Chapter 6 – Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

- Goals of Cryptography?

Cryptographic Foundations

- Confidentiality
- Integrity
- Authentication
- Nonrepudiation

Confidentiality

- Two main types of cryptosystems enforce
  - Symmetric cryptosystems
  - Asymmetric cryptosystems
- 3 scenarios
  - Data at rest, in transit, and in use

Integrity

- Digital signatures
- PKI and Cryptographic Applications?
- Hashes

Authentication

- Any ideas?

Nonrepudiation

- Any ideas?

Cryptography Concepts

- What is Cryptography?

Cryptography Concepts

- Plaintext
- Ciphertext
- Encrypt
- Decrypt

Cryptography Concepts

- All cryptography relies on ALGORITHMS
- Boolean mathematics
- Logical operations
  - AND, NOT, OR, XOR, Modulo

Cryptography Concepts

- One way functions
- Nonce
- Zero-Knowledge Proof

Cryptography Concepts

- Split Knowledge
  - Key Escrow
  - M of N controls
- Work Function
- Ciphers
  - Code vs Ciphers

Cryptography Concepts

- Transposition Ciphers
- Substitution Ciphers
- One-Time Pads
- Running Key Ciphers

Cryptography Concepts

- Block Ciphers
- Stream Ciphers
- Confusion and Diffusion

Modern Cryptography

- Cryptographic Keys
  - Symmetric Key Algorithms
  - Asymmetric Key Algorithms

Symmetric Key Algorithms

- Secret/Private Key Cryptography
- Ephemeral Key
- Key distribution is a major problem
- Does not implement nonrepudiation
- Algorithm is not scalable
- Keys must regenerated often

Asymmetric Key Algorithms

- Public Key Algorithms
- New users requires the generation of only one public-private key pair
- Can remove users easily
- Only need to make a new key if private key is compromised

Asymmetric Key Algorithms

- Can provide confidentiality, integrity, authentication, and nonrepudiation
- Simple process
- No preexisiting communication link needs to exist

Hashing Algorithms

- Digital Signatures
- Extremely difficult to replicate

Symmetric Cryptography

- Electronic Codebook (ECB) mode
- Cipher Block Chaining (CBC) mode
- Cipher Feedback (CFB) mode
- Output Feedback (OFB) mode
- Counter (CTR) mode
- Galois/Counter mode (GCM)

Symmetric Cryptography

- Counter with Cipher Block Chaining Message Authentication Code (CCM) mode
- Data Encryption Standard
- Triple DES
- International Data Encryption Algorithm
- BlowFish

Symmetric Cryptography

- SKIPJACK
- Rivest Ciphers
- Rivest Cipher 4 (RC4)
- Rivest Cipher 5 (RC5)
- Rivest Cipher 6 (RC6)
- Advanced Encryption Standard

Symmetric Cryptography

- CAST
- Memorize Table 6.9 in the book for the exam. This will come up in the CISSP

Symmetric Key Management

- Creation and Distribution of Symmetric Keys
- Offline Distribution
- Public Key Encryption
- Diffie-Hellman
- Storage and Destruction of Symmetric Keys

Symmetric Key Management

- Key Escrow and Recovery
  - Fair Cryptosystems
  - Escrowed Encryption Standard

Cryptographic Life Cycle

- Specifying the algorithm to use
- Identifying the acceptable key lengths for use with each algorithm and the type of data being transmitted
- Enumerate the security protocols to be used