

# Information Technology Security



PEARSON  
Prentice  
Hall

**Siti Rahayu Selamat  
Robiah Yusof  
Mohd Faizal Abdollah  
Nazrulazhar Bahaman**



SEM 1 - 2006/2007

# Information Technology Security

ROBIAH BT. YUSOF

Pensyarah

Fakulti Teknologi, Maklumat dan Komunikasi  
Kolej Universiti Teknikal Kejuruteraan Malaysia  
Karang Berkuang, 1200  
Ayer Keron, 70450 Melaka

Siti Rahayu Selamat  
Robiah Yusof  
Mohd Faizal Abdollah  
Nazrulazhar Bahaman

PEARSON  
Prentice  
Hall

## TABLE OF CONTENTS

### PREFACE

### CHAPTER 1 *INTRODUCTION TO INFORMATION SECURITY*

1.1 Introduction	1
1.2 Security Policy	2
1.3 Threats and Safeguards	4
1.4 Methods of Defense	8
1.5 Security Services	9
1.6 Security Mechanisms	13

### CHAPTER 2 *AUTHENTICATION AND BASIC CRYPTOGRAPHY*

2.1 Introduction to Authentication	23
2.2 Password	24
2.3 Introduction to Cryptography and Cryptography Algorithms	29
2.4 Methods of Cryptography Attacks	49

### CHAPTER 3 *PROGRAM SECURITY*

3.1 Secure Programs	66
3.2 Non-malicious Program Errors	67
3.3 Malicious Codes	69
3.4 Control Against Program Threats	76

### CHAPTER 4 *OPERATING SYSTEMS SECURITY*

4.1 Overview of Operating System Security	86
4.2 Security Methods of Operating System	89
4.3 Protection of Memory and Addressing	92
4.4 Protected Objects and Methods of Protection	99
4.5 Access Control vs. Capability	100



## **CHAPTER 5 DATABASE SECURITY**

5.1 Introduction	111
5.2 Security Requirements	116
5.3 Countermeasures: Computer-Based Controls	119
5.4 Countermeasures: Non Computer-Based Controls	123

## **CHAPTER 6 SECURITY IN NETWORKS**

6.1 Introduction to Network	127
6.2 Network Security	135
6.3 Network Security Threats	136
6.4 Network Security Controls	139
6.5 Firewall	150
6.6 Intrusion Detection Systems	152

## **CHAPTER 7 SECURITY IN APPLICATIONS**

7.1 Electronic Mail Security	161
7.2 Web Security	165
7.3 Security in Hypertext Transfer Protocol (HTTP)	170
7.4 Security in File Transfer Protocol (FTP)	174
7.5 Security in Network File System (NFS)	175
7.6 Security Using Biometric Technologies	180

## **CHAPTER 8 WIRELESS SECURITY**

8.1 Overview of Wireless Technology	191
8.2 Wireless Security Threats and Mitigation	193
8.3 Security of 802.11 Wireless LAN	195
8.4 Security of Bluetooth	205

CHAPTER 12 *DESIGNING, IMPLEMENTING AND  
MAINTAINING THE RECOVERY SOLUTIONS*

12.1	Designing the Backup and Recovery Solution	288
12.2	Selecting Products	310
12.3	Backup and Recovery Solution	314
12.4	Update Backup and Recovery Solution	327

REFERENCES	343
------------	-----

GLOSSARY	345
----------	-----

## PREFACE

### Overview

The greatest source of confusion in the business world today is information security. Executives read articles about the latest theft of credit cards or the billions of dollars in losses to hackers and expect that a quick solution can be found. The burden typically falls upon computer professionals who are otherwise brilliant at what they do but have little knowledge about security issues. This book is written based on our lecture notes for subject taught on three years undergraduate programme on information technology security. Each chapter is integrated with lab project that is designed to equipped student with hands-on experience on implementing the security techniques in their study environment which is based on various security issues. It also will expose the students on how to secure their rights, protecting their computing environment and preventing unauthorized people from reading and altering messages on a network. Any comments regarding this book are appreciated and you can email the comments to the authors: [srahs@yahoo.com](mailto:srahs@yahoo.com) or [robiah\\_mlk@yahoo.com](mailto:robiah_mlk@yahoo.com).

### Approach

The objective of this book is to introduce student in preparing a secure computing environment in theory and practical by using secure software, hardware and network. The task in the lab project will involve the managing setup process, PGP application, preventive tools, anti-virus and other security tools. These tools will help student in understanding and applying the computer and information security areas and processes. Each lab project offers student many opportunities to get hands-on and build new security tools skills. It also exposes students about threats that always attack their computing environment such as their information and network.

Upon completion of this theoretical and practical provided in this book, the students should have:

- Knowledge about threats and risk that are often attack the information and network.
- Substantial skills to use software or tools for managing the security of computing environment in general and IT security in particular.
- Skills on build the secure environment for any transaction in the network environment.

### Chapter Layout

Each chapter begins with a list of objectives. These include the important concepts to be mastered within the chapter. Extensive chapter reviews and self-review questions are included at the end of each chapter for self-study. They provide the student with a chance to build confidence with the exercises. This book contains 12 chapters which are Introduction to Information Security (Chapter 1), Authentication and Basic Cryptography (Chapters 2), Program Security (Chapter 3), Operating Systems Security (Chapter 4), Database Security (Chapter 5), Security in Networks (Chapter 6), Security in Applications (Chapter 7), Wireless Security (Chapter 8), Legal and Ethical Issues in Computer Security (Chapter 9), Cyberlaws (Chapter 10), Administering Security (Chapter 11) and Designing, Implementation and Maintaining the Recovery Solutions (Chapter 12).



# Information Technology Security

The objective of this book is to introduce student in preparing a secure computing environment in theory and practical by using secure software, hardware and network. The task in the lab project will involve the managing setup process, PGP application, preventive tools, anti-virus and other security tools. These tools will help student in understanding and applying the computer and information security areas and processes. Each lab project offers student many opportunities to get hands-on and build new security tools skills. It also exposes students about threats that always attack their computing environment such as their information and network.

Upon completion of this theoretical and practical provided in this book, the students should have:

- Knowledge about threats and risk that are often attack the information and network.
- Substantial skills to use software or tools for managing the security of computing environment in general and IT security in particular.
- Skills on build the secure environment for any transaction in the network environment.

