Certified Information Systems Security Professional, Part 6 of 9: Security Architecture and Apps

Meet the expert: Kevin is an international author, consultant and international >speaker. He is the official course development writer for ISC2 CISSP, ISACA CRISC

and mile2’s C)ISSO. Kevin has been educating IT professionals for over 30 years. He

also provides cyber security consulting and support services for organizations

around the world. Assisting them with setting up Information Security programs and

addressing areas ranging from in-depth risk analysis to policy creation and security

awareness.

Prerequisites: This series assumes a good understanding of enterprise networking and networking security. This is part 6 of a 9 part series.

Runtime: 02:06:58

Course description: This course discusses security architecture and models. It starts with the common concerns about security within software, risk management and how it integrates. Next, web applications, compliance with standards and investigate database security issues. Finally the role of artificial intelligence and knowledge discovery, software development models and change control processes. This course is part of a series covering the ISC(2) Certified Information Systems Security Professional (CISSP).

Course outline:

Security Architecture
- Introduction
- ESA Definition
- What Is Architecture?
- Architecture Components
- Objectives of Security Architecture
- Technology Domain Modeling
- Integrated Security is Designed Security
- Security by Design
- Summary

Architectural Models
- Introduction
- Architectural Models
- Virtual Machines
- Cloud Computing
- Summary

Components and Threats
- Introduction
- Memory Types
- Virtual Memory
- Memory Management
- Accessing Memory Securely
- Different States and System Functionality
- Types of Compromises
- Disclosing Data in an Unauthorized Manner
- Circumventing Access Controls
- Attacks
- Attack Type: Race Condition
- Attack Type: Data Validation
- Attacking Through Applications
- Buffer Overflow
- Attack Characteristics
- Attack Types
- More Attacks
- Host Name Resolution Attacks
- Even More Attacks
- Watching Network Traffic
- Traffic Analysis
- Cell Phone Cloning and Illegal Activities
- Summary
- Summary

Software Security Concerns
- Introduction
- How Did We Get Here
- Device vs. Software Security
- Why Are We Not Improving at a Higher Rate
- Usual Trend of Dealing with Security
- Where to Implement Security
- The Objective
- Systems Security
- Systems Security
- Programming Environment
- Security of Embedded Systems
- Summary

Software Lifecycle Process
- Introduction
- SDLC
- Integration of Risk Management into the SDLC
- Development Methodologies
- Maturity Models
- Secure Programming
- Programming Errors
- Security Issues
- Outsourced Development
- Trusted Program Modules
- Middleware
- Summary

Web Application Security
- Introduction
- OWASP Top Ten
- Modularity of Objects
- Object-Oriented Programming Characteristic
- Module Characteristics
- Linking Through COM
- Mobile Code with Active Content
- World Wide Web OLE
- ActiveX Security
- Java and Applets
- Common Gateway Interface
- Cookies
- PCI Requirements
- PA-DSS Requirements
- Vendor-Supplied Software
- Virtual Systems
- Virtualization Types
- Cloud Computing
- Summary
- Summary