

.NET Security

Table of Contents

INTRODUCTION	INTRO-1
Prerequisites	INTRO-2
Courseware Conventions	INTRO-3
Installing the Practice Files	INTRO-4
Software Requirements	INTRO-4
Installation	INTRO-4
About the Authors	INTRO-5
OVERVIEW OF SECURITY IN .NET	1-1
Security as a System	1-2
Security as an Afterthought.....	1-2
The Problem with COM.....	1-2
Security in .NET	1-4
The Common Language Runtime (CLR)	1-5
Managed and Unmanaged Code	1-5
Code Access Security Concepts.....	1-6
Assemblies.....	1-9
Designing Secure Systems.....	1-23
Evaluating Risks	1-23
Design Guidelines.....	1-25
The Ten Immutable Laws of Security	1-27
SECURITY ADMINISTRATION.....	2-1
Security Policy in the CLR	2-2
Policy Levels	2-2
Configuring Policy	2-5
Evidence	2-13
Working with Command Line Tools	2-18
Locating Caspol	2-18
Using Caspol.....	2-19
Creating Scripts	2-22
Additional Framework Security Tools	2-24
Other Security Tools	2-25
Microsoft	2-25
LAB 2: SECURITY ADMINISTRATION.....	2-31

Lab 2 Overview	2-32
Use the .NET Framework Configuration Tool	2-33
Use Caspol	2-37
CREATING SECURE ASSEMBLIES	3-1
Assembly Overview	3-2
Resolving Namespace Conflicts	3-2
Digital Signing	3-3
Signing an Assembly	3-6
Delayed Signing	3-10
Exception Handling	3-13
Fail to a Secure Mode	3-13
The Exception Class	3-13
The Try/Catch Block	3-14
Unhandled Exceptions	3-15
Using the Exception Object	3-17
The SecurityException Class	3-19
Creating Conditional Messages	3-21
Writing to the Windows Event Log	3-26
Redirecting Users in ASP.NET	3-28
Exception Handling Caveats	3-30
Protecting Source Code	3-31
Available Options	3-31
Coding Best Practices	3-33
Assume Attack	3-33
LAB 3: CREATING SECURE ASSEMBLIES	3-39
Lab 3 Overview	3-40
Write to the Windows Event Log	3-41
Strong Name an Assembly	3-45
DIGGING INTO CODE ACCESS SECURITY	4-1
Permission Requests	4-2
Requesting Minimum Permissions	4-3
Requesting Optional Permissions	4-10
Refusing Permissions	4-13
Requesting Permission Sets	4-15
Imperative Permissions	4-18
Choosing a Permissions Technique	4-20
Determining Effective Permissions	4-22

Code Groups and Evidence.....	4-22
Using the Permissions View Tool	4-29
Work with Permission Sets	4-29
Permissions Across Levels	4-31
The Stack Walk.....	4-36
LAB 4: DIGGING INTO CODE ACCESS SECURITY	4-41
Lab 4 Overview.....	4-42
Configure Permissions for an Assembly.....	4-43
Create an Assembly that Uses Imperative Permissions.....	4-47
UNDERSTANDING AND USING WINDOWS SECURITY	5-1
Windows Security Basics.....	5-2
Access Tokens.....	5-2
Securable Objects.....	5-4
Access Control Entries (ACEs)	5-5
Access Rights	5-9
Discretionary Access Control Lists (DACLS).....	5-11
Determining User Rights.....	5-12
DACLS and .NET	5-16
DACLS and the GAC.....	5-16
DACLS and .NET Security	5-16
Managing DACLS with the WMI Classes	5-17
LAB 5: UNDERSTANDING AND USING WINDOWS SECURITY	5-25
Lab 5 Overview.....	5-26
Use DACLS to Control Access to a File.....	5-27
Use WMI to Copy the DACL from One File to Another.....	5-31
ROLE-BASED SECURITY FOR WINDOWS APPLICATIONS	6-1
Role-Based Security Overview	6-2
Authentication	6-2
Identity	6-2
Authorization	6-2
Principal	6-4
.NET Security Classes.....	6-5
The System.Security.Principal Namespace.....	6-5
Implementing Application Security.....	6-11
Enabling Controls.....	6-11
Imperative Role-Based Security	6-12

