

.NET Security and Cryptography Using C#

Course No.

9414

Description

This five-day course for C# programmers provides practical and comprehensive coverage of implementing security and cryptography on .NET platforms, including security in ASP.NET Web Forms and Web services applications.

The course begins with an examination of the need for security and cryptographic, including a discussion of the fundamental role of cryptography as the underpinnings of all security mechanisms. An overview is presented of security and cryptography in the .NET Framework.

Next, cryptography using .NET is studied in detail. The fundamental concepts of cryptography are covered, including keys, pseudorandom number generation, hash algorithms and cryptanalytic attacks. Symmetric cryptography is covered. The problems with symmetric algorithms are discussed, and the basic concepts and programming of asymmetric cryptography is covered. Programming RSA with the .NET Framework is covered. The use of digital signatures in .NET is discussed in detail, including programming with DSA. This section of the course concludes with a chapter on XML cryptography, including XML encryption and XML signing.

The next section of the course covers .NET security, beginning with a discussion of the fundamentals of .NET Security that are common to both role-based (or user-based) and code access security (CAS). Role-based security is covered in detail. Principal permissions and the various identity classes are discussed. Code examples are presented using both imperative and declarative security. Code access security is covered, including the fundamental support provided by managed code and the CLR. There is a discussion of code groups, permission sets and evidence-based security. Both imperative and declarative CAS are covered.

The course concludes with a detailed discussion of security in ASP.NET Web Forms and Web services. The last chapter includes an introduction to some of the new security specifications.

The course is based on the book .NET Security and Cryptography by Peter Thorsteinson and G. Gnana Arun Ganesh, published by Prentice Hall this book is recommended as a supplement to the course.

Audience

Although the course is geared for programmers, it does explore some aspects of administration as it directly relates to the tasks of .NET security programming. Every programmer must have some administrative skills to be effective software developers, and this is especially true of security programming.

Prerequisites

A basic knowledge of programming the .NET Framework using C#. The last two chapters require a knowledge of ASP.NET and Web services.

Objectives

- Develop a solid basis in the theory of cryptography so you can understand how the security tools in the .NET Framework function
- Learn to use symmetric algorithms, asymmetric algorithms, and digital signatures
- Master both traditional encryption programming as well as the new techniques of XML encryption and digital signatures
- Gain a thorough understanding of the security model in the .NET Framework
- Implement role-based and code access security using the .NET Framework
- Learn how these tools and techniques apply to ASP.NET and Web services security

System Requirements

Course exercises require Microsoft Visual Studio .NET 2003 on Windows 2000 or XP. Internet Information Services should be installed. See the appropriate course Setup Guide for details.

A good minimal hardware profile for this course would have a Pentium 500-MHz or equivalent CPU, 256 MB of RAM, and at least 2 GB of free disk space for tools installation and courseware.

Duration

5 days

Course Contents

1. Introduction to .NET Cryptography and Security

- Why Cryptography and Security
- What Cryptography Can and Cannot Do
- Security in Windows
- Security in .NET and the CLR
- .NET Cryptography Programming
- .NET Security Programming.

2. Fundamentals of Cryptography

- Cryptographic Terminology
- Secret Keys vs. Secret Algorithms
- Brute-Force Attacks
- Symmetric Cryptography
- Asymmetric Cryptography
- Pseudorandom Number Generators
- Cryptographic Hash Algorithms
- Cryptanalytic Attacks
- Human Interaction and Trust

3. Symmetric Cryptography

- Symmetric Ciphers
- DES and Triple DES
- System.Security.Cryptography Namespace
- Symmetric Algorithm Class
- Cryptographic Streams
- Key Exchange Issues

4. Asymmetric Cryptography

- Problems with Symmetric Algorithms
- Private and Public Keys
- RSA
- Programming RSA with .NET Framework
- Saving Keys as XML
- Digital Certificates

5. Digital Signatures

- .NET Hash Algorithms
- MD5 and SHA Classes
- Digital Signing
- RSA Use in Digital Signing
- Digital Signature Algorithms

- Programming with DSA
- XML Cryptography
- XML Encryption
- Implementing XML Encryption Using .NET
- XML Signatures
- .NET Framework Support for XML Signatures

6. .NET Security Fundamentals

- Authentication and Authorization
- .NET Security Model
- Administering Windows Security
- Users and Roles
- Permissions
- User-Based Security
- Code Access Security

7. NET Role-Based Security

- Principal Permissions
- Generic Identity
- Windows Identity
- Forms Identity
- Passport Identity
- Imperative Role-Based Security
- Declarative Role-Based Security
- Credentials

8. .NET Code Access Security

- Need for Code Access Security (CAS)
- Security, Managed Code, and the CLR
- Luring Attack and Stack Walking
- Code Groups
- .NET Framework Configuration Tool
- Permission Sets
- Evidence-Based Security
- Imperative CAS
- Declarative CAS

9. ASP.NET Security

- Authentication, Authorization and Impersonation
- ASP.NET Configuration
- Credentials
- Forms Authentication
- Passport Authentication
- Windows Authentication
- ASP.NET Authorization
- ASP.NET Impersonation

10. Web Services Security

- Firewalls, SSL and VPNs
- HTTP Authentication
- Web Service Authentication Using SOAP Headers
- XML Signatures in Web Services
- XML Key Management
- Security Assertion Markup Language (SAML)
- Global XML Web Services Architecture (GXA)
- WS-Security
- Microsoft Web Services Enhancements (WSE)

About Keane

Keane partners with businesses and government agencies to *optimize* IT investments by delivering exceptional evolution, operation, and maintenance of mission-critical systems and business processes. A US company with a large offshore capability, Keane combines local knowledge and local senior leadership with scalable global delivery that results in low-risk, actionable, cost-effective services and solutions – and a partnership that feels like an extension of your organization.

In business since 1965, Keane is an agile, full-service IT services firm headquartered in the United States with approximately 12,000 employees globally. For more information on Keane's services, solutions, products, and locations, please visit www.keane.com.