CompTIA Security + 6.0 Cryptography and PKI

Filename: comptia-secplussy0501-6-2-cryptography_algorithms_basics
Title: Data Security and Privacy Practices
Subtitle: CompTIA Security+ (SY0-501)

6.2 Cryptography Algorithms Basics

- 6.2 Explain cryptography algorithms and their basic characteristics.
  - Basics
    - Plaintext = unencrypted text (readable)
    - Ciphertext = encypted text (Confidential)
    - Encryption algorithm = mathematical procedure for converting plaintext into ciphertext
    - Encryption key = a variable used in conjunction with a encryption algorithm to produce ciphertext
    - Encryption
      - Algorithm + key = Unique ciphertext
    - Symmetric-key encryption = same keys are used for encryption and decryption
    - Asymmetric-key encryption = a key pair are used in encryption and decryption
    - Hash Function/message digest = is as one-way mathmatical operation performed on a string of data that produces a fixed-length value
    - Comparison diagram
  - Symmetric algorithms
    - AES
      - Originally Rijndael
      - Establish by NIST in 2001
      - US Government adopted in 2002
      - Symmetric
      - Key bit lengths - 128, 192, 256
    - DES
      - Originally published in 1977
      - Block-cipher
      - 56 Bits
      - Brute Force vulnerabilities
    - 3DES
      - 1998
      - Increasing DES encryption perform three DES operations
      - 64 Bit Block size
      - Three Keys = 168 key bits
      - Two Keys = 122 key bits
      - One Key = 56 key bits
    - RC4
      - 1987 Ron Rivest
      - Stream Cipher
      - Fast and simplistic
      - Weak and insecure
      - Used in:
        - WEP, WPA, Formerly in SSL/TLS
    - Blowfish
      - 1993 by Bruce Schneier
      - Symmetric-key encryption
      - 64 Bit ket length
      - Alternative to DES
      - Resembles CAST-128
      - Block Cipher
    - Twofish
      - 1998 by a group of people (Bruce Schneier, Neils Ferguson)
      - symmetric-key
      - Block Cipher
      - Key bit lengths - 128, 192, 256
  - Cipher modes
    - A cipher is what is used to encrypt/decrypt data
    - A cipher-mode defines how to encrypt the data
    - CBC
      - Cipher block chaining(CCMP)
      - Uses IVs
      - Decryption will depend on all preceeding cipher-tex blocks
      - A single bit error can affect the decryption of all later cihper blocks
    - GCM
      - Galois/Counter Mode
      - Mode of operation for symmetric-key blok ciphers
      - Authenticated encryption algorithm

        - ECB
            - Electronic Code Book
            - Mode of Operation for block ciphers
            - Supports seperate key encryption for each block
        - CTR
            - CTM probably Counter-mode (Counter mode with Cipher Block Chaining Message Authentication Code Protocol)
            - Turns a block cipher into stream cipher
        - Stream vs. block
            - Stream Ciphers
                - Faster encryption
                - Less resource consumption (CPU, Memory)
                - w
            - Block Ciphers
                - With bit lengths of 64, 128, 192, 265 data that is smaller than the size of the implementation can cause padding to be added
    - Asymmetric algorithms
        - RSA
            - Introduced in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman
            - Public key/asymmetric key cryptology
        - DSA
            - Introduce by NIST in 1991
            - Digitial Signature Algorithm
        - Diffie-Hellman
            - Groups
            - DHE
            - ECDHE
                - Uses normal DHE suite with ECC
        - Elliptic curve
            - ECC is based on an algebraic structure of elliptic cureves
            - Can use smaller keys
            - Other technologies TLS, PGP, SSH use elliptic curves
        - PGP/GPG
            - PGP
                - Used for confidentiality and authentication
                - Combines hashing, data compression,symmetric-key encryption and public-key encryption
                - Public keys are bound to a username and email
            - GPG
                - Open source or free implementation of OpenPGP
    - Hashing algorithms
        - MD5
            - Introuduced in 1992 by Ron Rivest
            - Vulnerable
            - Can be used for basic file integrity and checksum
        - SHA
            - SHA-0 = 160 Bits
            - SHA-1 = 160 Bits
            - SHA-2 = 224, 256, 384, 512
            - SHA-3 = Same as SHA-2
        - HMAC
            - Stronger than MAC as it adds a hashing function by concatenating the meassage with a secret key and hashing both
            - Strength is determined by the hashing algorithm used and the strength of the secret key
            - HMAC-MD5 vs. HMAC-SHA1
        - RIPEMD
            - RACE Integrity Primitives Evaluation Message Digest
            - 128(collisions), 160(most common), 256, 320
    - Key stretching algorithms
        - Weak passwords or keys can strenghtened or increase the difficulty to attack the key
        - The key is fed into an algorithm that produces a stronger or enhanced key
        - BCRYPT
            - Password hashing function
            - Used in Unix/Linux-based systems to protect passwords
            - Salts passwords (adds bits) then encrypts with BlowFish
        - PBKDF2
            - Adds salt in a minimum of 64 Bits and hash passwords in WPA2, iOS, Cisco
    - Obfuscation
        - XOR
        - ROT13
            - http://www.rot13.com/
            - Cherokee
                - Fkhumhh (ROT3)
                - Purebxrr (ROT13)
        - Substitution ciphers
            - plain : abcdefghijklmnopqrstuvwxyz

- cipher : uhqdib meayln ofgxjc rkvstz wp
- Cherokee