



# **BITS 3423**

## **INFORMATION TECHNOLOGY SECURITY**

Faculty of Information and Communications Technology

Siti Rahayu Selamat  
Robiah Yusof  
Mohd Faizal Abdollah  
Nazrulazhar Bahaman



**ROBIAH BT. YUSOF**  
Pensyarah  
Fakulti Teknologi Maklumat dan Komunikasi  
Kolej Universiti Teknikal Kebangsaan Malaysia  
Karung Berkunci 1200  
Ayer Keroh, 75450 Melaka

SEM1 2006/2007

3423  
BITS

# INFORMATION TECHNOLOGY SECURITY

Siti Rahayu Selamat  
Robiah Yusof  
Mohd Faizal Abdollah  
Nazrulazhar Bahaman

Editor  
Prof. Madya Dr. Shahrin Sahib@Sahibudin

Faculty of Information and Communication Technology,  
Kolej Universiti Teknikal Kebangsaan Malaysia,  
Karung Berkunci 1200,  
75450 Melaka,  
Malaysia.

© FTMK, KUTKM 2006

All rights reserved. No part of this publication may be reproduced stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without either the prior written permission of the publisher.

The programs in this book have been included for their instructional value. They have been tested with care but are not guaranteed for any particular purpose. The author or publisher does not offer any warranties or representations nor does it accept any liabilities with respect to the programs.



## TABLE OF CONTENTS

PREFACE.....	1
1 INTRODUCTION TO INFORMATION SECURITY	
Lab 1.1 Using NTFS to Secure Local Resources	
1.1.1 Introduction.....	2
1.1.2 Hands-On Exercise / Step by Step.....	2
1.1.3 Using NTFS to Secure Local Resources.....	2
1.1.4 Self-Review Questions.....	4
Lab 1.2 Data Confidentiality	
1.2.1 Introduction.....	5
1.2.2 Hands-On Exercise / Step by Step.....	5
1.2.3 Data Confidentiality.....	5
1.2.4 Self-Review Questions.....	8
Lab 1.3 Data Availability	
1.3.1 Introduction.....	9
1.3.2 Hands-On Exercise / Step by Step.....	9
1.3.3 Data Availability.....	9
1.3.4 Self-Review Questions.....	12
Lab 1.4 Data Integrity	
1.4.1 Introduction.....	13
1.4.2 Hands-On Exercise / Step by Step.....	13
1.4.3 Data Integrity.....	13
1.4.4 Self-Review Questions.....	15
2 AUTHENTICATION AND BASIC CRYPTOGRAPHY	
Lab 2.1 Data Encryption.	
2.1.1 Introduction.....	16
2.1.2 Hands-On Exercise / Step by Step.....	16
2.1.3 Data Encryption.....	16
2.1.4 Self-Review Questions.....	19
Lab 2.2 Using the Windows 2000 Local Password Policy Settings for Length	
2.2.1 Introduction.....	20
2.2.2 Hands-On Exercise / Step by Step.....	20
2.2.3 Using the Windows 2000 Local Password Policy Settings for Length.....	20
2.2.4 Self-Review Questions.....	23
Lab 2.3 Using the Windows 2000 Local Policy Settings for Complexity	
2.3.1 Introduction.....	24
2.3.2 Hands-On Exercise / Step by Step.....	24
2.3.3 Using the Windows 2000 Local Policy Settings for Complexity.....	24
2.3.4 Self-Review Questions.....	26
Lab 2.4 Setting an Account Lockout Policy	
2.4.1 Introduction.....	27
2.4.2 Hands-On Exercise / Step by Step.....	27
2.4.3 Setting an Account Lockout Policy.....	27
2.4.4 Self-Review Questions.....	31
Lab 2.5 Decryption and Encryption Using PGP	
2.5.1 Introduction.....	32

	2.5.2 Hands-On Exercise / Step by Step.....	32
	2.5.3 Decryption and Encryption Using PGP.....	32
	2.5.4 Self-Review Questions.....	34
..... 1	3 PROGRAM SECURITY	
	3.0 Introduction.....	35
	3.1 Hands-On Exercise / Step by Step.....	35
..... 2	3.2 Removing Trojan Horse From an Infected System.....	35
..... 2	3.3 Self-Review Questions.....	38
..... 2	4 OPERATING SYSTEM SECURITY	
..... 4	4.0 Introduction.....	41
	4.1 Hands-On Exercise / Step by Step.....	41
	4.2 Operating Systems Hardening.....	41
..... 5	5 DATABASE SECURITY	
..... 5	5.0 Introduction.....	47
..... 5	5.1 Hands-On Exercise / Step by Step.....	47
..... 8	5.2 Database Security .....	47
..... 9	6 SECURITY IN NETWORKS	
..... 9	6.0 Introduction.....	49
..... 12	6.1 Hands-On Exercise / Step by Step.....	49
	6.2 Using IPsec to secure FTP Transaction.....	49
..... 13	6.3 Self-Review Questions.....	54
..... 13	7 SECURITY IN APPLICATIONS	
..... 15	7.0 Introduction.....	55
	7.1 Hands-On Exercise / Step by Step.....	55
	7.2 Securing FTP Server.....	55
..... 16	7.3 Self-Review Questions.....	61
..... 16	8 WIRELESS SECURITY	
..... 16	8.0 Introduction.....	65
..... 19	8.1 Hands-On Exercise / Step by Step.....	67
..... 20	8.2 Wireless Security Setup Using Multi-Function 802.11g Wireless Router.....	69
..... 20	8.3 Self-Review Questions.....	81
..... 23	9 LEGAL AND ETHICAL ISSUES IN COMPUTER SECURITY	
..... 24	9.0 Introduction.....	84
..... 24	9.1 Hands-On Exercise / Step by Step.....	84
..... 24	9.2 Case 1: Rights of Employees and Employers.....	84
..... 26	9.3 Case 2: Authentication and Ownership.....	85
..... 27	10 CYBERLAWS	
..... 27	10.0 Introduction.....	86
..... 27	10.1 Hands-On Exercise / Step by Step.....	86
..... 31	10.2 Case 1: Censorship of the Internet.....	86
	10.3 Questions.....	87
..... 32	10.4 Resources About Censorship.....	88

11 ADMINISTERING SECURITY	
11.0 Introduction.....	89
11.1 Hands-On Exercise / Step by Step.....	90
11.2 Computer Hardware and Software Company.....	90
12 DESIGNING, IMPLEMENTATION AND MAINTAINING THE RECOVERY SOLUTIONS	
12.0 Introduction.....	93
12.1 Hands-On Exercise / Step by Step.....	93
12.2 Active Directory Backup and Restore.....	93
12.3 Self-Review Questions.....	98
TUTORIAL	99
REFERENCES	112



.....	89
.....	90
.....	90
<b>OVERVIEW</b>	
.....	93
.....	93
.....	93
.....	98
.....	99
.....	112

## 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 lab module 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.

### Approach

The objective of this module is to introduce student in preparing a secure computing environment by using secure software, hardware and network. The task 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 offers student many opportunities to get hands-on and build new security tools skills. The lab module also exposes students about the threats to their computing environment such as their information and network. Upon completion of this lab module the students should have:

- Substantial skills to use software or tools for managing the security of computing environment in general and IT security in particular.
- Knowledge about threats and risk that are threatening the information and network.
- Skill to build a 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 self-review questions and tutorial are included at the end of each chapter for self-study. They provide the student with a chance to build confidence with the lab exercises. This module 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).