Synchronizing Internet Protocol Security (SIPSec)

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.

9 8 7 6 5 4 3 2 1

springer.com

DEDICATION

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF CONTRIBUTORS AND ORGANISATIONS

Alex Logvynovskiy	e-Centre for Infonomics, UK
Brendan Cotter	Kurt Geiger Ltd, UK
Sonny Nwankwo	University of East London, UK
Kasim Charhabagi	University of East London, UK
Harvey Freeman	Booze Allen Hamilton, USA
Charles Winer	Purdue University, Calumet, USA
Caterina Scoglio	Kansas State University, Kansas, USA
Victoria Repka	Kharkov National University of Radioelectronics, Ukraine
Maaruf Ali	Oxford Brooks University, UK
Vyacheslav Grebenyuk	Kharkov National University of Radioelectronics, Ukraine
Kia Makki	Florida International University, Miami, USA
Niki Passinou	Florida International University, Miami, USA
Siân Lambert	Manchester Metropolitan University, UK
Seamus Simpson	Manchester Metropolitan University, UK
Terry Cook	City University, USA.
Jen-Yao Chung	IBM Watson Research Centre, USA
Liang-Jie (LJ) Zhang	IBM Watson Research Centre, USA
Patrick Hung	University of Ontario, Institute of Technology, Canada
Dragana Martinovic	University of Windsor, Canada
Victor Ralevich	Sheridan Institute of Technology and Advance Learning, Canada
Pit Pichappan	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 architechture 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.