Declarative Role-Based Security	6-17
Combining Windows and Generic Role-Based Security	6-18
LAB 6: ROLE-BASED SECURITY FOR WINDOWS APPLICATIONS	6-27
Lab 6 Overview	6-28
Enable Controls Based on Role Membership	6-29
Protect Code with Role Checks	6-32
ISOLATED STORAGE	7-1
Understanding Isolated Storage	7-2
Overview of Isolated Storage	7-2
Uses for Isolated Storage	7-3
Isolated Storage Pitfalls	7-3
Mechanics of Isolated Storage	7-5
Obtaining a Store	7-5
Creating a Directory	7-6
Creating a File	7-6
Writing to a File	7-8
Reading from a File	7-9
Deleting a File or Directory	7-10
Storing Settings	7-11
Types of Isolation	7-17
Isolation by User and Assembly	7-17
Isolation by User, Assembly, and AppDomain	7-18
Using the GetStore Method	7-18
Roaming and Isolated Storage	7-19
Administering Isolated Storage	7-20
Using the Isolated Storage Tool	7-20
Setting Permissions for Isolated Storage	7-21
Allowed Usage and Security Risks	7-22
LAB 7: ISOLATED STORAGE	7-27
Lab 7 Overview	7-28
Save Log File Information on a Per-User Basis	7-29
Persist Form Size and Location Settings	7-32
SECURING SQL SERVER DATA	8-1
Installing SQL Server	8-2
SQL Server Setup	8-2
Installing the Desktop Engine (MSDE)	8-5

SQL Server in Visual Studio .NET	8-6
Server Explorer	8-6
Database Project	8-7
SQL Server Security Architecture	8-10
Authentication	8-10
SQL Server Roles	8-17
Creating Database Roles	8-21
Ownership and the dbo Account	8-22
Authorization and Permissions	8-24
The Permissions Statements	8-25
Understanding Ownership Chains	8-27
Guarding Against SQL Injection Attacks	8-28
Row-Level Permissions	8-29
Scripting Permissions	8-34
LAB 8: SECURING SQL SERVER DATA	8-41
Lab 8 Overview	8-42
Create SQL Server Logins	8-43
Script Permissions	8-47
INDEX	INDEX-1

.NET Security

Table of Contents

INTRODUCTION	INTRO-1
Prerequisites	INTRO-2
Courseware Conventions	INTRO-3
Installing the Practice Files	INTRO-4
Software Requirements	INTRO-4
Installation	INTRO-4
About the Authors	INTRO-5
ASP.NET SECURITY	9-1
ASP.NET Security Overview	9-2
IIS and ASP.NET Security	9-2
ASP.NET Authentication	9-2
Configuring ASP.NET Settings	9-4
Authorization	9-7
Configuring IIS Settings	9-8
Understanding ASP.NET Process Identity	9-12
Windows Authentication	9-15
Configuring Security in Web.config	9-15
Forms Authentication	9-21
Configuring Form-Based Security	9-21
Hashing Passwords	9-28
Using an XML File to Store User and Password Values	9-31
Custom Authentication	9-34
Storing Secrets Safely	9-34
Creating the SQL Server Objects	9-35
Coding the ASP.NET Application	9-36
Activating Custom Authentication	9-43
LAB 9: ASP.NET SECURITY	9-53
Lab 9 Overview	9-54
Configure Forms Authentication	9-55
Authenticate Users	9-58
ENTERPRISE SERVICES	10-1
Enterprise Services Overview	10-2
Overview of COM+	10-2

COM+ Security Concepts	10-6
Creating Serviced Components.....	10-9
The ServicedComponent Class	10-9
The Sample Application	10-10
Installing the Sample Application in COM+	10-15
Administering COM+ Security	10-18
Configuring Default Security Settings in COM+	10-18
Configuring Security for the COM+ Application	10-20
Testing the Inventory Application.....	10-32
The Sample Client Project	10-32
Programmatic Security.....	10-37
LAB 10: ENTERPRISE SERVICES.....	10-45
Lab 10 Overview	10-46
Install in COM+	10-47
Configure the Client Application	10-52
SECURITY FOR .NET REMOTING	11-1
.NET Remoting Overview	11-2
Remoting Features	11-2
Examining a Remoting Application	11-3
Hosting Remoting in ASP.NET	11-10
Choosing a Remoting Host	11-10
IIS Hosting	11-11
Creating the Client	11-14
Secure Remoting with IIS and ASP.NET	11-16
Authentication with the User's Credentials	11-16
Authentication with Specific Credentials	11-19
Authorization with the Web.config File	11-21
Authorization with Principal Permission Demands.....	11-24
LAB 11: SECURITY FOR .NET REMOTING	11-29
Lab 11 Overview	11-30
Create a Remoting Server and Client.....	11-31
Use IIS and ASP.NET to Secure the Remote Object	11-37
WEB SERVICES	12-1
Web Services Overview.....	12-2
Web Services Features.....	12-2
Examining a Web Service Application	12-2

