CS155b: E-Commerce

Lecture 12: February 22, 2001

C2C Internet Commerce
Remarks on First Hour Exam Blue Books

- “mass market” ≠ “network effects”
- “first-sale rule” ≠ “transfer of copyright”
- “digital signatures” ≠ “entity authentication”
- Signatures and signed documents need not be encrypted
Remaining Topics

- C2C Auctions
- B2B
  - Bob Glushko (Commerce One)
  - Bradley Kuszmaul (Akamai)
- Technology Regulation
  - Matt Blaze (AT&T Labs)
- WWW Searching
- ??? B2C ???
eBay Overview

- World’s largest “online trading community”
- Founded in Sept 1995 by Pierre Omidyar
- IPO in Sept 1998
- Current number of users: Approx. 20M
  (2M end of 1998; 12M middle of 2000)
- Current P/E ratio: 294
eBay Business Model

- Sellers pay small fee (<$2) per listed item.
- eBay takes a cut (~2.5%) of each sale.
- Buyers and sellers handle exchange and payment.
- eBay has no inventory, no transportation, no costs at all except website operation.

Conventional wisdom: Service is technically commoditizable, but strong network effects favor eBay.
Technical Foundations of Internet C2C Commerce

• Market Design (e.g., Auction Types)
• Payment Systems (can’t always use credit cards)
• E-Market Operations
  – Website Design Issues (e.g., UI)
  ★System Reliability and Availability
Auction Types

- Ascending bid structure
- Descending bid structure
- First-price, sealed bid

★ Second-price, sealed bid (Vickrey):
  - Highest bidder gets item
  - Pays second-highest bid price
  - Advantages: “Strategyproof,” user-friendly
“E-Cash” Based on Digital Signatures
Basic Withdrawal of $A

C = Customer
B = Bank

(A, C) → Subtract A from C’s Balance
Generate SN = serial number
Sig ← SIGN((A, SN), SK_B)

((A, SN), Sig) ←
Basic “E-Cash” Protocols, continued

• Spending
  – Customer gives \(((A, SN), \text{Sig})\) to Merchant
  – Merchant runs Verify\(((A, SN), \text{Sig}, PK_B)\)

• Redemption
  – Merchant sends \(((A, SN), \text{Sig})\) to its bank
  – Signature verification and settlement
“Blind Signature” Withdrawal Protocol

Customer

Bank

Generate SN

Z ← BlFn(A, SN)

(C, A, Z)

Subtract A from C’s Balance

BlSig ← SIGN(Z, SK_B)

(C, A, Z)

Sig ← BlFn⁻¹(BlSig)

(Z, BlSig)

Important Properties:

• Sig is a valid signature of (A, SN)
• C is “unlinkable” to SN during redemption

Mathematical idea: “random-self-reducibility”
“Other E-Cash” Desiderata

- Prevent “Double-spending”
- Detect double spending before redemption
- “Transferability”

Extensive body of good research.

Many protocols, trade-offs, lower bounds.

Decades of hope, work, and investment by cryptologic research community.
C2C Payment Reality

- Elegant “e-cash” technology not used.
- No-tech “solution”: PayPal

Discussion Point: When do no-tech solutions win? When should they?
Assignments for Week of February 26, 2001

Reading: Chapter 8 of Information Rules.

Written Homework: HW3 due in class on March 1, 2001.