Basics of Cryptography

Otakar A.

Introduction

- "Hidden writing"
- Increasingly used to protect information
- Can ensure confidentiality
    - Integrity and Authenticity too

History – The Manual Era

- Dates back to at least 2000 B.C.
- Pen and Paper Cryptography
- Examples
  - Scytale
  - Atbash
  - Caesar
  - Vigenère

History – The Modern Era

- Computers!
- Examples
  - Lucifer
  - Rijndael
  - RSA
  - ElGamal

Speak Like a Crypto Geek

Plaintext – A message in its natural format readable by an attacker

Ciphertext – Message altered to be unreadable by anyone except the intended recipients

Key – Sequence that controls the operation and behavior of the cryptographic algorithm

Keyspace – Total number of possible values of keys in a crypto algorithm

Speak Like a Crypto Geek (2)

Initialization Vector – Random values used with ciphers to ensure no patterns are created during encryption

Ensures the encryption of the same string twice does not return the same result.

Types of Cryptography

- Stream-based Ciphers
  - One at a time
  - Good for real-time services
- Block Ciphers
  - Substitution and transposition

Encryption Systems

- Substitution Cipher
  - Convert one letter to another
  - Cryptoquip
- Transposition Cipher
  - Change position of letter in text
  - Word Jumble (Anagram)
- Monoalphabetic Cipher
  - Caesar

Encryption Systems

- Polyalphabetic Cipher
  - Vigenère
- Modular Mathematics
  - Running Key Cipher
- One-time Pads
  - Randomly generated keys

Steganography

- Hiding a message within another medium, such as an image
- No key is required
- Example
  - Modify color map of JPEG image

Cryptographic Methods

- *Symmetric*
  - Same key for encryption and decryption
  - Key distribution problem
- *Asymmetric*
  - Mathematically related key pairs for encryption and decryption
  - Public and private keys

Cryptographic Methods

- *Hybrid*
  - Combines strengths of both methods
  - Asymmetric distributes symmetric key
    - » Also known as a *session key*
  - Symmetric provides bulk encryption
  - Example:
    - » SSL negotiates a hybrid method

Hashing Algorithms

- MD5
  - Computes 128-bit hash value
  - Widely used for file integrity checking
- SHA-1
  - Computes 160-bit hash value
  - NIST approved message digest algorithm

Birthday Attack

- Collisions
  - Two messages with the same hash value
- Based on the “birthday paradox”
- Hash algorithms should be resistant to this attack

Message Authentication Codes

- Small block of data generated with a secret key and appended to a message
- HMAC (RFC 2104)
  - Uses hash instead of cipher for speed
  - Used in SSL/TLS and IPSec

Digital Signatures

- Hash of message encrypted with private key
- Digital Signature Standard (DSS)
  - DSA/RSA/ECD-SA plus SHA
- DSS provides
  - Sender authentication
  - Verification of message integrity
  - Nonrepudiation

Encryption Management

- Key Distribution Center (KDC)
  - Uses master keys to issue session keys
  - Example: Kerberos
- ANSI X9.17
  - Used by financial institutions
  - Hierarchical set of keys
  - Higher levels used to distribute lower

Public Key Infrastructure

- All components needed to enable secure communication
  - Policies and Procedures
  - Keys and Algorithms
  - Software and Data Formats
- Assures identity to users
- Provides key management features

PKI Components

- Digital Certificates
  - Contains identity and verification info
- Certificate Authorities
  - Trusted entity that issues certificates
- Registration Authorities
  - Verifies identity for certificate requests
- Certificate Revocation List (CRL)

PKI Cross Certification

- Process to establish a trust relationship between CAs
- Allows each CA to validate certificates issued by the other CA
- Used in large organizations or business partnerships

Cryptanalysis

- The study of methods to break cryptosystems
- Often targeted at obtaining a key
- Attacks may be passive or active

Cryptanalysis

- Kerckhoff's Principle
  - The only secrecy involved with a cryptosystem should be the key
- Cryptosystem Strength
  - How hard is it to determine the secret associated with the system?

Cryptanalysis Attacks

- Brute force
  - Trying all key values in the keyspace
- Frequency Analysis
  - Guess values based on frequency of occurrence
- Dictionary Attack
  - Find plaintext based on common words

Cryptanalysis Attacks

- Replay Attack
  - Repeating previous known values
- Factoring Attacks
  - Find keys through prime factorization
- Ciphertext-Only
- Known Plaintext
  - Format or content of plaintext available

Cryptanalysis Attacks

- Chosen Plaintext
  - Attack can encrypt chosen plaintext
- Chosen Ciphertext
  - Decrypt known ciphertext to discover key
- Differential Power Analysis
  - Side Channel Attack
  - Identify algorithm and key length

Cryptanalysis Attacks

- Social Engineering
  - Humans are the weakest link
- RNG Attack
  - Predict IV used by an algorithm
- Temporary Files
  - May contain plaintext

E-mail Security Protocols

- Privacy Enhanced Email (PEM)
- Pretty Good Privacy (PGP)
  - Based on a distributed trust model
  - Each user generates a key pair
- S/MIME
  - Requires public key infrastructure
  - Supported by most e-mail clients

Network Security

- Link Encryption
  - Encrypt traffic headers + data
  - Transparent to users
- End-to-End Encryption
  - Encrypts application layer data only
  - Network devices need not be aware

Network Security

- SSL/TLS
  - Supports mutual authentication
  - Secures a number of popular network services
- IPSec
  - Security extensions for TCP/IP protocols
  - Supports encryption and authentication
  - Used for VPNs