Certified Information Systems Security Professional, Part 4 of 9: Cryptography and Net Topologies

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 4 of a 9 part series.

Runtime: 02:58:00

Course description: This course covers symmetric and asymmetric cryptography and their history will be covered along with topics like Public key infrastructure, and various attacks. Also network and communication security will be discussed with topics inluding: network topologies, cabling and finally end with looking at network solutions. This course is part of a series covering the ISC(2) Certified Information Systems Security Professional (CISSP).

Course outline:

Asymmetric Cryptography
- Introduction
- Asymmetric Cryptography
- Public Key Cryptography Advantages
- Asymmetric Algorithm Disadvantages
- Symmetric vs. Asymmetric
- Asymmetric Algorithms
- Asymmetric Algorithm: Diffie-Hellman
- Asymmetric Algorithms: RSA
- Asymmetric Algorithms: El Gamal and ECC
- Example of Hybrid Cryptography
- When to Use Which Key
- Using the Algorithm Types Together
- Digital Signatures
- Digital Signature and MAC Comparison
- What if You Need All of the Services?
- U.S. Government Standard
- Summary

Public Key Infrastructure
- Introduction
- Why Do We Need a PKI
- Environment
- PKI and Its Components
- CA and RA Roles
- Let's Walk Through an Example
- Digital Certificates
- What Do You Do with a Certificate?
- Components of PKI: Repository and CRLs
- Summary

Cryptography and Attacks
- Introduction
- Cryptography and Attacks
- Steganography
- Key Management
- Link vs. End-to-End Encryption
- End-to-End Encryption
- Email Standards
- Secure Protocols
- SSL and the OSI Model
- SSL Connection Setup
- Secure Email Standard
- SSH Security Protocol
- Network Layer Protection
- IPSec Key Management
- Key Issues Within IPSec
- IPSec Handshaking Process
- SAs in Use
- IPSec Is a Suite of Protocols
- IPSec Modes of Operation
- Attacks on Cryptosystems
- More Attacks
- Summary
- Summary

Network Communications Security
- Introduction
- Network Security Issues
- Network and Communications Security
- Communications Security
- Network Security Methods
- Network-Based Security Problems
- Summary

Network Topologies
- Introduction
- Network Topologies: Physical Layer
- Topology Type: Bus
- Topology Type: Ring
- Topology Type: Star
- Network Topologies: Mesh
- Summary of Topologies
- LAN Media Access Technologies
- One Goal of Media Access Technologies
- Transmission Types: Analog and Digital
- Transmission Types: Synchronous and Asynchronous
- Two Types of Carrier Sense Multiple Access
- Transmission Types: Number of Receivers
- Media Access Technologies: Ethernet
- Media Access Technologies: Token Passing
- Media Access Technologies: Polling
- Summary

Network Technologies and Cabling
- Introduction
- Cabling
- Cabling Types: Coaxial
- Cabling Types: Twisted Pair
- Cabling Issues: Plenium-Rated
- Types of Networks
- Network Technologies
- Network Configurations
- MAN Technologies: SONET

(Continued on page 2)

Certified Information Systems Security Professional, Part 4 of 9: Cryptography and Net Topologies

- Wide Area Network Technologies
- WAN Technologies Are Circuit or Packet Switched
- Cicuit Switching
- WAN Technologies: ISDN
- ISDN Service Types
- WAN Technologies: DSL
- WAN Technologies: Cable Modem
- Packet Switching
- WAN Technologies: Packet Switched
- Packet Switched Networks
- WAN Technologies: X.25
- WAN Technologies: Frame Relay
- WAN Technologies: ATM
- Multiplexing
- Permanent Virtual Circuits
- Summary