NETWORK SECURITY

An Introduction to Techniques & Standard

Kamaruzzaman Seman • Shaharudin Ismail • Waidah Ismail

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

NETWORK SECURITY

An Introduction to
Techniques & Standard

NETWORK SECURITY

An Introduction to Techniques & Standard

KAMARUZZAMAN SEMAN
SHAHARUDIN ISMAIL
WAIDAH ISMAIL

Penerbit USIM
UNIVERSITI SAINS ISLAM MALAYSIA
Bandar Baru Nilai
Negeri Sembilan
2007

Cetakan pertama 2007

Diterbitkan di Malaysia oleh
Penerbit USIM:
Universiti Sains Islam Malaysia,
Bandar Baru Nilai, 71800 Nilai,
Negeri Sembilan Darul Khusus
Tel : 06-798 8045 / Faks : 06-798 8054

Reka Letak & Urus Cetak:
AMPANG PRESS SDN. BHD.
6, Jalan 6/91, Taman Shamelin Perkasa
Batu 3½ Jalan Cheras
56100 Kuala Lumpur, MALAYSIA
Tel : 03-9284 9448 / Faks : 03-9284 9105
e-mel: ampress@streamyx.com

Perpustakaan Negara Malaysia Data Pengkatalogan-dalam-Penerbitan
Cataloguing-in-Publication Data

Kamaruzzaman Seman
Network security : an introduction to techniques and standard /
Kamaruzzaman Seman, Shaharudin Ismail, Waidah Ismail.
ISBN 978-983-2950-46-2
1. Computer networks--Security measures. 2. Computer security.
I. Shaharudin Ismail. II. Waidah Ismail. III. Title.
005.8

TABLE OF CONTENTS

PREFACE

The world has undergone a revolution in information and communication technology due to the increasing demands for information transmissions. The Internet has been the pinnacle to the worldwide interlocking communication network. The users such governments and private firms keep enormous amount of information on people, products, commodities, and processes. Clearly, the information needs to be protected from praying eyes.

However, despite the many good things promised by the Internet, it is completely vulnerable to various security threats such as eavesdropping, replay, modification, theft and many others. We have read many reports on the attacks conducted by adversaries to information kept in computers.

This books attempts to provide introductory materials to students as well as individuals who are interested to learn about network security. The discussion encompasses a broad scope of topics including threats, encryption, authentication, forensic, and security policies. Our noble objective when we prepared this book was to offer to audience not only the theoretical concepts, but it also covers the standard of practices in network security.

In the course of preparing this text book, every attempt has been made to make the contents and the facts presented as accurate as possible. However, we cannot give a one hundred percent guarantee to the correctness of facts and figures appeared here. Therefore, the authors or publisher shall not be responsible for whatever difficulties or accidents occurred in your organization as a result of adopting the methods or information given in this book.

AKNOWLEDGEMENTS

The authors are highly indebted to many individuals throughout the preparation of this book. Special thanks to the Dean of the Faculty of Science and Technology, Prof Dr Jalani Sukaimi for his strong support and encouragement, and to the management of Universiti Sains Islam Malaysia for their supportive policies on academic publication activities. Many thanks also to the editors for their constructive comments to make this book a success. Our gratitude also goes to colleagues who have contributed great ideas and suggestions. Finally, but not least to our families and parents who have been very patience and supportive to this costly ventures.

Authors:

Kamaruzzaman Seman
Shaharudin Ismail
Waidah Ismail

About the Authors

Kamaruzzaman Seman obtained B.E.Eng (Hons) from Universiti Teknologi Malaysia in 1985, MSc in Telematics from Essex University, UK in 1986, and PhD in Electrical Engineering (Broadband Comm.) from Strathclyde University, UK in 1994. He was a full professor in telecommunication at the Faculty of Electrical Engineering, Universiti Teknologi Malaysia from 2000-2003. From end of 2003 – to 2005 he was with Telekom Research and Development Sdn Bhd. The last post held was the Head of Applied Research Division. From Dec 2005 he has been a Professor at the Faculty of Science and Technology, Universiti Sains Islam Malaysia. He has taught many subjects in Telecommunication and Computer Engineering such as Telecommunication Switching, Data Communication, Principle of Communication Engineering, Stochastic Processes, and Digital Electronics. His research interests are telecommunication switching design, Protocols designs, network performance modeling, network security, network management, multimedia communications, and Next Generation Broadband Network Architecture. Currently his is a Senior Member of IEEE.

