Secure Development in .Net

Course Number 4028 – 40 Hours

Overview

.NET revolutionizes application security by providing the framework for developing secure Windows and Web applications. This course teaches you the basic concepts underlying Code Access Security, role-based security, and how to implement security in your applications to protect your code and your users against attack.
In this course, you'll learn about the security features in .NET. You'll gain an understanding of the new security architecture in the .NET Framework, and about Code Access Security in the Common Language Runtime. You'll explore how to administer security policy using visual and command-line tools. You also learn how to write script to implement security

On Completion, Delegates will be able to

- Administer security policy
- Create and digitally sign assemblies
- Validate data and handle errors safely
- Choose the right permission set for your code
- Manage Windows security
- Use Windows role-based security in your applications
- Work with Isolated Storage
- Secure your ASP.NET applications effectively
- Implement ASP.NET security using SQL Server
- Implement COM+ security with Serviced Components
- Secure Remoting with IIS and ASP.NET
- Create secure Web Services
- Deploy security policy and secure applications
- Understand Cryptography in .NET
- Handle common threats like buffer overflows, SQL injection and cross-site scripting

Who Should Attend

C# and .NET developers who wish to get up and running on developing well defended .NET applications.

Prerequisites

- Experience with C# and .NET programming

JOHN BRYCE
Leading in IT Education
a matrix company

matrix

Course Contents

Module 1: Overview of Security in .NET
- Security as a System
- Security in .NET
- Designing Secure Systems

Module 2: Security Administration
- Security Policy in the CLR
- Configuring Policy
- Working with Command Line Tools
- Other Security Tools

Module 3: Creating Secure Assemblies
- Assembly Overview
- Exception Handling
- Protecting Source Code
- Coding Best Practices

Module 4: Digging into Code Access Security
- Permission Requests
- Permission Requests (continued)
- Determining Effective Permissions

Module 5: Understanding and Using Windows Security
- Windows Security Basics
- DACLs and .NET

Module 6: Role-Based Security for Windows Applications
- Role-Based Security Overview
- .NET Security Classes
- Implementing Application Security

Module 7: Isolated Storage
- Understanding Isolated Storage
- Mechanics of Isolated Storage
- Types of Isolation
- Administering Isolated Storage

Module 8: Securing SQL Server Data
- Installing SQL Server
- SQL Server in Visual Studio .NET
- SQL Server Security Architecture

Module 9: ASP.NET Security
- ASP.NET Security Overview
- Windows Authentication
- Forms Authentication
- Custom Authentication

Module 10: Enterprise Services
- Enterprise Services Overview
- Creating Serviced Components
- Administering COM+ Security
- Testing the Inventory Application

Module 11: Security for .NET Remoting
- .NET Remoting Overview
- Hosting Remoting in ASP.NET
- Secure Remoting with IIS and ASP.NET

Module 12: Web Services
- Web Services Overview
- Disabling Unwanted Protocols
- Secure Web Services with IIS and ASP.NET

Module 13: Deployment
- Deploying Security Policy
- No-Touch Deployment
- .NET Deployment Options
- Deploying ASP.NET Applications

Module 14: Cryptography in .NET
- Basic Cryptographic Concepts
- Working with Data
- Using Asymmetric Cryptography
- Hash Codes
- Digital Signatures
- Creating Random Keys

Module 15: Handling Common Threats
- Thinking about Security
- Buffer Overflows
- SQL Injection
- Cross-Site Scripting
- Keeping Current
- The Human Element