Course Outline

Security Concepts for Software Developers (What Every Programmer Needs to Know)

Course Summary

Description

The first course of this curriculum is designed to expose software developers to the key security concepts that they need to know to appreciate what Secure Coding is all about. This is a language agnostic course that focuses on the concepts, techniques and mechanisms required to secure data and to create secure software that enforces and maintains data protection. Most developers are aware of some of these concepts, but they do not fully appreciate the significance of each in relation to the other, and how these topics ultimately affect their ability to evaluate and implement secure coding practices. Any factors that affect software security should be carefully considered, and fully understood. There is a lot of decision making that goes into each coding project, and this course helps ensure that developers are adequately equipped to make properly informed choices.

This course focuses on the main concepts, and leaves the implementation to later courses. It explores the foundations of security, and covers what every programmer needs to know about security.

Objectives

At the completion of this course, Students will be able to:

- Learn software security design principles and how to apply them
- Understand the importance of Defense-in-Depth
- Learn to create manageable security policies that you can actually implement
- Learn how to protect electronic data and software systems
- Apply common design patterns and best practices
- Understand how to correctly use Certificates, Authentication, Authorization and Encryption
- Learn how Cryptography can be used to protect your data
- Expose developers to common threats, so they can implement defenses to help avoid them
- Appreciate the necessity of a secure infrastructure and culture

Topics

- Security Design Principles
- Security Principles
- Authentication
- Authorization
- Protecting Data
- Encryption
- Cryptography
- Certificates
- Security Policies
- Operational Security
- Understanding Threats
- Common Attack Vectors

Prerequisites

Experience with at least one programming language is a prerequisite for this course.

Duration

Four Days

Course Outline

Security Concepts for Software Developers (What Every Programmer Needs to Know)

Course Outline

I. *Security Design Principles*
A. Security Goals
B. Secure Systems Design
C. Secure Design Principles
D. Evaluating the Landscape
E. Incentive

II. *Security Principles*
A. Defense-in-Depth
B. Diversity-in-Defense
C. Securing the Weakest Link
D. Fail-Safe Stance
E. Secure by Default
F. Simplicity
G. Usability
H. Security Features Do Not Imply Security

III. *Authentication*
A. Something You Know
B. Something You Have
C. Something You Are
D. Pulling it all together

IV. *Authorization*
A. Access Control Lists (ACLs)
B. Access Control Models
C. The Bell-LaPadula Model

V. *Protecting Data*
A. Confidentiality
B. Message Integrity
C. Data Integrity
D. Accountability
E. Availability
F. Non-Repudiation

VI. *Encryption*
A. Encryption Systems
B. Cost of encryption
C. Key Based Encryption Systems
D. Symmetric Keys
E. Public Keys
F. Encryption Algorithms
G. Analyzing popular encryption schemes
H. Symmetric vs. Asymmetric Encryption
I. Hashing Algorithms

VII. *Cryptography*
A. History of Cryptography
B. Math and Algorithms
C. Message Authentication
D. DES for Encryption
E. DES ECB and CBC Analysis
F. 3DES
G. HMAC/MD5 and SHA for Authentication
H. Strength (e.g., complexity, secrecy, characteristics of the key)
I. Cryptovariable or key

VIII. *Certificates*
A. Digital Certificates
B. Paper Certificates and Identity Cards
C. Authorities that Issue Physical Certificates
D. Difference Between Physical and Digital Certificates
E. Standards For Digital Certificates
F. X.509 as Authentication Standard
G. Public Key Certificate
H. Viewing digital certificates

IX. *Security Policies*
A. Concept of Security Policy
B. Key Security Elements
C. Security Awareness Programs
D. Vital role of a security policy
E. Classification of Security policy
F. User policies
G. IT policies
H. General Policies
I. Partner Policies
J. Types of Security Policies: Issues Specific Policies
K. Contents of Security Policy
L. Security levels
M. Agency Specific AIS and Telecommunications Policies
N. Configuration of security policy
O. National Policy and Guidance
P. Implementation of security policy
Q. Incident Handling and Escalation Procedures

Security Concepts for Software Developers (What Every Programmer Needs to Know)

Course Outline (Cont.)

R. Security operations and life cycle management
S. Securing Assets

X. *Operational Security*

A. Configuration Management
B. Defining Responses to Security Violations
C. Compliance with Law and Policy
D. Intellectual Property
E. Electronic Communications Privacy Act
F. Transborder encryption issues
G. Issue-specific Security Policy (ISSP)
H. E-mail Security Policies

XI. *Understanding Threats*

A. Defacement
B. Infiltration
C. Phishing
D. Pharming
E. Insider Threats
F. Click Fraud
G. Denial of Service (DOS)
H. Data Theft and Data Loss
I. "Good Enough" Security

XII. *Common Attack Vectors*

A. Worms and other Malware
B. Buffer Overflows
C. Client-State Manipulation
D. SQL Injection
E. Password Security
F. Cross-Domain Security in Web Applications