

## **Acknowledgements**

This work was carried out in cooperative research and development project. Our deepest gratitude is due to my supervisor, Dr. Yahyia Abdalla Mohammed for his guidance, encouragement, and kind helpful which made this work possible.

I am, also would like to thank Engineer Nazar Elshamy for his unlimited support and helps.

And, of course, thank my family for standing beside me all the time.

# Abstract

IPSec is a framework of open standards for ensuring private communications over IP networks which has become the most popular network layer security control. It can provide several types of data protection: confidentiality, integrity, data origin authentication and access protection. The most common uses is a virtual private network (VPN) which is built on top of existing physical networks that can provide a secure communications mechanism for IP information transmitted between networks.

This research seeks to assist organizations in mitigating the risks associated with the transmission of sensitive information across networks by providing practical example on implementing security services based on Internet Protocol Security (IPSec) and show how IPSec can effect on file transferring time through the networks.

Implementation of IPSec had been done in a Linux Router in two deferent LANs and the testing result shown that there is an effect in transferring time of the data with a large size. The data analysis gives a leaner equation with a factor of X (the file size) equal (0.20) before IPSec implementation and it increase to (0.21) after IPSec implementation and this increase the time of files transferring through the network.

## المستخلص

أمن بروتوكول الإنترنت (IPSec) هو إطار من المعايير المفتوحة لضمان الاتصالات الخاصة عبر شبكات بروتوكول الإنترنت (IP) التي أصبحت الأكثر شعبية كمتحكم لبطاقة أمن الشبكة. يمكنه توفير عدة أنواع من الحماية للبيانات : السرية والتكامل وتوثيق بيانات المنشأ وحماية الوصول. الاستخدامات الأكثر شيوعاً هي شبكة خاصة افتراضية (VPN) التي بنيت أعلى الشبكات القائمة المادية التي يمكن أن توفر آلية لتأمين اتصالات البيانات ومعلومات بروتوكول الإنترنت (IP) التي تنتقل بين الشبكات.

يسعى هذا البحث لمساعدة المنظمات في مجال التخفيف من المخاطر المرتبطة بقل المعلومات الحساسة عبر الشبكات من خلال تقديم مثال عملي على تنفيذ الخدمات الأمنية يعتمد على أمن بروتوكول الإنترنت (IPSec) ، وتبين كيف أن أمن بروتوكول الإنترنت يمكن أن يستخدم كوسيلة لحل القضايا الأمنية بالشبكة.

تطبيق أمن بروتوكول الإنترنت (IPSec) تم عمله في جهاز التوجيه لينكس في شبكتين محليتين مختلفتين ونتيجة الاختبار أظهرت أن هناك أثر في زمن نقل البيانات ذات الحجم الكبير، وتحليل البيانات أعطى معادلة خطية بمعامل لقيمة (X وهي حجم الملف) تساوي (0.20) قبل تطبيق IPSec وزاد إلى (0.21) بعد تطبيق IPSec وهذا زاد من زمن نقل الملفات عبر الشبكة.

# Table of Contents

Title	Page
Acknowledgements	i
Abstract	ii
المستخلص	iii
Table of contents	iv
List of Figures	viii
List of Tables and Charts	ix
List of Abbreviations	x
<b>Chapter 1: Introduction</b>	<b>1</b>
1.1 Introduction	2
1.2 Problem definition	2
1.3 Solution and objective	2
1.4 Scope	2
1.5 Methodology	3
1.6Thesis Layout	3
<b>Chapter 2: IPSec and Kerberos</b>	<b>4</b>
2.1 IPSec Definition	5
2.2 IPSecurity	6

2.2.1 Authentication Header (AH)	7
2.2.1.1 Authentication Header (AH) modes	7
2.2.1.2 Integrity protection process	8
2.2.1.3 AH Header	9
2.2.1.4 Transport mode	10
2.2.1.5 Tunnel mode	11
2.2.1.6 Authentication Algorithms	13
2.2.2 Encapsulating Security Payload (ESP)	14
2.2.2.1 ESP Modes	14
2.2.2.2 Packet Fields	15
2.2.2.3 ESP in Transport Mode	17
2.2.2.4 ESP in Tunnel Mode	18
2.2.3 Internet key Exchange (IKE)	18
2.2.3.1 Phase One Exchange	19
2.2.3.2 Main mode	19
2.2.3.3 Aggressive mode	20
2.2.3.4 Phase Two Exchange	20
2.2.3.5 Key Management	22
<b>Chapter 3: Implementation Environment and Software</b>	<b>23</b>
3.1 Network Scenario	24
3.2 Some Network Components Definitions	24
3.2.1 Router	24

3.2.2 Proxy Server	26
3.2.3 WAN Devices	26
3.2.3.1 Asymmetric Digital Subscriber Line (ADSL)	26
3.2.3.2 Single-Pair High-speed Digital Subscriber Line (SHDSL)	26
3.3 IPSec Software	27
3.4 Bandwidth Software Tools	29
<b>Chapter 4: Security Services Implementation, Testing and Results</b>	<b>31</b>
4.1 IPSec platform	32
4.2 Servers Configuration	32
4.2.2 Certification Authority Configuration	33
4.2.3 Setting up OpenVPN	33
4.3 Network Performance Results	35
<b>Chapter 5: Conclusion and Recommendation</b>	<b>39</b>
5.1 Conclusion	40
5.2 Recommendation	40
<b>References</b>	<b>41</b>
<b>Appendix</b>	<b>43</b>

## List of Figures

<b>Figure No</b>	<b>Page</b>
2.1: AH Tunnel mode packet	7
2.2: AH Transport mode packet	8
2.3: AH Header	10
2.4: IPSec in AH Transport Mode	10
2.5: IPSec in AH Tunnel Mode	12
2.6: HMAC for AH Authentication	13
2.7: ESP Tunnel Mode Packet	14
2.8: ESP Transport Mode Packet	15
2.9: ESP Packet Fields	17
2.10: IPSec in ESP Transport Mode	17
2.11: IPSec in ESP Tunnel Mode	18
3.1: Network Scenario	24
4.1: Implementation scenario	32
4.2: Downloading time before and after IPSec Implementation	36
4.3: Uploading time before and after IPSec Implementation	38

## **List of Tables and Charts**

<b>Table No</b>	<b>page</b>
1: Downloading Time before IPSec Implementation	35
2: Downloading Time after IPSec Implementation	35
3: Uploading Time before IPSec Implementation	37
4: Uploading Time after IPSec Implementation	37

# List of Abbreviations

<b>Term</b>	<b>Definition</b>
3DES	Triple Data Encryption Standard
ADSL	Asymmetric digital subscriber line
AES	Advanced Encryption Standard
AH	Authentication Header
BGP	Border Gateway Protocol
CA	Certificate Authority
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
KDC	Key Distribution Center
ICV	Integrity Check Value
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
ISAKMP	Internet Security Association Key Management Protocol
LAN	Local Area Network
MAC	Message Authentication Code
MIT	Massachusetts Institute of Technology
NAT	Network Address Translation
NTP	Network Time Protocol
OSPF	Open Shortest Path First

RIP	Routing Information Protocol
SA	Security Association
SAD	Security Association Database
SHDSL	Single-Pair High-speed Digital Subscriber Line
SPD	Security Policy Database
SPI	Security parameters index
SSH	Secure Shell
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network