Micropayment Protocol

Presented by

Monica Fengqiu Wu

- CMPE296U Web Application
Micropayment Protocol

Outline

• What is micropayment?
• Important aspects of micropayment
• 3 existing examples: MilliCent, NetBill, MPTP
• Summary
Micropayment Protocol

What is Micropayment?

• No exact definition

• Small-amount payment transactions

• Transactions are conducted via open networks, such as the Internet

• Low transaction cost

• Provide information-based services and merchandise, e.g., newspaper, journals, game, music, on-line education, and software rental.
Micropayment Protocol

Important Aspects of Micropayment Protocol

• Current existing payment methods applicable?
  - cash, credit card, check, eCash, eCheck, etc.

• General payment solution: charge upon aggregation amount using the existing payment methods, then consume it little by little.

• Cost! Cost! Cost!

• Limited involved parties – 3 are common.

• Security and authentication

• Easy to deploy

- CMPE296U Web Application
Micropayment Protocol

What impacts on cost?

- Payment methods
- Goods delivery - Over the Internet? By courier?
- Account management – large casual accounts
- Encryption
- Transaction model (on-line/off-line)
- Intermediary money producing
Micropayment Protocol

Sample 1: MilliCent – Relationship model

- CMPE296U Web Application
Micropayment Protocol

Sample 1: MilliCent – How does it work?

1. purchase vendor scrip using broker scrip
2. return vendor scrip and change in broker scrip
3. purchase using vendor scrip
4. deliver merchandise/services
5. request vendor scrip if none is in stock
6. return vendor scrip and associated secret

- CMPE296U Web Application
Micropayment Protocol

Sample 1: MilliCent – Architecture

- CMPE296U Web Application
Micropayment Protocol

Sample 1: MilliCent – scrip structure and customer secret generation

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Value</th>
<th>scrip-id</th>
<th>customer-id</th>
<th>expiration-date</th>
<th>customer properties</th>
<th>certificate</th>
</tr>
</thead>
</table>

Scrip structure

- CMPE296U Web Application
Micropayment Protocol

Sample 1: MilliCent – scrip signature

- CMPE296U Web Application
Micropayment Protocol
Sample 1: MilliCent – scrip validation (authentication)

- CMPE296U Web Application
Micropayment Protocol

Sample 2: NetBill - Relationship Model

- CMPE296U Web Application
Micropayment Protocol

Sample 2: NetBill – How does it work?

1. Price request
2. Price quote
3. Purchase request
4. Delivery encrypted goods
5. EPO
6. EPO+invoice+decryption key
7. Approval+decryption key
8. Decryption key

- CMPE296U Web Application
Micropayment Protocol

Sample 2: NetBill – Architecture

- CMPE296U Web Application
Micropayment Protocol

Sample 2: NetBill – Authentication, encryption and signature

• Authentication - Public key based Kerberos for Distributed Authentication (PKDA).

• Encryption – RSA public key algorithm and DES (Data Encryption Standard).

• Signature – Digital Signature Algorithm (DSA) during payment phase.
Micropayment Protocol

Sample 3: MPTP – Relationship model

- CMPE296U Web Application
Micropayment Protocol

Sample 3: MPTP – Payword

- A chain of paywords, \( w_1, w_2, ..., w_n \). Each payword \( w_i \) is worth some value, for example, 5 cents, so the chain has value \( n \times 5 \) cents.

- To generate the payword chain, uses a hash function \( h \) (e.g., MD5 or SHA) for \( i = n-1, n-2, ..., 1, 0 \). \( w_i = h(w_{i+1}) \)

Here, \( w_n \) is a random selected number; \( w_0 \) is the root of the payword chain, and defines a value for each payword, but it is not a payword itself.

- A payment encloses only the last payword, not a list of individual

- To spend the payword, user need sign a commitment

- User-specific and vendor-specific. No value to another vendor.
Sample 3: MPTP – Authentication and signature

• MPTP uses signature validations to authenticate each party.
• User’s payment has two parts: certificate with broker’s signature; chained payword with user’s signature.
• Broker’s decryption key is known to all parties.
• Chained payword has user’s signature.
• Between customer and broker, they use checksum together with a shared secret key to authenticate with each other.
Micropayment Protocol

Open issues

• Taxes
• Foreign currency exchange, export/import
• Money laundering
• Insider fraud
• Privacy and anonymity

- CMPE296U Web Application
Micropayment Protocol

3 existing protocol comparison table

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Security</th>
<th>Economy</th>
<th>Transaction _mode</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>MilliCent</td>
<td>Higher</td>
<td>Better</td>
<td>Off-line</td>
<td>Better</td>
</tr>
<tr>
<td>NetBill</td>
<td>Highest</td>
<td>Good</td>
<td>On-line</td>
<td>Good</td>
</tr>
<tr>
<td>MPTP</td>
<td>high</td>
<td>best</td>
<td>Off-line</td>
<td>Best</td>
</tr>
</tbody>
</table>

- CMPE296U Web Application
Micropayment Protocol

Summary

• Basic micropayment concepts
• 3 existing micropayment protocols
• Cost and security often get trade-off with each other
• Micropayment marketplace does exist
• Future micropayment marketplace

- CMPE296U Web Application