Level of Implementation

- Internet Layer Security
  - Ex. IP Security Protocol (IPSEC)
  - Host-to-Host Basis, No Packets Discrimination

- Transport Layer Security
  - Ex. Secure Sockets Layer (SSL)
  - Process-to-Process Basis, Need Modified Apps

- Application Layer Security
  - Ex. Pretty Good Privacy, Kerberos
  - Document-Level, Need Modified Apps
Application Layer Security

- Secure Electronic Transaction (SET)
  - Jointly Developed by Visa and MasterCard
  - A Method to Secure Business Transaction Over Open Networks
  - Encrypt and Transmit a Sensitive Document
- Kerberos
  - Originated at MIT
  - On Standard Track with the IETF. Default Network Authentication in MS Windows 2000
  - Distributed Authentication, Key Distribution System
  - Auth. of Two Parties and Dist. of Keys

Key Functionality

- Authentication
  - Verification of the Identity of a Party
- Integrity
  - Assurance that the Data Received is the Same as Generated
- Confidentiality
  - Protection of Information from Disclosure
- Authorization
  - Determination if a Principal should be Allowed to Perform an Operation
Secure Electronic Transaction (SET)

- A Method to Secure Payment Card Transaction Over Open Networks

Overview
  - Concepts
  - Encryption Process
  - Processing Sample

Concepts

- Secret Key Cryptography
- Public Key Cryptography
- Digital Envelope
- Message Digest
- Digital Signature
- Key Exchange
- Certificate
- Certificate Authority
Secret Key, Public Key

- Secret Key Cryptography
  - Symmetric Cryptography
  - The Same Key is Used to Encrypt and Decrypt
- Public Key Cryptography
  - Asymmetric Cryptography
  - One Key to Encrypt and One Key to Decrypt
  - Public Key and Private Key
  - Data Encrypted with Either Key can only be Decrypted Using the Other Key

Digital Envelope

- Encryption
  - Encrypt a Message Using a Secret Key
  - Encrypt the Key Using the Recipient’s Public Key
- Decryption
  - Decrypt the Secret Key Using the Recipient’s Private Key
  - Decrypt the Message Using the Decrypted Secret Key
Message Digest

- A Value Generated for a Message that is Unique to that Message
- Small, Compared to the Message Itself
- Highly Unlikely for Two Messages to Have the Same Message Digest (1 in $10^{48}$ for SET)

Digital Signature

- Encrypt a Message Using the Sender’s Private Key
- The Recipient Decrypts the Message Using the Sender’s Public Key
- Ensured that the Message Could only be Encrypted by the Sender
- In SET, Encrypted Message Digest = Digital Signature
Key Exchange

- Each SET Participant Has Two Public/Private Key Pairs
- “Key Exchange” Pair for Encryption and Decryption
- “Signature” Pair for Creation and Verification of Digital Signatures

Certificate, Certificate Authority

- Certificate
  - Digitally Signed by CA, Containing a Participant’s ID and Public Key
  - Can Be Decrypt Using CA’s Public Key
- Certificate Authority (CA)
  - Trusted Third Party Used to Authenticate a Participant’s Public Key
  - A Participant Identifies Himself with CA, CA Returns a Digitally Signed Certificate Containing a Participant’s ID and Public Key
Simple Transaction Process

- Alice Wants to Send Bob a Message Securely Over an Open Network

![Diagram showing the simple transaction process]

Encryption Process (Alice)

![Diagram showing the encryption process (Alice)]
Decryption Process (Bob)

- Alice’s public signature key
- Alice’s certificate
- Bob’s private key-exchange key
- Bob’s private key-exchange key
- symmetric key
- message
- m digest
- compare
- m digest
- m digest

SET Processing

- Cardholder Registration
- Merchant Registration
- Purchase Request
- Payment Authorization
- Payment Capture
- Etc.
Kerberos

• A Distributed Authentication and Key Distribution System
  – A Client Wants Secure Transaction with a Server
  – KDC Distributes a Session Key for the Client and Server to Use

• Overview
  – Concepts
  – Key Distribution

Concepts

• Shared Secrets
• Authenticators
• Key Distribution Center
• Session Keys
• Session Tickets
• Symmetric Cryptography
• Digital Signatures
• Certificate Authority
• Secret Key
• Digital Envelope
Key Distribution Center (KDC)

- Physically Secure Server
- Maintains Participant Account Information
  - Long-Term Key
    - Cryptographic Key Known Only to the Participant and KDC
    - Usually Derived from the Log-in Password
<table>
<thead>
<tr>
<th>SET vs Kerberos</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Needs Trusted Intermediary (CA)</strong></td>
</tr>
<tr>
<td><strong>CA Issues Certificate to Identify Principal</strong></td>
</tr>
<tr>
<td><strong>To Exchange Message Securely</strong></td>
</tr>
<tr>
<td><strong>Needs Trusted Intermediary (KDC)</strong></td>
</tr>
<tr>
<td><strong>KDC Maintains Principal’s A/C Info</strong></td>
</tr>
<tr>
<td><strong>To Distribute Key to Establish Secure Channel</strong></td>
</tr>
</tbody>
</table>