Computer Security and Penetration Testing

Encryption and Password Cracking
Objectives

• Understand basic cryptographic principles
• Understand the fundamentals of encryption
• Describe the most common ciphers in use today
• Identify the most common attacks on passwords
• Use various programs for cracking passwords
Encryption and Password Cracking

• Strong passwords
  – Good defense against unwanted entry
• Guessing, stealing, or cracking passwords
  – Foundation of defeating any kind of security
Cryptography

- **Cryptography**
  - Algorithm *encrypts* a ciphertext document from a *plaintext* document
  - Algorithm *decrypts* the ciphertext back into plaintext

- **Transposition**
  - Change in the position or order of letters or words
  - Does not rely on length of password
  - Transposition is based on probabilities
  - Anyone can break a transposition cipher based on frequency of letters
Cryptography (continued)

• Substitution
  – Replacement of a letter or group of letters with another letter or group of letters
  – **Enigma**
    • Possibly the most famous substitution cryptography machine
    • Used by the German Army during World War II
  – **Turing Bombe**
    • Machine to crack the “Enigma Code”
    • Developed by Alan Turing
Cryptography (continued)

• Substitution (continued)
  – Colossus
    • Programmable computer (1943 by Max Newman)

• Common terms when dealing with cryptography
  – Cleartext
  – Cyphertext
  – Key
  – Algorithm
  – Hash
Symmetric and Asymmetric Key Encryption

• Encryption can be performed with either a symmetric key or an asymmetric key
Symmetric Key Encryption

• Sometimes called secret key algorithms
• Uses same key to encrypt and to decrypt the data
• Sender and recipient must have a copy of the key
  – Inherent vulnerability of secret key algorithms is that the key must be transmitted
• Faster than asymmetric key algorithms
Symmetric Key Encryption (continued)

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Security</th>
<th>Speed (Pentium PC)</th>
<th>Key length</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>low</td>
<td>4.0 Gb/s</td>
<td>56 bits</td>
</tr>
<tr>
<td>3DES</td>
<td>good</td>
<td>1.5 Gb/s</td>
<td>112 bits</td>
</tr>
<tr>
<td>IDEA</td>
<td>good</td>
<td>2.0 Gb/s</td>
<td>128 bits</td>
</tr>
<tr>
<td>3IDEA</td>
<td>very good</td>
<td>1.0 Gb/s</td>
<td>256 bits</td>
</tr>
<tr>
<td>Skipjack</td>
<td>good</td>
<td>4.0 Gb/s</td>
<td>80 bits</td>
</tr>
<tr>
<td>CLIPPER chip</td>
<td>good</td>
<td>-</td>
<td>80 bits</td>
</tr>
</tbody>
</table>
Symmetric Key Encryption (continued)

• **Stream Ciphers**
  – Use a key stream to encrypt and decrypt a plaintext message

• Key stream is similar to a **one-time pad**
  – A list of random numbers from 1 to 25
  – Numbers in the one-time pad are added to the letters in the plaintext to encrypt
    • And subtracted from the cyphertext to decrypt
  – Algorithm **XORs** key stream with plaintext message
Symmetric Key Encryption (continued)

- **Block Ciphers**
  - Operate on blocks of data
- Algorithm breaks the plaintext document into blocks (usually 8 or 16 bytes long)
  - Operates on each block independently
- Plaintext will always be padded
- Block ciphers allow you to reuse keys
Asymmetric Key Algorithms

- Also called public key algorithms
- Two keys for encrypting and decrypting data
- Each user has a public key and a private key
  - Public keys can be sent unencrypted over unsecured media
- Public key encrypts data
  - Private key decrypts data encrypted with public key
Asymmetric Key Algorithms (continued)

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Security</th>
<th>Speed</th>
<th>Key length</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>good</td>
<td>fast</td>
<td>varies (1024 safe)</td>
</tr>
<tr>
<td>Diffie-Hellman</td>
<td>good</td>
<td>slower than RSA</td>
<td>varies (1028 safe)</td>
</tr>
<tr>
<td>DSS</td>
<td>low</td>
<td>—</td>
<td>512 bits</td>
</tr>
</tbody>
</table>
Asymmetric Key Algorithms (continued)

- **DSA (Digital Signature Algorithm)**
  - Digital signature connects documents with the holder of a specific key
  - Considered too slow for general encryption

- **Digital Time Stamps**
  - Connects document with a specific time of origination
Cryptanalysis

- Cryptanalyst decodes messages to make them readable
- First and most important step in cryptanalysis
  - Detecting the key values
Description of Popular Ciphers

- Average user tends to confuse the categories within the cryptographic taxonomy