Building the Web Service Client.....	12-5
The Proxy Class.....	12-8
Disabling Unwanted Protocols.....	12-10
Disabling GET and POST	12-10
Disabling WSDL.....	12-14
Secure Web Services with IIS and ASP.NET	12-16
Authentication with the User’s Credentials	12-16
Authentication with Specific Credentials	12-19
Authorization with the Web.config File.....	12-21
Authorization with Principal Permission Demands.....	12-22
LAB 12: WEB SERVICES	12-29
Lab 12 Overview.....	12-30
Build and Test a Web Service	12-31
Secure the Web Service	12-35
DEPLOYMENT.....	13-1
Deploying Security Policy	13-2
Creating Security Policy Packages.....	13-2
Double-Click Deployment	13-4
Enterprise Deployment	13-5
Scripting Security Policy Deployment	13-7
No-Touch Deployment.....	13-8
How No-Touch Deployment Works.....	13-8
The RichClient Sample Application.....	13-8
.NET Deployment Options	13-14
Private Assemblies	13-14
Shared Assemblies	13-16
The Global Assembly Cache	13-17
Deploying with Visual Studio .NET	13-19
Creating Setup Projects.....	13-20
Customize the Setup Project	13-25
Other Editors.....	13-27
Finalize the Setup Project	13-30
Test the Install.....	13-31
Deploying ASP.NET Applications	13-34
Deployment.....	13-34
Create a Web Setup Project	13-35
LAB 13: DEPLOYMENT	13-43

Lab 13 Overview	13-44
Create a Merge Module	13-45
Create a Setup Project	13-48
CRYPTOGRAPHY IN .NET.....	14-1
Basic Cryptographic Concepts	14-2
Symmetric Cryptography	14-2
Asymmetric Cryptography.....	14-4
Using Symmetric and Asymmetric Cryptography Together	14-5
Working with Data.....	14-6
Using Symmetric Encryption.....	14-6
Symmetric Decryption.....	14-10
Using Asymmetric Cryptography	14-13
Generating a Key Pair.....	14-13
Encrypting a Message with the Public Key	14-15
Decrypting a Message with the Private Key	14-17
Hash Codes	14-20
How Hashing Works	14-20
Calculating a Hash.....	14-20
Verifying a Hash.....	14-22
Digital Signatures.....	14-25
Generating a Signature.....	14-25
Verifying a Signature.....	14-27
Creating Random Keys.....	14-31
Supporting Web Farms	14-31
Generating Random Values.....	14-32
LAB 14: CRYPTOGRAPHY IN .NET	14-39
Lab 14 Overview.....	14-40
Generate and Publicize a Public Key	14-41
Initiate a Secure Conversation.....	14-44
HANDLING COMMON THREATS	15-1
Thinking about Security	15-2
Buffer Overflows	15-3
Anatomy of a Buffer Overflow	15-3
Configuring the Sample Application.....	15-4
How .NET Guards Against Buffer Overflows	15-5
The Dangers of Unmanaged Code	15-7
SQL Injection	15-10

How SQL Injection Works	15-10
Other SQL Injection Possibilities.....	15-13
Guarding Against SQL Injection.....	15-14
Cross-Site Scripting	15-18
Understanding Cross-Site Scripting.....	15-18
Guarding Against Cross-Site Scripting	15-22
Keeping Current.....	15-25
BugTraq and NTBugTraq.....	15-25
SANS Institute.....	15-25
Microsoft Web Sites	15-25
Software Update Services	15-26
The Human Element.....	15-27
What Makes a Good Hacker?	15-27
How Good Hackers Operate	15-27
Preventing Attacks	15-28
INDEX.....	INDEX-1

