

Synchronizing Internet Protocol Security (IPSec)

Advances in Information Security

Sushil Jajodia

Consulting Editor

Center for Secure Information Systems

George Mason University

Fairfax, VA 22030-4444

email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

SECURE DATA MANAGEMENT IN DECENTRALIZED SYSTEMS edited by Ting Yu and Sushil Jajodia; ISBN: 978-0-387-27694-6

NETWORK SECURITY POLICIES AND PROCEDURES by Douglas W. Frye; ISBN: 0-387-30937-3

DATA WAREHOUSING AND DATA MINING TECHNIQUES FOR CYBER SECURITY by Anoop Singhal; ISBN: 978-0-387-26409-7

SECURE LOCALIZATION AND TIME SYNCHRONIZATION FOR WIRELESS SENSOR AND AD HOC NETWORKS edited by Radha Poovendran, Cliff Wang, and Sumit Roy; ISBN: 0-387-32721-5

PRESERVING PRIVACY IN ON-LINE ANALYTICAL PROCESSING (OLAP) by Lingyu Wang, Sushil Jajodia and Duminda Wijesekera; ISBN: 978-0-387-46273-8

SECURITY FOR WIRELESS SENSOR NETWORKS by Donggang Liu and Peng Ning; ISBN: 978-0-387-32723-5

MALWARE DETECTION edited by Somesh Jha, Cliff Wang, Mihai Christodorescu, Dawn Song, and Douglas Maughan; ISBN: 978-0-387-32720-4

ELECTRONIC POSTAGE SYSTEMS: Technology, Security, Economics by Gerrit Bleumer; ISBN: 978-0-387-29313-2

MULTIVARIATE PUBLIC KEY CRYPTOSYSTEMS by Jintai Ding, Jason E. Gower and Dieter Schmidt; ISBN-13: 978-0-378-32229-2

UNDERSTANDING INTRUSION DETECTION THROUGH VISUALIZATION by Stefan Axelsson; ISBN-10: 0-387-27634-3

QUALITY OF PROTECTION: Security Measurements and Metrics by Dieter Gollmann, Fabio Massacci and Artsiom Yautsiukhin; ISBN-10: 0-387-29016-8

Additional information about this series can be obtained from

<http://www.springer.com>

Synchronizing Internet Protocol Security (SIPSec)

by

Charles A. Shoniregun
University of East London
UK

 Springer

Charles A. Shoniregun
Reader in Computing
KNURE/KSAC Distinguished Professor
School of Computing & Technology
University of East London
Docklands Campus, University Way
London E16 2RD
United Kingdom
Email: C.Shoniregun@uel.ac.uk

Library of Congress Control Number:

Synchronizing Internet Protocol Security (SIPSec) by Charles A. Shoniregun

ISBN-13: 978-0-387-32724-2

e-ISBN-13: 978-0-387-68569-4

Printed on acid-free paper.

© 2007 Springer Science+Business Media, LLC.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

9 8 7 6 5 4 3 2 1

springer.com

DEDICATION

To my late mother Juliana O. Shoniregun (1934–2006)

TABLE OF CONTENTS

Dedication v

List of contributors and organisations xvii

Preface xix

Acknowledgements xxi

Chapter 1

Research overview and conceptual understanding

of internet protocol security (IPSec)

1. Introduction 1

2. Research rationale 2

3. Research hypothesis 5

5. Methods and methodology 9

6. Internet architecture board (IAB)? 10

7. IPSec roadmap 12

8. Analogy of IPSec 18

9. IPSec relationship with other protocols 20

10. Business perception 26

11. Summary of chapter one 27

References 28

Chapter 2

Internet communication protocols

1. Introduction 31

2. TCP/IP protocol 31

3. Security problems of TCP/IP layers 34

4. Benefits and limitations of implementing security at the application, transport, network, and data link layers 41

5. IPSec standards 46

6. Why AH 54

7. Why ESP 56

8. Security association (SA) and key management 62

9. IKE: hybrid protocol 64

10. Policy 69

11. Summary of chapter two 70

References 73

Chapter 3

Internet protocol versions 4 (IPv4) and 6 (IPv6)

