Certified Information Systems Security Professional, Part 2 of 9: Access and Security Models

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 2 of a 9 part series

Runtime: 02:20:47

Course description: Access control is the heartbeat of information security. This course will talk about role access, layers of access, control characteristics, administrative controls and technical access. It will also cover architecture computer security concepts. This course is part of a series covering the ISC(2) Certified Information Systems Security Professional or CISSP.

Course outline:

Access Control Types
- Introduction
- Role of Access Control
- Definitions
- More Definitions
- Layers of Access Control
- Layers of Access Control Continued
- Access Control Mechanism Examples
- Access Control Characteristics
- Summary

More Access Control Types
- Introduction
- Preventative Control Types
- Administrative Controls
- Controlling Access
- Other Ways of Controlling Access
- Technical Access Controls
- Physical Access Controls
- Accountability
- Threats to Access Control
- Control Combinations
- Summary

Information Classification
- Introduction
- Information Classification
- Information Classification Criteria
- Declassifying Data
- Types of Classification Levels
- Summary

Access Control Models
- Introduction
- Models for Access
- Discretionary Access Control
- Enforcing a DAC Policy
- Mandatory Access Control Model
- MAC Enforcement Mechanism: Labels
- Where Are They Used?
- Role-Based Access Control
- Acquiring Rights and Permissions
- Rule-Based Access Control
- Access Control Matrix
- Access Control Administration
- Access Control Methods
- Network Access Control
- Policy on Network Services
- Remote Centralized Administration
- RADIUS Charcteristics
- TACACS+ Characteristics
- Diameter Characteristics
- Decentralized Access Control Administration
- Summary
- Summary

Trusted Computing Base
- Introduction
- System Protection: Trusted Computing Base
- System Protection: Reference Monitor
- Security Kernel Requirements
- Summary

Protection Mechanisms
- Introduction
- Security Modes of Operation
- System Protection: Levels of Trust
- System Protection: Process Isolation
- System Protection: Layering
- System Protection: Application Program Interface
- System Protection: Protection Rings
- What Does It Mean to Be in a Specific Ring
- Summary

Security Models
- Introduction
- Security Models
- Security Models Continued
- State Machine
- Information Flow
- Bell-LaPadula
- Rules of Bell-LaPadula
- Biba
- Clark-Wilson Model
- Non-Interference Model
- Brewer and Nash: Chinese Wall
- Take-Grant Model
- Summary

Evaluation Criteria
- Introduction
- Trusted Computer System Evaluation Criteria
- TCSEC Rating Breakdown
- Evaluation Criteria: ITSEC
- Comparison of Ratings
- ITSEC: Good and Bad
- Common Criteria
- Common Criteria Components
- First Set of Requirements
- Second Set of Requirements
- Package Ratings
- Common Criteria Outline

(Continued on page 2)

Certified Information Systems Security Professional, Part 2 of 9: Access and Security Models