Electronic Commerce

- how to buy and sell things on-line
- point-of-sale technology
  - phone cards, electronic (unforgeable) plane tickets, subway tokens, etc.
- issues
  - privacy
  - preventing fraud
  - lowering cost

Traditional Commerce: Cash

- anonymous
- low fraud
- prone to loss or theft
- best for small purchases
- in some places and times, held in large quantities

Traditional Commerce: Checks

- not anonymous
- prone to fraud
- used mostly for small purchases
- cashier's check
  - cumbersome, but fixes most problems with checks

Credit Cards

- not anonymous
- fraud-prone, but complex countermeasures
- combines payment method with borrowing
  - focus here on payment
- two modes of use
  - pay in person, with signature
  - pay remotely, with number only

Fraud Tolerance

- fraud costs borne by parties that can best detect and fight fraud
  - economic decision to tolerate a certain level of fraud
  - consumer covers first $50 of fraud
  - bank covers remaining fraud cost
  - merchant accepting sale without signature covers loss if card was bogus or stolen

Controlling Fraud

- on-line checking of cards against list of bad card numbers
  - works well in U.S. because phone system is very cheap and reliable
- on-line AI monitoring of usage patterns
- when buying with number only, ship only to billing address
- cost/benefit analysis of new fraud prevention technology

Sources of Fraud

- how criminals get card numbers
  - dishonest merchant employees
  - dumpster diving
  - mail interception
  - theft of cards and merchant records
  - make up phony numbers
- how criminals use card numbers
  - make new cards (rare)
  - buy stuff over the phone

Debit Cards

- like credit card, except
  - bank gets consumer's money earlier
  - no $50 liability limit for consumers
    - » some issuers voluntarily provide $50 limit
  - sometimes protected by crypto
    - » PIN numbers

Goals of Electronic Commerce

- what everyone wants
  - monitor and control fraud
  - reduce transaction costs
  - allow fast, remote purchasing
- consumers want anonymity
- banks want interest on the "float"
- merchants want useful data about consumers

Credit Cards and SSL

- simple approach
  - use browser's secure-connection support to connect consumer and merchant
  - mimic ordering by phone
- works well for selling a physical good for delivery by snail-mail
  - really no different than phone purchase

Credit Cards and SSL

- problems if delivering product electronically
  - no time to check
- still prone to merchant-side fraud
- still prone to number-stealing on client side

Credit Cards and SET

- SET (Secure Electronic Transaction) protocol pushed by credit card companies
- main effect: merchant learns consumer's number is valid, but doesn't learn the number
- very complicated specification
- current implementations don't interoperate
- future of SET: uncertain

Smart Cards

- tamper-resistant device that looks like a credit card
- software and state implanted by bank or credit card company
- uses cryptography to talk to point-of-sale terminals
- very popular in Europe, starting to spread elsewhere

Smart-Card Characteristics

- hardly any memory: 32k ROM, 16k non-volatile RAM, 16k RAM typical
- small, cheap, low-power processor
- (sometimes) dedicated crypto hardware
- gets power from terminal
- costs a few dollars to manufacture
  - in quantity
- moderately tamper-resistant

Smart Credit Cards

- card has private key built in
- card has encrypted/signed conversation with credit card company server to verify its identity
  - might use challenge/response
  - might need consumer's PIN number to derive private key
- to commit fraud, must steal card or learn private key

Stored-Value Cards

- cash value is stored in the card itself
  - value usually low
- card programmed to limit its own spending
- card authenticates itself off-line to terminal
- if you lose the card, tough luck
- many uses
  - phone card (common in Europe)
  - subway fare (Metrocard in NYC)

Anonymity and Fraud

- stored-value cards could be anonymous
  - no matching of card to owner
  - no matching of card to transactions
- but anonymity invites fraud
  - no way to stop dishonest card-issuer employee from making his own free cards
  - adversary who learns one card's private key can clone it infinitely
- records needed to reduce fraud

Anonymity and the Law

- anonymous money transfer seriously hurts law enforcement
- can't "follow the money"
  - tax evasion
  - money laundering
  - bribery and campaign finance
  - for-profit crime in general
- government probably won't allow truly anonymous money

Case Study: Subway Tokens

- assume
  - allow trips cost $1
  - consumer buys $20 card
  - throw away card when it's used up
  - worried about fraud by
    - » card manufacturers and sellers
    - » payment-collection terminals
    - » card holders

Strategy

- divide cards into groups
- each group has a secret key
  - known only to cards in group, and issuer
- card knows how much value it stores
- to spend a token, card tells terminal a cryptographic fact
  - token presents fact to issuer to prove that a purchase was made

Crypto Trick: Hash Chains

- use a one-way function H(x)
  - example: SHA-1 cryptographic hash
- choose x_0 arbitrarily
- define $x_{i+1} = H(x_i)$

Using Hash Chains

- initially, tell the card x_0, terminal x_{1000}
- on use of card
  - terminal tells card i, x_i
  - card responds with x_{i-1}
- if a terminal knows x_k, then 1000-k units were spent at that terminal

Practical Details

- initially, tell terminal a "terminal code" T
  - different for each terminal
- hash chain defined by $x_0 = H(\text{secret} + T)$
- when terminal gets to end of hash chain, call redemption center and get a new one
- protocol enhanced to pass T to card

Card Groups

- divide cards into groups
  - each group has a different secret
- track sales and redemptions by group
  - if there's too much fraud in a group, cancel the group
    - » customers can redeem their cancelled cards
  - associate groups with card vendors
- terminal has separate hash chain per group

Analysis

- protocol uses only hashing, no encryption
- terminals cryptographically prevented from cheating
- card-holders can cheat only by stealing cards or tampering with cards
- per-group tracking puts upper bound on loss due to compromise of one group

Smart Card Applications

- credit card
- stored value
- loyalty card
- multi-function cards?
  - who controls card space?
  - interactions between hostile functions
  - many other issues

Micropayment Systems

- current e-commerce has high per-transaction costs
  - crypto uses computer power
  - storage and on-line availability requirements
- micropayment systems try to lower costs for low-value transactions
  - lower incentive to commit fraud, so fewer countermeasures required
- pay-per-view web pages

Cost Analysis for Merchant

- cost of fast, networked machine, including software, support, and maintenance: $300,000 per year = 1 cent per second
- handling costs can be 2% of transaction
  - must handle 50 cents per second
- peak load is 10 times average
  - must be able to handle $5 per second
- can do 10 RSA encryptions per second
  - minimum transaction is 50 cents

Micropayment Strategies

- drop features
  - anonymity
  - receipts and paper trail
  - a universal currency
  - strong fraud detection
- approaches
  - weaker crypto
  - lottery methods

Electronic Commerce Summary

- many alternatives
- many legal issues unresolved
- for Web commerce, insecurity of client machines is a big problem
- e-commerce is going to happen anyway