1. Introduction 75

2. IPv4 standard 76

3. IPv4 limitations and possible solution 80

4. IPv6 standard 83

5. Difference between IPv4 and v6 92

6. Transition	97
7. Summary of chapter three.....	105
References	105
Chapter 4	
Implementations and limitations of the IPSec	
1. Introduction.....	107
2. Classification and taxonomy of the IPSec	107
3. Combining the IPSec protocols to create a Virtual Private Network (VPN).....	108
4. IPSec in Windows.....	119
5. Linux.....	127
6. Solaris	128
7. FreeBSD.....	132
8. Cisco IOS IPSec configuration overview	136
9. Routers	139
10. Limitations of the IPSec	141
11. Summary Of Chapter four	153
References	153
Chapter 5	
Synchronising Internet Protocol Security (SIPsec) model	
1. Introduction.....	155
2. Analysis of questionnaire survey.....	155
3. Case studies.....	156
4. Laboratory experiments	157
5. Current IPSec solutions	157
6. Public key algorithms	161
7. Analysis of findings	164
8. Conceptual understanding of SIPSec model.....	166
9. Policy reconciliation	172
10. Palmistry	178
11. Fingerprint	182
12. Face.....	184
13. Iris	185
14. Result summary of hypotheses.....	187
15. Summary of chapter five.....	188
References	188
Chapter 6	
Discussion	
1. Introduction.....	191
2. Issues in IPSec	191
3. IPSec is an application specific.....	199
4. Current use of biometrics technology.....	203

5. Combining biometrics with IPSec 204

6. Underpinning assumption of SIPSec 207

7. Summary of chapter six 207

References 208

Chapter 7

Conclusion

1. Dependence on information technology 211

2. Global issues on internet security 213

3. Root causes of attacks 214

4. Recommendation 217

5. Contribution to knowledge 217

6. Future work 218

References 218

Index..... 219

LIST OF FIGURES

<i>Figure 1–1.</i> Conceptual ideology of IPSec identity.....	14
<i>Figure 1–2.</i> IPSec on two trusted private networks.....	16
<i>Figure 1–3.</i> IPSec running on host machine.....	16
<i>Figure 1–4.</i> IPSec on host machines.....	17
<i>Figure 1–5.</i> SA concepts of follow one another	17
<i>Figure 1–6.</i> SA concept of partially superimposed.....	18
<i>Figure 1–7.</i> Analogy of IPSec as a House	18
<i>Figure 1–8.</i> Internet relationship with software and hardware.....	19
<i>Figure 1–9.</i> Analogy of IPSec Packets	19
<i>Figure 1–10.</i> Protocols relationship within IPSec	24
<i>Figure 1–11.</i> IPSec in different modes	26
<i>Figure 2–1.</i> TCP/IP Protocol Stack and OSI Reference Model.....	33
<i>Figure 2–2.</i> Data passing from one host to another.....	34
<i>Figure 2–3.</i> IPSec transport mode	48
<i>Figure 2–4.</i> IP packet in IPSec transport mode	49
<i>Figure 2–5.</i> IPSec tunnel mod	51
<i>Figure 2–6.</i> IPSec tunnel mode implementation	51
<i>Figure 2–7.</i> IP packet in IPSec tunnel mode.....	52
<i>Figure 2–8.</i> ESP Protocol (a and b)	52
<i>Figure 2–9.</i> IP packet in IPSec nested tunnel implementation	53
<i>Figure 2–10.</i> IP packet in IPSec nested tunnel mode	53
<i>Figure 2–11.</i> Contents of AH	55
<i>Figure 2–12.</i> IP packet protected by AH in transport mode	56
<i>Figure 2–13.</i> IP packet protected by AH in tunnel mode	56
<i>Figure 2–14.</i> ESP header and Trailer	60
<i>Figure 2–17.</i> IP packet protected by ESP in tunnel mode	60
<i>Figure 2–15.</i> The structure of the packets in the tunnel mode	61
<i>Figure 2–16.</i> The structure of the packets in the transport mode	61
<i>Figure 2–18.</i> IP packet protected by ESP in transport mode	62
<i>Figure 2–19.</i> IKE phase 1 main mode	66
<i>Figure 2–20.</i> IKE phase 1—aggressive mode	66
<i>Figure 3–1.</i> Content of precedence bit.....	77
<i>Figure 3–2.</i> Packet fragment.....	79
<i>Figure 3–3.</i> IPv4 Address formats	80
<i>Figure 3–4.</i> Underline principle of unicast.....	87
<i>Figure 3–5.</i> Structure of AGUA.....	87
<i>Figure 3–6.</i> Structure of Link Local Addresses	88
<i>Figure 3–7.</i> Structure of Site Local Addresses	89
<i>Figure 3–8.</i> Underline principle of Anycast	89
<i>Figure 3–9.</i> Underline Principle of Multicast.....	90

