Glenda Whitbeck
Global Computing Security Architect
Spirit AeroSystems

Cryptography Review

January 7, 2011

History of Cryptography

- History
  - 2000 B.C. Egyptian Hieroglyphics
  - Atbash - Hebrew
    - Original alphabet mapped to different letter
    - Type of Substitution Cipher – monoalphabetic
      (multiple alphabets would be polyalphabetic)
  - 400 B.C. Spartans scytale cipher
    - Papyrus wrapped around a staff
  - 100-44 B.C. Caesar cipher
    - Shifted alphabet by 3 letters
    - Alphabet is the algorithm, key is the # shifted
  - 16th Century – Vigenere Cipher
    - Polalphabetic that used table where intersection between plaintext and key word repeated as necessary produced ciphertext
  - World War II – Germany's Enigma machine

Services of Cryptosystems

- **Confidentiality** – Read by Authorized Entities Only
- **Integrity** – Data hasn't been altered
- **Authentication** – Verifies identity of user
- **Authorization** – Provides key or password to allow access
- **Nonrepudiation** – Ensures sender can't deny sending the message

Strength of a Cryptosystem

- **Algorithm**
  - Confusion (substitution)
  - Diffusion (transposition)
  - Known or Secret More Secure? Kerckhoff's Principle Algorithm should be Publicly Known
- **Key Management**
  - Protect Keys and Keep Secret
- **Length of the Key**
- **Initialization Vectors**
  - Random values used with algorithms to prevent patterns
- **Implementation**

Ciphers

- **Running Key Cipher**
  - Use of things around you
    - Example Book #, Page #, Line #, 5th Word
- **Concealment Cipher**
  - Hidden in a message (like every 4th word)
- **Block Cipher**
  - Message divided into blocks
  - Each block is encrypted separately
- **Steam Cipher**
  - Encrypts individual bits of the message
  - One bit is XORed to message bits

Encryption Algorithms

Symmetric

Characteristics

- Confidentiality only
- Not Scalable – n users need n(n-1)/2 keys
- Key Management Difficult
- Used to encrypt Bulk Data

Block Ciphers

- S-boxes for substitution & transposition
- Modes (ECB, CBC, CFB, OFB, CTR)
- Examples - DES, 3DES, Blowfish, Twofish, IDEA
- RC5,RC6, AES, SAFER, Serpent

Steam Ciphers

- More difficult to get right
- Key stream generators
- XOR bits
- Example – RC4

Asymmetric

Characteristics

- Used by Public Key Cryptography
- Used to Encrypt Keys (except Diffie-Hellman)
- Provides Authentication and Non-Repudiation
- Based on one-way function which is easier to compute one direction and hard the opposite direction
- Private key knows how to get through the "trapdoor"
- Examples
  - El Gamal – Slowest
  - Eliiptic Curve Cryptosystems – most efficient
  - LUC
  - Knapsack – Insecure

