



# Windows® 2000 Security

Suriname University of Technology



31051000647205

New  
Riders

Roberta Bragg

# Contents

## **Introduction xv**

Who This Book Is For xv

How This Book Is Organized xvi

Conventions Used in This Book xvii

## **I Concepts and Definitions 1**

### **1 Basic Security Concepts 3**

The Three A's of Security 4

Security Policy 9

Computer Security Objectives 9

Miscellaneous Security Terms 13

For More Information 14

Summary 15

### **2 Cryptology Introduction 17**

Historical Background 18

Today's Cryptographic Algorithms 20

Common Cryptographic Algorithms 27

Methods of Attack 33

For More Information 33

Summary 34

### **3 New Protocols, Products, and APIs 35**

Web-Related Protocols 37

Remote Access Protocols 40

IPSec 53

Secure Communication Between DHCP and Dynamic DNS 62

Microsoft-Specific APIs and Security Protocols 64

For More Information 68

Summary 69

## **4 Public Key Infrastructure (PKI) 71**

Certification Authority 72

Registration Authority 73

Certificates and Keys 74

Certificate Repository 76

Certificate Revocation List (CRL) 77

Certificate Trust Models 79

Clients and Client Software 86

PKI Procedures 86

For More Information 90

Summary 90

## **5 Kerberos in the RAW 91**

Kerberos Basics 93

Kerberos Components and Algorithms 95

Kerberos Trust Path 116

Encryptions and Checksums 119

For More Information 121

Summary 121

## **II Securing the OS 123**

### **6 Security from the Get-Go 125**

Users and Groups 126

Introduction to the Active Directory 131

Rights and Privileges 138

Windows 2000 NTFS 142

Default Registry Permissions 148

Soft Protection and Windows File Protection 151

The Windows 2000 Encrypting File System (EFS) 152

Best Practices 158

For More Information 159

Summary 159

<b>7</b>	<b>User Authentication</b>	<b>161</b>
	LM and NTLM Authentication	162
	Kerberos in Windows 2000	163
	The Big Picture: Network Logon	176
	Get Smart! Using Smart Cards with Windows 2000	179
	For More Information	186
	Summary	186
<b>8</b>	<b>Lifecycle Choices</b>	<b>187</b>
	Installation Do's and Don'ts for Improved Security	188
	Maintenance	192
	System Recovery: Repair Overview	203
	Death and Dismemberment	211
	Best Practices	212
	For More Information	212
	Summary	213
<b>9</b>	<b>Security Tools</b>	<b>215</b>
	Using the Security Configuration and Analysis Tool Set	216
	Group Policy	225
	Support Tools	230
	Resource Kit Tools	230
	Choosing the Tool to Use	248
	Best Practices	249
	For More Information	249
	Summary	249
<b>10</b>	<b>Securing Windows 2000 Professional</b>	<b>251</b>
	Setting Up and Securing the User and Group Database	252
	Windows 2000 Professional in a Windows NT 4.0 Domain	258
	Managing Local Security Settings with Group Policy	260
	Matching Security Settings to the Abilities of the User	271
	Policy Implementation and Enforcement	272
	Securing Wireless Connections	275
	Protocols and Processes for Secure Data and Application Access	277

<b>18</b>	<b>Interoperability</b>	<b>463</b>
	UNIX Interoperability	464
	PKI Interoperability	473
	Macintosh	477
	Novell	479
	IBM Mainframe and AS400	481
	Single Sign-On	482
	Directory Integration: The Case for Metadirectories	484
	Best Practices	485
	For More Information	486
	Summary	486
<b>19</b>	<b>Web Security</b>	<b>487</b>
	Securing Windows 2000 Server	489
	Securing the Web Site	493
	Tools	501
	Monitoring, Measuring, and Maintaining	509
	Best Practices	511
	For More Information	511
	Summary	512
<b>20</b>	<b>Case Study in Interbusiness Access: Distributed Partners</b>	<b>513</b>
	Business Model	514
	Network Infrastructure Security	516
	Active Directory Architecture Backbone	521
	Authentication and Authorization	523
	Public and Private Interface Processes	525
	Summary	526
	<b>Resources</b>	<b>527</b>
	Books	527
	Microsoft Site Information	528
	Other Web Sites	529
	White Papers	529
	<b>Index</b>	<b>531</b>