Cryptography

Mike Smith

26/04/10 - Rev.31

IPSec

- **Authentication Header - AH** - used for authentication protocol
- **Encapsulating Security Payload - ESP** - used for authentication and encryption
- **Transport Mode** - payload of the message is protected
- **Tunnel Mode** - both payload and routing are protected
- **Security Association - SA** - Simplex, keeps record of parameters

Hashing

- Hash for message digest provides integrity
- HMAC - used with secret key to provide integrity and data origin authentication
- CBC-MAC - uses symmetric block algorithm, provides integrity and data origin authentication
- CMAC - same as CBC-MAC but uses complex logic
- MD2, MD4, MD5, SHA, HAVAL, Tiger

Asymmetric

- Also called Public Key Cryptography
- Each person has private and public key
- For Confidentiality - Sender encrypts with receivers public key - secure message format
- For Authentication - Sender encrypts with their private key - open message format

Strengths

- Better key distribution than symmetric
- Better scalability than symmetric
- Can provides authentication and nonrepudiation

Weaknesses

- Much slower than symmetric
- Mathematically intensive

Examples

- Rivest-Shamir-Adleman - RSA
- Elliptic Curve Cryptosystem - ECC
- Diffie-Hellman
- El Gamal
- Digital Signature Algorithm - DSA
- Merkle-Hellman Knapsack

Symmetric

- Also called secret keys
- For n people, requires n(n-1)/2 keys
- Same key to encrypt/decrypt at both ends
- Block and Stream types

Strengths

- Much faster than asymmetric
- Hard to break if using a large key size

Weaknesses

- Requires secure mechanism to deliver keys
- Each pair need a unique key
- Confidentiality, but not authenticity or nonrepudiation

Examples

- Data Encryption Standard - DES
  - Electronic Code Book - ECB
  - Cipher Block Chaining - CBC
  - Cipher Feedback - CFB
  - Output Feedback - OFB
  - Counter - CTR
- Triple-DES (3DES)
  - DES-EEE3
  - DES-EDE3
  - DES-EEE2
  - DES-EDE2
- Blowfish
- International Data Encryption Algorithm - IDEA
- RC4, RC5 and RC6
- Advanced Encryption Standard - AES
  - Rijndael

History

- 2000 BC Egypt - atbash - substitution
- 400 BC Sparta - scytale cipher - wooden rods
- 100 - 44 BC Caesar cipher
- 16th Century - Vigenere Polyalphabetic cipher
- 1917 - Gilbert Vernam - Vernam cipher - one-time pad
- 1920 - William Friedman - Father of Modern Cryptography
- WW II - German Enigma
- 1970 - Lucifer - IBM
- 1976 - DES

Services

- Confidentiality - cryptography protects confidentiality
- Integrity - cryptography helps with hashing algorithms and message digests
- Authentication - used for this too
- Authorization - upon proving identity can then have key to some resource
- Nonrepudiation - cannot deny sending message

Encryptions at various levels

- End-to-end encryption happens within the application
- SSL encryption takes place at the transport layer
- PPTP encryption takes place at the data link layer
- Link encryption takes place at the data link and physical layer

Cryptosystem

- Software
- Protocols
- Algorithms - Kerckhoffs' Principle - Publicly known
- Keys

Steganography

- Carrier - signal, data stream or file
- Stego-medium - medium in which hidden
- Payload - concealed information

Public Key Infrastructure

- Certificate Authority - CA
  - Takes liability for the authenticity of the individual
  - Binds the individuals identity to the public key
  - Requires cross certification with other CAs
  - Maintains Certificate Revocation Lists - CRLs
- Registration Authority - RA
  - Performs certificate registration duties
  - Broker between user and CA
- Certificate Repository, Certificate revocation system, OCSP
- Provides all services

Strong Cipher

- Confusion - carried out using substitution
- Diffusion - carried out using transposition