Certified Information Systems Security Professional, Part 3 of 9: Cryptography and Operations

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 3 of a 9 part series.

Runtime: 02:27:48

Course description: Operations security is where all the theory and policies are put into action. Topics in this course will include administration responsibilities, redundancy and fault tolerance, and threats to operations. Also, an overview of cryptography and how it can be used in something like access will be discussed. This course is part of a series covering the ISC(2) Certified Information Systems Security Professional (CISSP).

Course outline:

Admin Responsibilities
- Introduction
- Operations Issues
- Role of Operations
- Administrator Access
- Computer Operations: System Administrators
- Security Administrator
- Operational Assurance
- Audit and Compliance
- Some Threats to Computer Operations
- Specific Operations Tasks
- Agenda
- Product Implementation Concerns
- Logs and Monitoring
- Records Management
- Change Control
- Resource Protection
- Contingency Planning
- System Controls
- Trusted Recovery
- Summary

Redundancy and Fault Tolerance
- Introduction
- Fault-Tolerance Mechanisms
- Duplexing, Mirroring, And Checkpointing
- Redundant Array of Independent Disks
- Fault Tolerance
- Redundancy Mechanism
- Backups
- Backup Types
- Summary

Operational Issues
- Introduction
- Remote Access
- Facsimilie Security
- Email Security
- Before Carrying out Vulnerability Testing
- Vulnerability Assessments
- Methology
- Penetration Testing
- Ethical Hacking
- Hack and Attack Strategies
- Protection Mechanism: Honeypot
- Summary

Threats to Operations
- Introduction
- Threats to Operations
- Data Leakage: Social Engineering
- Data Leakage - Object Reuse
- Object Reuse
- Why Not Just Delete the File or Format the Disk
- Data Leakage: Keystroke Logging
- Data Leakage: Emanation
- Controlling Data Leakage: TEMPEST
- Controlling Data Leakage: Control Zone
- Controlling Data Leakage: White Noise
- Summary
- Summary

Cryptography Terms
- Introduction
- Cryptography Objectives
- Cryptographic Definitions
- A Few More Definitions
- Some More Definitions
- Symmetric Cryptography: Use of Secret Keys
- Summary

Historical Uses of Cryptography
- Introduction
- Cryptography Uses Yesterday and Today
- Historical Uses of Symmetric Cryptography
- Scytale Cipher
- Substitution Cipher
- Caesar Cipher Example
- Vigenere Cipher
- Polyalphabetic Substitution and Vigenere Example
- Enigma Machine
- Vernam Cipher
- Running Key and Concealment
- Summary

Cryptography Foundations
- Introduction
- One-Time Pad Characteristics
- Binary Mathmatical Fuction
- Key and Algorithm Relationship
- 128-Bit Keys vs. 64-Bit Keys
- Breaking Cryptosystems: Brute Force
- Breaking Cryptosystems: Frequency Analysis
- Determining Strength in a Cryptosystem
- Characteristics of Strong Algorithms
- Open or Closed
- Summary

Modern Cryptography
- Introduction

(Continued on page 2)

Certified Information Systems Security Professional, Part 3 of 9: Cryptography and Operations

- Types of Ciphers Used Today
- Encryption/Decryption Methods
- Symmetric Ciphers: Block Cipher
- S-Boxes Used in Block Ciphers
- Symmetric Ciphers: Stream Cipher
- Encryption Process and Symmetric Characteristics
- Strength of a Stream Cipher
- Let's Dive in Deeper
- Symmetric Key Cryptography
- Symmetric Key Management Issue
- Summary

Symmetric Algorithms

- Introduction
- Symmetric Algorithms Examples
- Symmetric Downfalls
- Secret vs. Session Keys
- Symmetric Algorithms: DES
- Evolution of DES
- Block Cipher Modes: CBC
- Block Cipher Modes: ECB, CFB, and OFB
- Symmetric Ciphers: AES
- Other Symmetric Algorithms
- Agenda
- MAC- Sender
- Hashing Algorithms
- Protecting the Integrity of Data
- Data Integrity Mechanisms
- Weakness in Using Only Hash Algorithms
- More Protection in Data Integrity
- Security Issues in Hashing
- Birthday Attack
- Summary
- Summary