<i>Figure 3–10. Structure of Multicast Addresses</i>	90
<i>Figure 3–11. Structure of High–Order 3</i>	90
<i>Figure 3–12. Stateful Server Mode.....</i>	91
<i>Figure 3–14. IPv6 Extension Header.....</i>	93
<i>Figure 3–13. IPv6 Header format</i>	94
<i>Figure 3–15. Different Transition technologies.....</i>	97
<i>Figure 3–16. Dual IP layer architecture.....</i>	99
<i>Figure 3–17. SIIT and NAT-PT</i>	103
<i>Figure 3–18. Bump in the stack (BITS) and Bump in the API (BIA)</i>	104
<i>Figure 3–19. Socks and TRT</i>	104
<i>Figure 4–1. IKE/ISAKMP configuration policy.....</i>	113
<i>Figure 4–2. Crypto Map Configuration</i>	118
<i>Figure 4–3. Screen shot: net.exe.....</i>	122
<i>Figure 4–4. Screen shot: IPv6 install.....</i>	123
<i>Figure 4–5. Screen shot: IPv6 via network connections control panel</i>	123
<i>Figure 4–6. Screen shot: ipconfig command</i>	124
<i>Figure 4–7. Screen shot: ping6 command</i>	124
<i>Figure 4–8. Screen shot: tracert6 command</i>	125
<i>Figure 4–9. Screen shot: ipv6 rc (view the route cache)</i>	125
<i>Figure 4–10. Screen shot: ipv6 nc (view the neighbour cache).....</i>	126
<i>Figure 4–11. Screen shot: ipv6 if (view interface information).....</i>	126
<i>Figure 4–12. Screen shot: ipv6 ifc (configure interface attribute).....</i>	127
<i>Figure 4–13. Screen shot: Windows 2003 IPv6 via network connections ..</i>	128
<i>Figure 4–14. Screen shot: find out hostname. * files.....</i>	130
<i>Figure 4–15. Screen short: Sample of ipsecinit.conf file.....</i>	130
<i>Figure 4–16. Screen shot: netstat command.....</i>	131
<i>Figure 4–17. Screen shot: IP nodes and nsswitch.conf file</i>	131
<i>Figure 4–18. Screen shot: Kernel Configuration</i>	132
<i>Figure 4–19. Screen shot: Kernel automatically recognises devices.....</i>	133
<i>Figure 4–20. Screen shot: Installation main menu</i>	133
<i>Figure 4–21. Screen shot: Disk partition</i>	133
<i>Figure 4–22. Screen shot: Disk partition editor.....</i>	134
<i>Figure 4–23. Screen shot: Select ‘All’ using arrow keys.....</i>	134
<i>Figure 4–24. Screen shot: User confirmation requested.....</i>	134
<i>Figure 4–25. Screen shot: Canned distribution sets</i>	135
<i>Figure 4–26. Screen shot: Notification message for lost disk contents</i>	135
<i>Figure 4–27. Screen shot: Notification message for extracting sshare command.....</i>	135
<i>Figure 4–28. Screen shot: Notification message for completing installation.....</i>	135
<i>Figure 4–30. IOS Configuration at Initiator Router</i>	136
<i>Figure 4–29. Screen shot: Network interface information required.....</i>	136

