وَمَا خَلْفَهُمْ وَلَا يُحِيطُونَ بِشَيْءٍ مِّنْ عِلْمِهِ إِلَّا بِمَا

شَاءَ وَسِعَ كُرْسِيُّهُ السَّمَوَاتِ وَالْأَرْضَ وَلَا يَئُودُهُ حِفْظُهُمَا

وَهُوَ الْعَلِيُّ الْعَظِيمُ ﴿٢٥٥﴾

صدق الله العظيم

DEDICATION

I dedicate this work to:

My mother

for her support and creating an
enhancing atmosphere for me.

My father

for his support and
encouragement.

ACKNOWLEDGEMENT

First I give my full praise to **ALLAH** for giving me the will, the opportunity and the people to help me with my work. No words can be sufficient.

After that I dedicate my work to Prof. Saad Daoud Al-Shamma not only for supervising this work, but for doing so with sincerity.

Then, my gratitude and sincerest appreciation goes to the Nile Electronic Systems Center (NESC) for allowing me to use their premises, and for their assistance and technical support.

I am also indebted to Ustaza Intsar Ibrahim for kindly providing me with RC4 algorithm code.

Finally no words are enough for my friend Ala Addin Ismaiel for coming to my rescue when badly needed in the spirit of a true friend.

To all of you friends:

I can not and well not forget what you have done for me.

ABSTRACT

This thesis focuses on designing and implementing a system that can transmit voice over Local Area Network (LAN) in a secure manner. The implementation of the system is done by using both hardware and software. The system consists of a managing server and the end-user units. Signals provided between them by using an especial, nonstandard, private and customizable protocol.

This system provides other services beside the secure voice transmission including the ability to work in static or dynamic Ethernet LAN. In addition, it has a dynamic HTML page to configure the end-user units.

مستخلص

تم في هذا البحث تصميم نظام لنقل الصوت عبر الشبكات المحلية بشكل يدعم السرية في النقل. يتكون هذا النظام من جزئين هما جهاز حاسب شخصي يعمل كمخدم مركزي يدير ويتحكم في جميع عمليات النظام ووحدات (هواتف) مستخدمى النظام. بمعنى أن هذا النظام يتكون من العتاد الصلب والبرمجيات الداعمة له.

يتم التحكم في هذا النظام عبر إشارات مختلفة يتم تبادلها بين الوحدات من جهة والمخدم المركزي من جهة أخرى. تمثل هذه الإشارات بروتوكول التخاطب بين مكونات النظام. يمتاز هذا البروتوكول بأنه خاص وقابل للتعديل والتطوير.

يوفر هذا النظام عدد من الخدمات الأخرى بجانب نقل الصوت عبر الشبكات المحلية بصورة تدعم السرية . فهو يوفر صفحة انترنت محمية بكلمة مرور في وحدات المستخدمين تمكن المشرف على الشبكة من تهئية هذه الوحدات من أي جهاز في الشبكة. كما يمكن أن يعمل هذا النظام ضمن الشبكات المحلية ذات العنوان الثابت أو الديناميكي.

TERMINOLOGIES

ATM	Asynchronous Transfer Mode
CVSD	Continuously Variable Slope Delta Modulation
DES	Data Encryption Standard
HTTP	Hypertext Transfer Protocol
IOS	International Organization for Standards
IP	Internet Protocol
IPv4	Internet Protocol version 4
MMUSIC	Multiparty Multimedia Session Control working group
OSI	Open System Interconnection
PSTN	Public Switching Telephone Network
QoS	Quality of Service
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SSL	Secure Sockets Layer
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
TCP	Transport Control Protocol
TLS	Transport Layer Security
TDES	Triple Data Encryption Standard
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
WPA	WiFi Protected Access protocol
WEP	Wired Equivalent Privacy protocol

List Of Figures

Figure	Title	Page #
1-1	OSI Model vs TCP/IP Model-----	02
1-2	IPv4 header -----	03
1-3	TCP header -----	05
1-4	UDP header -----	06
1-5	SIP protocol stack -----	07
1-6	SIP architecture. -----	08
2-1	Encryption category according to the number of keys -----	13
2-2	Simplified Model of Single-key Encryption -----	14
2-3	DES implementation -----	15
2-4	Initialization of S -----	17
2-6	Using (T) to produce initial permutation of (S) -----	18
2-6	Stream Generation in RC4 -----	18
2-7	RC4 example -----	19
3-1	The System Components -----	26
3-2	System Operation -----	27
3-3	Part one of the end-user Unit -----	29
3-4	Part two of the end-user Unit -----	30
3-5	General format of the protocol header -----	31
3-6	REQUIST_TO_REGISTER packet -----	33
3-7	REPLY_FOR_REGISTER packet -----	33
3-8	CALL_REQUIST packet -----	33
3-9	CALL_REPLY Packet with status NOT_AVAILABLE -----	34
3-10	CALL_REPLY Packet with status BUSY or FREE -----	34

