

# Contents at a Glance

---

*Introduction* *xxi*

---

## **Part I**      **Introduction to .NET Security**

---

<b>Chapter 1</b>	Understanding .NET Security	<b>3</b>
<b>Chapter 2</b>	.NET Framework Security Overview	<b>23</b>
<b>Chapter 3</b>	Avoiding Common Errors and Traps	<b>51</b>

---

## **Part II**      **Desktop and LAN Security**

---

<b>Chapter 4</b>	.NET Role-Based Security Techniques	<b>69</b>
<b>Chapter 5</b>	Policies and Code Groups in Detail	<b>107</b>
<b>Chapter 6</b>	Validation and Verification Issues	<b>147</b>
<b>Chapter 7</b>	.NET Cryptographic Techniques	<b>171</b>
<b>Chapter 8</b>	LAN Security Requirements	<b>203</b>

---

## **Part III**      **Web-based Security**

---

<b>Chapter 9</b>	Web Server Security	<b>233</b>
<b>Chapter 10</b>	Web Data Security	<b>263</b>
<b>Chapter 11</b>	Securing XML and Web Services	<b>299</b>

---

## **Part IV**      **Other Security Topics**

---

<b>Chapter 12</b>	Active Directory security	<b>337</b>
<b>Chapter 13</b>	Wireless Device Security	<b>363</b>
<b>Chapter 14</b>	Win32 API Overview	<b>389</b>
<b>Chapter 15</b>	Win32 API Advanced Techniques	<b>413</b>
<b>Glossary</b>		<b>439</b>

*Index* *455*

# Contents

---

*Introduction*

*xxi*

<b>Part I</b>	<b>Introduction to .NET Security</b>	<b>1</b>
<b>Chapter 1</b>	<b>Understanding .NET Security</b>	<b>3</b>
	An Overview of .NET Framework Enhancements	5
	Using Role-based Security	7
	Executing Code in the Managed Environment	9
	Security Problems .NET Can't Stop	11
	Stupid User Tricks	12
	Some External Forces	13
	Poorly Patched Systems	14
	Inept Enterprise Policies	15
	Windows File Protection Vulnerabilities	17
	.NET Framework Security Architecture Considerations	18
	Securing the Binary Output	18
	Understanding the Effects of Garbage Collection	18
	Considering the Requirements of Object-Oriented Programming	19
	Understanding Native Code Access Concerns	19
	Summary	21
<b>Chapter 2</b>	<b>.NET Framework Security Overview</b>	<b>23</b>
	Locating the Security Information You Need	24
	Dealing with Patches	25
	Locating General Security Tips for Everyone	26
	Finding .NET Framework Specific Security Tips	27
	Understanding the System.Runtime.Remoting.Contexts Namespace	28
	Contexts Namespace Overview	28
	SynchronizationAttribute Attribute Example	29

Understanding the System.Security Namespace	31
Security Namespace Overview	31
SecurityManager Class Example	32
Understanding the System.Security.Cryptography Namespace	35
Cryptography Namespace Structure Overview	36
Cryptography Namespace Structure Example	36
Understanding the System.Security.Permissions Namespace	39
Understanding the System.Security.Policy Namespace	39
Understanding the System.Security.Principal Namespace	40
Understanding the System.Web.Security Namespace	41
Understanding the System.DirectoryServices Namespace	41
DirectoryServices Namespace Overview	42
DirectoryServices Namespace Example	42
Summary	50
<b>Chapter 3</b>	
<b>Avoiding Common Errors and Traps</b>	<b>51</b>
Preventing Data Entry Errors	52
Putting the Time back into Access	53
Checking the Data Range	53
Checking the Data Length	55
Keeping Unnecessary Characters Controlled	57
Providing Precise Help	59
Stopping Buffer Overruns	60
Understanding How Buffer Overruns Work	60
Keeping Exploits Controlled	61
Controlling Access	61
Understanding Code Access Control Issues	61
Understanding User Access Control Issues	62
Setting Privileges Appropriately	62
Avoiding Canonical Representation Issues	63
Summary	64