<i>Figure 4–31. IOS Configuration at Responder Router</i>	137
<i>Figure 4–32. Basic concept of a firewall</i>	144
<i>Figure 4–33. Packet-filtering router</i>	144
<i>Figure 4–34. ALG connections to the application layer</i>	145
<i>Figure 4–35. CLG connections</i>	145
<i>Figure 4–36. NAT implementation</i>	147
<i>Figure 4–37. Translation table</i>	148
<i>Figure 5–1. Link-to-link encryption</i>	158
<i>Figure 5–2. Modified packet flow</i>	159
<i>Figure 5–3. IPSec tunnel mode protected packet</i>	159
<i>Figure 5–4. Modified IPSec packets</i>	159
<i>Figure 5–5. IPSec inside the TLC packet</i>	160
<i>Figure 5–6. TLC protected packet</i>	161
<i>Figure 5–7. IPSec impact factors</i>	165
<i>Figure 5–8. SIPSec Model</i>	168
<i>Figure 5–9. SIPSec Biometric Elements and Components</i>	170
<i>Figure 5–10. IPSec policy configuration</i>	174
<i>Figure 5–11. SIPSec application policy</i>	175
<i>Figure 5–12. Palmistry</i>	176
<i>Figure 5–13. Face Reading</i>	176
<i>Figure 5–14. Face Feature</i>	177
<i>Figure 5–15. Astrological Weight</i>	178
<i>Figure 5–16. Five States in the Palmistry Process</i>	179
<i>Figure 5–17. Palm Size</i>	179
<i>Figure 5–18. Palm Quality</i>	179
<i>Figure 5–19. Finger Shape</i>	179
<i>Figure 5–20. Palm Mountain</i>	180
<i>Figure 5–21. Palm Lines</i>	180
<i>Figure 5–22. Life Lines</i>	180
<i>Figure 5–23. Head Lines</i>	180
<i>Figure 5–24. Love Lines</i>	180
<i>Figure 5–25. Career Lines</i>	181
<i>Figure 5–26. Success Lines</i>	181
<i>Figure 5–27. Marriage Lines</i>	181
<i>Figure 5–28. Hand and Palm-vein pattern</i>	181
<i>Figure 5–29. Fingerprint Patterns</i>	183
<i>Figure 5–30. Six universal expressions</i>	184
<i>Figure 5–31. Distance Transform</i>	185
<i>Figure 5–32. Understanding Iris Recognition</i>	186
<i>Figure 6–1. Interception</i>	196
<i>Figure 6–2. Interception</i>	197
<i>Figure 6–3. Modification</i>	197