3-11	CALL_END Packet with status CALL_CANCELED -----	35
3-12	CALL_START Packet -----	35
3-13	CALL_END Packet with status CALL_ENDED -----	35
3-14	Negative acknowledgment “NOT_FOUND” packet -----	36
3-15	The starting page -----	38
3-16	Access the page by the administrator only -----	38
3-17	The configuration page -----	39

List Of Tables

Table	Title	Page #
1-1	The functionality of TCP/IP layers -----	03
1-2	IPv4 header fields description -----	04
1-3	Defines SIP messages -----	08
1-4	Defines SIP messages -----	09
2-1	Performance of symmetric cipher algorithms on Pentium II-----	19
2-2	Applications of public key encryption -----	21
3-1	Signals between the two units of end user unit -----	31
3-2	The available commands -----	32
3-3	The available statuses -----	32

Table Of Contents

DEDICATION	II
ACKNOWLEDGEMENT	III
ABSTRACT	IV
	V
مستخل ص	
TERMINOLOGIES	VI
FIGURES INDEX	VII
TABLES INDEX	IX

Chapter one Introduction

1.1 Voice over Internet Protocol (VoIP)	01
1.1.1 Definition	01
1.1.2 The importance of Voice over IP	01
1.2 Overview of Internet Protocol (IP) Network	02
1.2.1 IP protocol (Internet Layer)	03
1.2.2 Transport Control Protocol (TCP) (Transport Layer) ---	04
1.2.3 User Datagram Protocol (UDP)(Transport Layer) -----	05
1.3 Voice over Internet Protocol Signaling	06
1.3.1 Session Initiation Protocol (SIP)	06
1.3.2 Key Benefits of Session Initiation Protocol	07
1.3.3 Session Initiation Protocol Components	07
1.3.4 Session Initiation Protocol Messages	08
1.3.5 Session Initiation Protocol supported protocols	09

1.4 Introduction to security -----	10
1.4.1 Security Services and Attacks -----	10
1.4.1.1 Security -----	10
1.4.1.2 Security attacks -----	11
1.5 Cryptography -----	11

Chapter two The security concepts

2.1 Cryptography algorithms categories -----	13
2.2 Single-key encryption -----	14
2.2.1 Block cipher -----	14
2.2.1.1 Data Encryption Standard (DES) -----	14
2.2.2 Stream cipher -----	16
2.2.2.1 RC4 encryption algorithm -----	16
2.2.2.1.1 RC4 Definition -----	16
2.2.2.1.2 RC4 Implementation -----	17
2.2.2.1.3 RC4 features -----	19
2.3 Public-key Encryption -----	20
2.3.1 The uses of public-key encryption -----	20
2.3.2 RSA algorithm -----	21
2.3.2.1 Description of the Algorithm -----	21
2.4 Security in Voice Communication System over Network -----	23

Chapter three Implementation

3.1 General overview of the system -----	26
3.1.1 The system components -----	26
3.1.2 The system operation -----	27
3.2 A detailed view of the hardware implementation -----	29
3.2.1 Part one of end-user unit (U1) -----	29

3.2.2	Part two of end-user unit (U2) -----	30
3.3	A detailed view of the software implementation -----	31
3.3.1	Signals and Protocol Implementation -----	31
3.3.1.1	(U1-U2) signals -----	31
3.3.1.2	(U2-S) signals -----	31
3.3.1.2.1	Header fields' description -----	32
3.3.1.3	The protocol Implementation -----	33
3.3.2	The code description -----	36
3.3.2.1	The server programming -----	37
3.3.2.2	The module programming -----	37
3.4	The security implementation -----	40
3.4.1	Key Distribution -----	40
<u>Chapter four</u> Conclusion and Recommendations		
4.1	Conclusion -----	41
4.2	Recommendations -----	41
<u>References</u>	-----	43
<u>Appendix</u>		
Appendix A	The Hardware Specifications of the Part Two of the End user Unit -----	44
Appendix B	CVSD theory -----	49