

## Internet Security Fundamentals

### Course Length

1 Day

### Course Outline

#### *Introduction*

Historical Perspective  
Threats  
Building Blocks

#### *Algorithms*

Ciphers: DES, RC4, AES, RSA, ECC  
Authentication  
Digital Signatures: DSS  
Message Digests: MD5, SHA-1, SHA-N  
Public-Key Infrastructure and its Limitations  
Key Exchange and Management  
Random Number Generation  
Certificates (X.509)

#### *Secure Transport*

Architecture, Handshaking and Messaging  
SSL/TLS  
IPsec  
Kerberos  
SSH  
Designing a System

#### *Web Security*

Architecture, Handshaking and Messaging  
HTTP  
Authentication Schemes  
Proxy Servers  
Designing a System

#### *Secure Content*

Architecture and Scope  
Digital Enveloping  
XML Security  
S/MIME  
Designing a System

#### *802.11*

Architecture, Handshaking and Messaging  
Known Security Problems  
Designing a System

#### *Conclusion*

### Course Summary

This comprehensive seminar will lead attendees through the architecture and design process for developing a secure Internet solution. The seminar will cover the basics of secure Internet communication schemes, including the building blocks of encryption, authentication, and message integrity. Popular networking protocols such as SSL, IPsec, and others, will be examined to understand how their use affects system architecture.

### Who Should Attend

System engineers, software architects, software engineers, test engineers, technical managers, project managers and marketing managers who want to design secure communication schemes for Internet-enabled products.

### Prerequisites

Some experience with communications software development, such as sockets programming, is helpful but not required.

### Benefits

After attending this workshop, attendees will be able to:

- Begin the process of designing a secure Internet solution
- Distinguish the attributes of different security algorithms
- Identify the known risks that must be protected against
- Distinguish different security protocols and their applications
- Understand the architectural implications of security design choices
- Make an informed decision between securing the transport or the data