---

<b>Part II</b>	<b>Desktop and LAN Security</b>	<b>67</b>
<b>Chapter 4</b>	<b>.NET Role-Based Security Techniques</b>	<b>69</b>
	Understanding How .NET Role-Based Security Differs	70
	Defining Code Access Security versus Role-based Security	71
	Defining Membership and Evidence	75
	Using Permission Objects	77
	Using Principal and Identity Objects	81
	Using the Permission View Tool	83
	Using the .NET Framework Configuration Tool	87
	Working with Code Groups	88
	Creating and Defining Permission Sets	90
	Defining Policy Assemblies	91
	Adding Configured Applications	92
	Defining Effective Declarative Security	92
	Defining Effective Imperative Security	93
	Securing the Registry	93
	Using the RegistryPermission Class	94
	A Word about Registry Security	97
	Developing a Secure Desktop Application Installation	98
	Using the StrongNameIdentityPermission Class	98
	Using the System.Reflection.Assembly.Evidence Property	103
	Summary	106
<b>Chapter 5</b>	<b>Policies and Code Groups in Detail</b>	<b>107</b>
	Using the Code Access Security Policy Tool	108
	Listing the Permissions and Code Groups	109
	Making Group Modifications	111
	Making Permission Modifications	113
	Adding an Assembly	116
	Resolving Security Errors in Assemblies	117
	Using the .NET Wizards	118

Using Code Groups	118	
Understanding the Default Groups	119	
Working with Code Groups	120	
Adding New Permissions	128	
Using Policy Objects	139	
Installing a New Permission	140	
Creating a Code Group Based on the Permission	142	
Designing a Named Permission Test Program	143	
Summary	145	
<b>Chapter 6</b>	<b>Validation and Verification Issues</b>	<b>147</b>
Ensuring Trust in the Managed Environment	148	
Validating Your Code	149	
Checking the Intermediate Language (IL) Code	150	
Validating the Standard Check	151	
Circumventing and Fixing the Standard Check	152	
Protecting Your Code with Dotfuscator	156	
Creating a Security Deployment Package	159	
Relying on the AppDomain for Managed Code	160	
Accessing Another Application	160	
Understanding Component Access Problems	163	
Extending the AppDomain to Unmanaged Code	164	
Working with External Functions	165	
Working with External Programs	167	
Summary	169	
<b>Chapter 7</b>	<b>.NET Cryptographic Techniques</b>	<b>171</b>
Administering the Cryptographic Settings	172	
Using the Certification Authority Utility	173	
Managing the Cryptographic Classes	179	
Understanding the Supported Cryptographic Methods	184	
Beware of the Cracked Symmetric Algorithm	185	
Learning about the Asymmetric Algorithm	186	

---

Encrypting and Decrypting Files	187	
Using Symmetric Cryptography	187	
Using Asymmetric Cryptography	189	
Deriving a Key from a Password	195	
Using the System.Security.Cryptography.X509Certificates Namespace	196	
Using Hash Functions	199	
Summary	200	
<b>Chapter 8</b>	<b>LAN Security Requirements</b>	<b>203</b>
<hr/>		
Working with Sockets	205	
Using the SocketPermission Class	205	
Using the Secure Socket Layer (SSL) Protocol	209	
Using the System.Net.NetworkCredential and System.Net.CredentialCache Classes	210	
Understanding RPC Security	212	
Working with DCOM	213	
Maintaining Control with COM Attributes	214	
Developing a Component with Attributes	216	
Creating a Test Application	217	
Developing a Secure Server Application Installation	220	
Working with COM+	220	
Creating a COM+ Component	221	
Working with the SecurityCallContext Class	223	
Adding Security to a COM+ Application	225	
Summary	229	
<b>Part III</b>	<b>Web-based Security</b>	<b>231</b>
<hr/>		
<b>Chapter 9</b>	<b>Web Server Security</b>	<b>233</b>
<hr/>		
Keeping the Server Safe	235	
Authentication Techniques	236	
Authorization Techniques	246	
Communication with Other Servers	249	