Figure 6–4. Disinformation or fabrication..... 197

Figure 6–5. VPN Connection200

LIST OF TABLES

<i>Table 1–1.</i> IPSec related Requests for Comment (RFC) Documentation	13
<i>Table 1–2.</i> Classification of passive and active attacks	21
<i>Table 2–1.</i> IP layer security vs Session layer security	41
<i>Table 2–2.</i> Encapsulating Security Payload (ESP)	52
<i>Table 2–3.</i> Companies Supporting IPSec software and hardware	71
<i>Table 3–2.</i> Precedence field	77
<i>Table 3–1.</i> IPv4 Header format	78
<i>Table 3–3.</i> IPv4 classes	79
<i>Table 3–4.</i> Range of special addresses	81
<i>Table 3–5.</i> Support for IPv6 by IXPs	84
<i>Table 3–6.</i> Support for IPv6 by ISPs	84
<i>Table 3–7.</i> Operating Systems IPv6 Status	85
<i>Table 3–8.</i> IPv6 Status of Commercial Routers	85
<i>Table 3–9.</i> IPv6 Status of Commercial Firewalls	85
<i>Table 3–10.</i> Operating Systems IPv6 Status	85
<i>Table 3–11.</i> Operating Systems IPv6 Status	86
<i>Table 3–12.</i> Values of scope filed	91
<i>Table 3–13.</i> Comparisons between the IPv4 and v6 Headers	96
<i>Table 3–14.</i> Main differences between IPv4 and v6	98
<i>Table 4–1.</i> Classification and Taxonomy of the IPSec operations	108
<i>Table 4–2.</i> Microsoft IPSec Components	120
<i>Table 4–3.</i> Enabling IPv6 on various operating systems	140
<i>Table 4–4.</i> Displaying IPv6 interface information	140
<i>Table 4–5.</i> Basic IPv6 command	140
<i>Table 4–6.</i> Vendors that are currently aware of affected products	152
<i>Table 5–1.</i> Organisational Adoption of IPSec	156
<i>Table 5–2.</i> IPv4 and v6 Test results	157
<i>Table 5–3.</i> Database integration	167
<i>Table 5–4.</i> Summary of hypotheses tested and results	187
<i>Table 6–1.</i> Securing general-purpose network servers	198
<i>Table 6–2.</i> Table of biometric technologies	206

LIST OF CONTRIBUTORS AND ORGANISATIONS

<i>Alex Logvynovskiy</i>	e-Centre for Infonomics, UK
<i>Brendan Cotter</i>	Kurt Geiger Ltd, UK
<i>Sonny Nwankwo</i>	University of East London, UK
<i>Kasim Charhabagi</i>	University of East London, UK
<i>Harvey Freeman</i>	Booze Allen Hamilton, USA
<i>Charles Winer</i>	Purdue University, Calumet, USA
<i>Caterina Scoglio</i>	Kansas State University, Kansas, USA
<i>Victoria Repka</i>	Kharkov National University of Radioelectronics, Ukraine
<i>Maaruf Ali</i>	Oxford Brooks University, UK
<i>Vyacheslav Grebenyuk</i>	Kharkov National University of Radioelectronics, Ukraine
<i>Kia Makki</i>	Florida International University, Miami, USA
<i>Niki Passinou</i>	Florida International University, Miami, USA
<i>Siân Lambert</i>	Manchester Metropolitan University, UK
<i>Seamus Simpson</i>	Manchester Metropolitan University, UK
<i>Terry Cook</i>	City University, USA.
<i>Jen-Yao Chung</i>	IBM Watson Research Centre, USA
<i>Liang-Jie (LJ) Zhang</i>	IBM Watson Research Centre, USA
<i>Patrick Hung</i>	University of Ontario, Institute of Technology, Canada
<i>Dragana Martinovic</i>	University of Windsor, Canada
<i>Victor Ralevich</i>	Sheridan Institute of Technology and Advance Learning, Canada
<i>Pit Pichappan</i>	Annamalai University, India
British Telecommunications Plc (BT), UK	
CERT Coordination Centre, USA	
Cisco, USA	
Dell, UK	
e-Centre for Infonomics, UK	
Honeywell, UK	
Internet Engineering Task Force (IETF)	
InternetSecurity.org.uk, UK	
Intrusion.com	
Microsoft Corp, USA	
National Security Agency, USA	
Sun Microsystems, Inc., USA	
TEISME.com, UK	
University of Massachusetts, USA	
VeriSign, Inc, USA	