Shaharudin Ismail earned his Bachelor's Degree in Computer Science from University of Denver, Colorado, USA in 1994 and his Master's Degree in Information Technology (Computer Science) from Universiti Kebangsaan Malaysia (UKM) in 2005. Currently, he is a lecturer for Information Security and Assurance program in Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM). Prior to that, he worked as Policy Research Executive at National ICT Security and Response Centre (NISER). He was responsible in creating and managing strategic role initiatives for NISER. He is also actively carrying out research and analysis on ICT related matters especially in the field of information security.

Waidah Ismail is currently working as lecturer in Universiti Sains Islam Malaysia (USIM). She obtained her Master in Information

Technology from University Technology MARA, Shah Alam. Her first degree was in Computer Science from University of Liverpool, United Kingdom and Diploma in Computer Science in University Technology MARA, formerly known as MARA Institute of Technology. She was a security Analyst for three years at IT-365 Sdn Bhd prior to joining USIM. She has been working in the information technology industry for almost 8 years mainly in the Security environment in Banking Sector. She is well-versed in Operating System: Unix, Windows NT and Windows 2000 and for programming in Java Programming and VB.NET

About this Book

This book attempts to explain to readers the basic concept of network security in the simplest manner. The authors avoid using any complex jargon or terms which ordinary readers may find hard to digest. Nevertheless, the simplicity approach adopted here does not mean that we have sacrificed the technical correctness of the subject matter.

Chapter 2 explains the threats to the public computer network or to be more specific threats to the network security. This chapter will discuss the type of attacks including the passive attacks and also the active attacks. Chapter 2 ends with a discussion of the types of vulnerabilities.

Chapter 3 describes the various encryption algorithms that have been developed by researchers throughout the decades. The explanation divides the algorithms into two classes: stream ciphers and block ciphers.

Chapter 4 will not only explain how to prevent information or other access but also at the same time identify the authority of access to the system via audit log.

Today, computers provide a mission-critical information services for the modern corporation. The organization should be aware that the disaster comes in all shapes and sizes that will give impact to their businesses. One of the most important things to protect organization from disaster is to plan for any disaster, which will be the focus in Chapter 5.

Finally, Chapter 6 will briefly discuss some of the cyber laws in the United States and Malaysia. The British Standard 7799 (BS7799), ISO/IEC 17799 and ISO/IEC 27001 will conclude this book.

NETWORK SECURITY
AN INTRODUCTION TO TECHNIQUES & STANDARD

The world has undergone a revolution in information and communication technology due to the increasing demands for information transmissions. The Internet has been the pinnacle to the worldwide interlocking communication network. The users such governments and private firms keep enormous amount of information on people, products, commodities, and processes. Clearly, the information needs to be protected from praying eyes. However, despite the many good things promised by the Internet, it is completely vulnerable to various security threats such as eavesdropping, replay, modification, theft and many others. We have read many reports on the attacks conducted by adversaries to information kept in computers. Today, computers provide a mission-critical information services for the modern corporation. The organization should be aware that the disaster comes in all shapes and sizes that will give impact to their businesses. One of the most important things to protect organization from disaster is to plan for any disaster. This books attempts to provide introductory materials to students as well as individuals who are interested to learn about network security. The discussion encompasses a broad scope of topics including threats, encryption, authentication, forensic, and security policies. This book explains the threats to the public computer network or to be more specific threats to the network security, describes the various encryption algorithms that have been developed by researchers throughout the decades. The explanation of encryption algorithms are divided into two classes: stream ciphers and block ciphers. This book also explains how to prevent information or other access and identify the authority of access to the system via audit log. Some cyber laws in the United States and Malaysia, the British Standard 7799 (BS7799), ISO/IEC 17799 and ISO/IEC 27001 are also discussed. Our noble objective when we prepared this book was to offer to audience not only the theoretical concepts, but it also covers the standard of practices in network security.

ISBN 978-983-2950-46-2
9 789832 950462