Administering the Server	249	
Using the Microsoft Baseline Security Analyzer	250	
Using the IIS Lockdown Tool	252	
Avoiding Distributed Denial of Service (DDOS) Attacks	253	
Don't Process Out-of-Band (OOB) Messages	254	
Using the Performance Counter Approach	254	
Overcoming Apparent Communication Errors	258	
Using Web-based Application Testing Techniques	259	
Developing a Secure Web-based Application Installation	260	
Summary	261	
<b>Chapter 10</b>	<b>Web Data Security</b>	<b>263</b>
Defining the Database Connection	264	
Securing the DBMS	265	
Developing a Database Application	267	
Stemming the Tide of Leaking Information	277	
Implementing Data Encryption	278	
Understanding Remoting and Data Encryption	279	
Understanding Automatic Deserialization	280	
Understanding Remoting and Code Access Security	281	
Creating a Remoting Component	283	
Creating a Remoting Host Application	286	
Creating a Remoting Client Application	288	
Using HttpChannel Security	293	
Using SSL to Communicate Credentials	294	
Adding SSL Support to a Server	294	
Creating an SSL Application	296	
Summary	298	
<b>Chapter 11</b>	<b>Securing XML and Web Services</b>	<b>299</b>
Securing Web Services	301	
XML and Security	302	

Web Service Proxy Security Considerations	303
Working with SoapHttpClientProtocol Class Security	305
Working with DiscoveryClientProtocol Class Security	308
Using the System.Security.Cryptography.Xml Namespace	312
Understanding the System.Security.Cryptography.Xml Namespace	313
Creating and Verifying XML Digital Signatures	314
Working with WS-Security	318
Working with the eXtensible Access Control Markup Language	320
Using the Visual Studio .NET Passport Features	321
Passport Features in the System.Web.Security Namespace	323
A Simple Passport Example	323
Using the Web Service Features of COM+ 1.5	325
Performing the Application Setup	326
Creating a Simple COM+ Test Application	328
Verifying the Application Is Safe	332
Summary	332

---

## **Part IV      Other Security Topics      335**

---

<b>Chapter 12</b>	<b>Active Directory Security</b>	<b>337</b>
	Monitoring Active Directory	338
	Using the ADSI Viewer Utility	339
	Other Active Directory Tools	342
	Using Active Directory in Place of the Registry	343
	Understanding Domain Trust Relationships	345
	Defining the Domain Trust Issues	345
	Working Directly with the Domain Controller	346
	Managing Directory Services	353
	Using Declarative Active Directory Security	353
	Using Imperative Active Directory Security	354
	Defining Write Access to Active Directory	357
	Summary	362

<b>Chapter 13</b>	<b>Wireless Device Security</b>	<b>363</b>
	.NET Compact Framework Security Considerations	365
	Understanding Wireless Security Issues	365
	Discovering Which Classes Apply to Both Environments	367
	Developing a Simple .NET Compact Framework Program	369
	The Two Environments of Wireless Programs	374
	Overcoming Direct Execution Problems	375
	Avoiding Browser-Based Application Issues	376
	Effects of Security Policy on Mobile Applications	380
	Component Calling Limitations	381
	Using the System.Web.Security Namespace	382
	Defining File Security Using the FileAuthorizationModule Class	383
	Defining Form Security Using the FormsAuthentication Class	384
	Summary	386
<b>Chapter 14</b>	<b>Win32 API Overview</b>	<b>389</b>
	Knowing When to Use the Win32 API	391
	Win32 API and .NET Framework Differences	391
	Avoiding Dangerous APIs	392
	Understanding the Windows Security API	395
	Considering Access Problems with the Win32 API	399
	Using the Run As Windows Feature	399
	Understanding Resources Both Granted and Denied	400
	Using the Access Control Editor	401
	Using the Security Configuration Editor	403
	Working with SIDs	405
	Accessing an ACE Directly	408
	Summary	411

---

<b>Chapter 15</b>	<b>Win32 API Advanced Techniques</b>	<b>413</b>
	Working with the DACL	414
	Working with the SACL	418
	Writing the Auditing Code	418
	Running the Application	423
	Considering a Security Setting Alternative	424
	Securing Controls and Components	425
	Securing Files	426
	Using the RegGetKeySecurity() and RegSetKeySecurity() Functions	429
	Working with Remote Unmanaged Components	432
	Setting Up the General DCOM Environment	432
	Using the General DCOM Security Options	434
	Working with Component Level Security	435
	Setting the Authentication Level	436
	Summary	437
<b>Glossary</b>		<b>439</b>
	<i>Index</i>	455