PREFACE

The open design of the Internet has not only opened many new opportunities for communications, but it has also opened many new avenues for attackers against organisations network and computing resources. This book is a critical investigation of the Internet Protocol Security (IPSec) based on combination of theoretical investigation and practical implementation, which provides an in-depth understanding of the IPSec framework. The benefits of IPSec were exploited while the delimiting factors cannot be ignored. Information security has become a major concern in recent times as more and more computers are being connected to the global Internet. With so much data transferring over public networks, the risk of sensitive information has increased exponentially and the increase of Internet hosts continuously requires additional security support. The IPSec may be used in three different security domains: Virtual private networks, Application-level security, and Routing security. It comprises of suite of protocols, which are developed to ensure that the integrity, confidentiality and authentication of data communications over an IP network. The IPSec is predominately used in virtual private networks (VPNs). But when used in application-level security or routing security, the IPSec is not a complete solution and must be coupled with other security measures to be effective. As with other security systems, poor maintenance can easily lead to a critical system failure. This research is concerned with an investigation of the vulnerabilities that impair the IPSec, and detailed the packet-by-packet analysis of the protocol transactions in IPSec. The IPSec uses a number of different algorithms and protocols to provide a cohesive security framework. But the Internet has also given intruders the opportunity to carry out diverse levels of attacks, which threatening the privacy of users and integrity of important data. In depth research has also led to more significant reasons why IPSec has failed in certain situation. The current standard for the Internet protocol (IP) is completely unprotected, allowing hosts to inspect or modify data in transit. However, the use of one technique to overcome one problem raised issues for another. A more general and flexible solution is require, which can be easily integrated with the current IPSec without changes to it specification. This book also identifies the security problems facing the Internet communication protocols; the risks associated with Internet connection, delimitations of the IPSec and finally proposed a ‘Synchronisation of Internet Protocol Security (SIPSec)’ model. I strongly believed that the readers of this book would gain an in-depth knowledge of the problematic nature of IPSec architecture/operations and why SIPSec is necessary.

ACKNOWLEDGEMENTS

My searching for knowledge enhancement in Internet security has triggered many questions relating to the conceptual operations and the limitations of the IPsec. Having authored many books, it became apparent that the amount of existing work in IPsec cannot be ignored and the work have contributed to what has led me to rethink what can be done to enhance the current IPsec security performance. However, it is difficult to acknowledge all the people that have directly or indirectly contributed to this book. But some names cannot be forgotten — many thanks to my editor Susan Lagerstrom-Fife, publishing director Jennifer Evans and Rudiger Gebauer for their support. Indeed, those kind reminders and useful comments from Sharon Palleschi are all appreciated.

A special thank you to a dear friend Dr Alex Logvynovskiy of e-Center for Infonomics, for his never-ending contribution.

I sincerely thank Prof Mike Thorne, Alan Ingle, Vice Chancellor's Group – University of East London and all my post graduate students for their support. Undoubtedly, my reflection to past experiences in industry and academia has help to bridge the gap in my understanding of the IPsec architecture and its limitations. I would also like to acknowledge my appreciation to the following organisations: Cisco, Dell, e-Center for Infonomics, IETF, HP, IBM, Microsoft Corp, AOL, BT, InternetSecurity.com, DTI, eBay, Lucent Technology, InternetSecurity.org.uk, TEISME.com and Sky Broadband.

Many thanks to all the organisations that voluntarily participated in the survey questionnaire and the security managers/analysts who gave their time to be interviewed and participated in the case study observations.

The time spent in research and writing this book has been particularly difficult on my family. My absence, irritability and frustration to carry on have often reached uncharted personal heights. Tangential thanks go to my beauty queen and my angels for all their support, of which even the most carefully chosen words cannot adequately represent.

Finally, to the memory of my late parents, their energetic approach towards education cannot be ignored in my contribution to knowledge—education is a lifetime learning experience. And also to the memory of my late grannies, their ideology has greatly impacted what I live to believed that twenty years is not forever and the experience gain within that period remains for ever and an additional value added bonus to individual knowledge.