CS 161 – Electronic Commerce

15 November 2006

Stages in E-commerce purchase
Stages in e-commerce purchase

- Advertising
- Solicitation
- Negotiation
- Purchase
- Payment
- Delivery
- Ordering/support

Credit cards as an enabler

- Standard purchase model reveals credit information
- Overhead costs can be high for microtransactions
- Acquiring Bank vs. Consumer Bank
- Payment processors
Why is a credit card transaction 50¢?

Information goods

• Consider the purchase of an information good or service:
  – Library information
  – Search services
  – Software
  – Video clips

• These transactions may be large value or microtransactions

• In either case, atomicity is crucial
What is atomicity?

- I won’t try to give a formal definition
- 3 types of atomicity:

  - **Money atomicity**
    - All money transfers complete with non-ambiguous results
    - Money is neither destroyed nor created
  
  - **Goods atomicity**
    - One receives goods if and only if one pays
    - Example: Cash On Delivery parcels

  - **Certified delivery**
    - Both buyer and seller can prove the delivered content
    - If you get bogus goods, you can prove it
SSL model

- Consumer sends card # direct to merchant
- Similar to today's phone order
- Must trust merchant with card info
- Weak atomicity
- High transaction costs

Third party intermediary (Verisign)

- Protects consumer's card info
- Use Internet for reaching Cybercash gateway to acquirers
- Adds to credit card card cost
Digicash

1. Consumer asks bank for anonymous digicash
2. Bank sends anonymous digicash bits to consumer
3. Consumer sends digicash to merchant in payment
4. Merchant checks that digicash has not been double spent
5. Bank verifies that digicash is valid

Problems
- No atomicity
- Anonymity restricted in US
- Interrupt transaction: ambiguous state
- Detecting double spending is expensive

NetBill goals

- Real service
- Highly atomic transactions
- Micro-transactions
- Full security and privacy
NetBill features

- Focus on info goods/services (journal articles)
- Microtransaction (10¢ purchase: 1¢ overhead)
- Variable pricing
- Fully integrated access control
- DES/RSA/DSA combo for best performance
- Electronic statements & account creation
- Certified delivery: proof of purchase/content

Netbill model

- An electronic credit card to enable network based commerce
- Provides billing services on behalf of network attached merchants.
Netbill protocol

(All messages are encrypted with shared key S)

1 Buyer requests price
2 Seller makes offer
3 Buyer accepts offer
4 Goods delivered encrypted with K
5 Buyer signs EPO (electronic purchase order) <price, crypto-checksum, timeout>
6 Seller countsigns EPO, and signs K
7 NetBill checks account, timeout; stores K & crypto-checksum; transfers price money; sends signed receipt including K
8 K received; goods decrypted

Netbill protocol – low level
Netbill protocol – low level

[Diagram showing the Netbill protocol with labeled steps:]
1. Consumer Application
2. Checkbook
3. Goods
4. Merchant Application
5. Till
6. Approval
7. Transaction Server
8. Check
9. Invoice
Netbill protocol – low level

- Money atomicity
  - Accounts are held at a single server, and are modified with local atomic (ACID) transactions
- Goods atomicity
  - Customer receives decryption key for goods only if she pays
  - If customer pays, decryption key available from multiple sources (merchant and NetBill server)
  - Key can be delivered by alternative network (such as telephone) if necessary
- Certified delivery
  - If customer receives junk or bogus goods, can prove the contents to a judge
  - Crypto checksum of goods (signed by both customer and merchant) are stored at NetBill server
  - Signed copy of decryption key stored by all parties!

Role of Anonymity in EC
Why study anonymity?

- Privacy concerns
  - individual
  - corporate
  - national
- Technology for collecting private statistics
- Understand theoretical limits, countermeasures
- Understanding semi-anonymity
  - Allows government search in exceptional circumstances
- Insights
  - e-commerce
  - distributed protocols
  - cryptography
  - survivability

Anonymous computation

- There is extensive work on anonymous and secret communication (cryptography)
- But what if we want to compute a function of the secure values?
- In puzzle, we want to add “encrypted” values
- Examples:
  - Compute census statistics on usage or population
  - Make an anonymous purchase and then be able to prove that goods were delivered correctly
  - Anonymously auction goods — without revealing any bids (except the winning bid) or bidders
Is anonymous computation feasible?

- Good news:
  - In theory: any computation can be anonymized
- Bad news:
  - In general, constructions are complicated
  - Most constructions multiply number of messages by a factor of at least 1000 (and often, much higher, like $10^{20}$)
  - Usually, simple IP location tracing (traffic analysis) reveals identity of parties
  - Computation requires complex crypto operations.
  - Running times for "simple" anonymous computations are usually measured in days or years.

- So researchers have relied on partial solutions
  - Mixes, pseudonyms, escrow

Mixes

- Use intermediate forwarding agents
- Examples: onion routing, crowds, anonymizer.com, etc.
- Idea simultaneously thought of by several researchers

- Problems:
  - intermediary knows all
  - subject to traffic analysis and statistical analysis
  - can not link old messages to new messages

© 2006 Doug Tygar
Pseudonymous identity

- Establish a consistent, but disguised identity
- Example: mail forwarders
- Can disguise basic facts about identity, but may be traceable from patterns of use
- Once identity is revealed, then all previous uses are traceable

Escrow

- Use pseudonym, but store real identity where law enforcement can find it.
  - Refinement: split identity into multiple parts
  - Store them in different locations
- Depends on procedural mechanisms (e.g. search warrants) for privacy
- Has drawbacks of pseudonym
- Government approach to cryptography
Auction types

- Auctions
  - Allocate scarce resources
  - Proposed to ration Internet bandwidth

- Three types of auctions
  - English auction (price goes up)
    - advantages: encourages "honest" bids
    - disadvantages: slow
      - not private
  - Sealed bid auction
    - advantages: constant time
    - disadvantages: does not encourage "honest" bids, auctioneer knows all
  - Dutch auction (price goes down)
    - advantages: protects privacy
    - disadvantages: slow
      - does not encourage "honest" bids

Vickrey auction

- Vickrey gave a way to combine best features of English auctions and sealed-bid auction

- Second-price auction
  - Highest bidder wins
  - Price is the value of the second highest bid
  - Example: Alice is highest bidder for $100;
    Bob is second highest bidder for $80;
    Alice wins the bid, but pays only $80