Digital Signatures

Provide

- Authentication
- Nonrepudiation
- Integrity

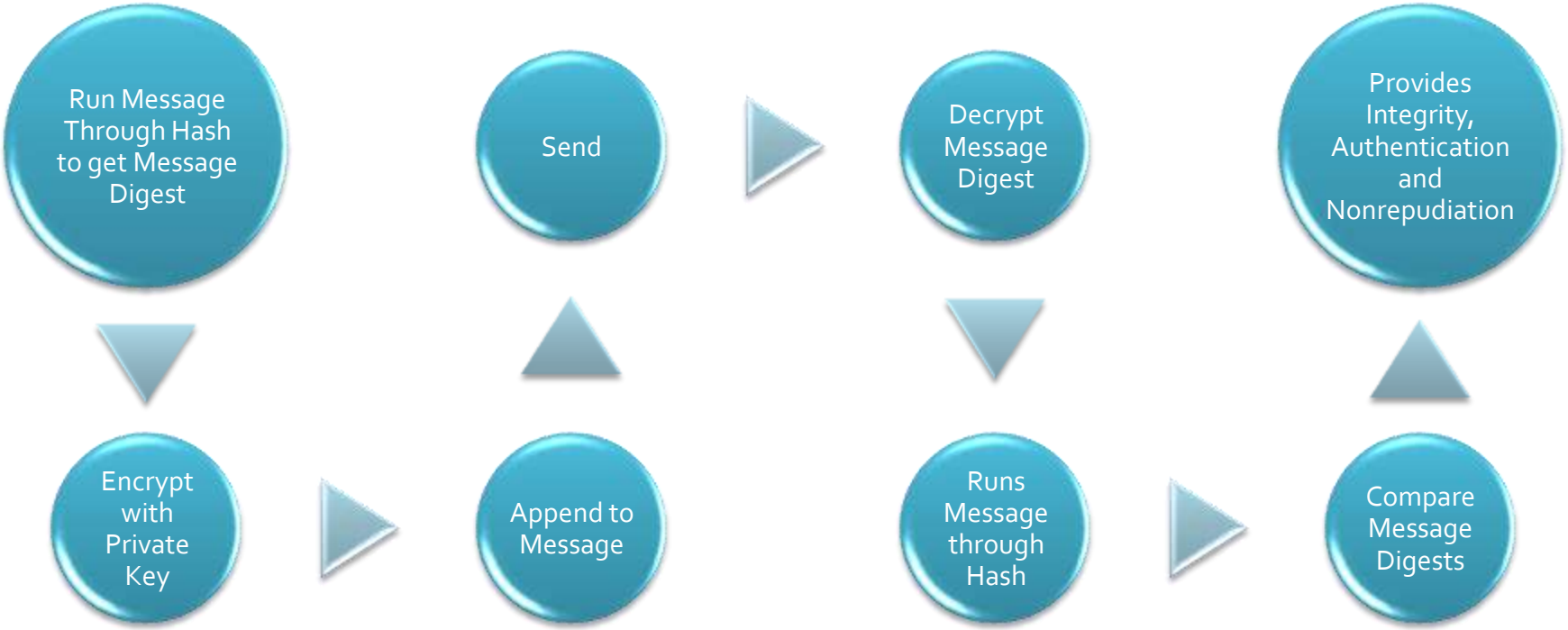
Uses Hash

- For Integrity
- Sender uses hash to create message digest
- Receiver also uses hash and compares

Uses Asymmetric Algorithm

- To encrypt hash with senders Private Key for Nonrepudiation and authentication
- Unencrypted with senders Public Key and compared

Digital Signature



Hashing Algorithms

128 bit MD

- MD2
- MD4
- MD5
- Ripe MD-128

160 bit MD

- SHA-1
- Ripe MD-160

Others

- SHA-256,384,512
- HAVAL Variable
- Tiger – 192-bit digest

Security of Messages

- Encryption provides confidentiality
- Running through a hash provides integrity
- Digital Signatures provide Authentication, Nonrepudiation and Integrity
- Encryption with Digital Signature provides Confidentiality, Authentication, Nonrepudiation and Integrity

Public Key Infrastructure

RA

- Certification Registration
- Verifies Identification of Requestor
- Acts as Broker Between User and CA

CA

- Trusted Organization or Server
- Creates, Signs and Hands out Certificates
- Vouches for Person's Identity
- Certificate Revocation List (CRL)

Certificate

- Serial #
- Version #
- Identity Info
- Algorithm
- Lifetime Dates
- Signature of Issuing Authority

Email Standards

- **Multipurpose Internet Mail Extension** (MIME)
- **Secure MIME** (SMIME)
  - Encryption
  - Digital Signing
  - Extends MIME Standard
  - Encryption and Hashing Algorithms Can be Specified
  - Follows Public Key Cryptography Standards (PKCS)
  - Provides Confidentiality (encryption), Integrity (Hashing), Authentication (through X.509 Certs) and Nonrepudiation (Signed Message Digests)
- **Pretty Good Privacy**

Internet Security

- HTTP Secure (HTTPS)
  - HTTP running over SSL (Secure Sockets Layer)
  - Client Generates Session Key and Encrypts with Server Public Key
  - Protects Channel
- Secure HTTP (S-HTTP)
  - Protects Each Message
- Secure Electronic Transfer (SET)
  - Proposed by Visa and MasterCard For More Secure Credit Card Transactions
  - Involves Issuer, Cardholder, Merchant, Acquirer, Payment Gateway
  - All Would Have to Upgrade Software – So Not Fully Implemented Yet
- Secure Shell (SSH)
  - Tunneling Mechanism

Internet Security

- Internet Protocol Security (IPSEC)
  - Method of setting up a secure channel
  - Open modular framework
  - Uses two basic protocols
    - Authentication Header
      - Provides authentication and integrity
    - Encapsulating Security Payload
      - Provides both those and confidentiality
  - Each Device has Security Association's (SA)
    - Configurations it Can Support
    - Used to Negotiate
    - Needs 1 Inbound and 1 Outbound for All Connections
  - Security Parameter Index (SPI)
    - Keeps track of all the SA's
  - Key Management
    - De Facto Standard is Internet Key Exchange (IKE)

Attacks

- Cipher-Only
- Known-Plaintext
- Chosen-Plaintext
- Chosen-Ciphertext
- Adaptive….
- Differential Cryptanalysis
- Linear Cryptanalysis
- Side-Channel Attacks
- Replay Attacks
- Algebraic Attacks
- Analytic Attacks
- Statistical Attacks