

Electronic Payment Systems

ISA 767, Secure Electronic Commerce
Mar. 30, 2005
Jaehong Park, jpark2@gmu.edu
George Mason University

References

- K. Laudon, and C. Traver, E-Commerce: Business, Technology, Society, Second Edition, Addison Wesley, 2003
- Warwick Ford and Michael Baum, Secure Electronic Commerce, 2nd ed. Prentice-Hall, 2000
- William Stallings, Network Security Essentials, Prentice-Hall, 2000
- Witold Stabla, Electronic Payment Systems, online document.
- N. Asokan et. al., The State of the Art in Electronic Payment Systems, IEEE Computer., Sep. 1997.

© Jaehong Park 2005

2

Generic Payment Systems

- Cash
- Checking transfer
- Credit Card
- Stored Value
- Accumulating Balance Payment System

© Jaehong Park 2005

3

Cash

- Instantly convertible to other forms of value w/o intermediation of any other institution
- Portable, no authentication, micropayment-usable
- Free transaction fee
- No hardware or account is required
- Anonymous and untraceable
- Only for smaller transactions
- Easily stolen, no float (time gap between purchase and actual payment)
- Cash purchase is likely to be final and irreversible

© Jaehong Park 2005

4

Checking transfer

- Funds are transferred directly via a signed draft or check from a consumer's checking account to a merchant or other individual
- Second most common form of payment in terms of number of transactions, most common in terms of total amount spent
- For both small and large transactions
- Not for micropayment
- Some float
- Not anonymous, need third-party institutions
- Security risk for merchants, hence authentication is required
- Ensured checks (closer to cash) reduce this risk

© Jaehong Park 2005

5

Credit Card

- Credit card association (visa, mastercard), issuing banks, clearinghouses
- Reduce the risk of theft, increase consumer convenience
- Merchant's fee, increased consumer spending
- Federal Regulation Z places the risks of transaction on the merchant and credit card issuing bank

© Jaehong Park 2005

6

Stored Value

- Account created by depositing funds into an account and from which funds are paid out or withdrawn as needed
- Similar to checking transfer except writing a check
- E.g., debit cards, gift certificates, prepaid cards
- No protection by regulation Z
- P2P payment system like PayPal is a variation of stored value.
 - No prepayment requirement
 - Requires account with stored value (either checking account or credit card)

© Jaehong Park 2005

7

Accumulating Balance Payment Systems

- Accounts with accumulating expenditures and periodic payments
- E.g., utility account, phone account, Amex accounts

© Jaehong Park 2005

8

E-Payment

- Participants
 - At least, payer (client, consumer), payee (merchant), financial institutions (issuer and acquirer)
 - Optionally, payment gateway and CAs
- Flow of money from the payer via the financial institutions to payee
- Direct payment vs. Indirect payment
 - Direct payment: interaction between payer and payee
 - Indirect payment: no interaction between them (e.g., Electronic fund transfer)

© Jaehong Park 2005

9

E-Payment

- Three categories **by the money transfer time**
 - **Pay-in-advance system**
 - A certain amount of money is taken away from the payer before purchase is made
 - E.g., smart card-based e-purse, e-cash, certified check
 - **Pay-now system**
 - Online debit card
 - **Pay-later system**
 - Online credit card, digital checking transfer

© Jaehong Park 2005

10

E-payment Requirements

- Security
 - Identification, authentication, authorization, confidentiality, integrity, availability, reliability, non-repudiation, etc.
- Interoperability (standardization)
- Large number of client/merchant involved
- Traceability vs. Untraceability
- Simplicity
- Flexibility
- Anonymity
- Cheapness
- Productivity
- Reliability
- Scalability

© Jaehong Park 2005

11

Technologies (or Mechanisms)

- Cryptography
- Trusted hardware/software
- Secure communication in open network such as Internet
- Digital certificates
- Public Key Infrastructure (CAs)

© Jaehong Park 2005

12

Digital Wallet

- **Functions**
 - To secure the payment process from consumer to merchant
 - To authenticate the consumer using digital certificate
 - To store and transfer value from consumer to merchant
- **Advantage**
 - Convenience (easy checkout)
 - Reduction of risk of fraud and the use of stolen cards
 - Lower transaction costs
- **Obstacle**
 - Need to be widespread
 - Fear on privacy
 - Eliminating repudiation
- **Client-based vs. server-based digital wallet**
 - Gator.com vs. MSN Wallet

© Jaehong Park 2005

13

E-Payment Systems

- Electronic Check
- Payment Card
- Electronic Money

© Jaehong Park 2005

14

Electronic Check

- Clearing between payer and payee is based on existing banking settlement system
- Dematerialization of payment instrument is passed on via computer networks like Internet.
- Examples
 - Simple: individual payment to settle accounts at online auction sites
 - Sophisticated: Treasury Department to transfer billions of dollars electronically.
- Advantages
 - no need to reveal account info to other individuals
 - Less expensive than credit cards for merchants
 - Faster than paper check
- Achex (now Western Union's MoneyZap), eCheck

© Jaehong Park 2005

15

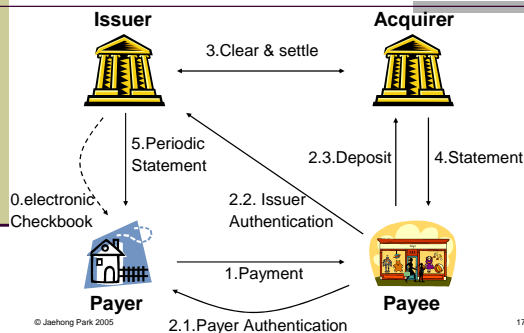
eCheck by FSTC

- Founded in 1998 by Financial Services Technology Consortium (FSTC) of 15 banks, gov. agencies, and tech. companies
- Use of hardware based e checkbook (PCMCIA card reader, Smartcard, etc.)
- E checkbook
 - Consumer's digital signature in the form of a private key
 - Issuer's public key

© Jaehong Park 2005

16

eCheck Payment System



© Jaehong Park 2005

17

eCheck Discussion

- Requirements
 - User email account
 - Must possess the necessary security hardware (smartcard, PCMCIA card reader, etc.)
 - Need a bank account that offers e-check services
- Advantages
 - Low cost of check handling
 - Unforgiving for simple errors
 - Various checks can be written (traveler's, certified)
- Disadvantage
 - Slow user adaptation
 - Only a bank can be drawee
 - Lack of anonymity
 - Additional intermediary costs

© Jaehong Park 2005

18

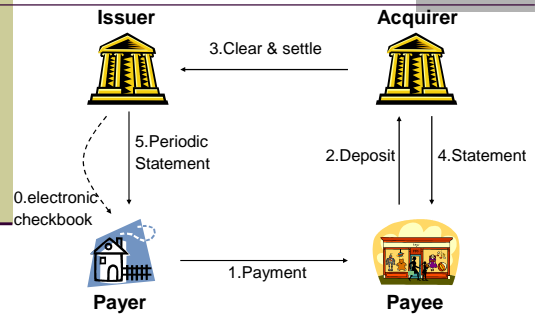
Variation of eCheck payment scenarios

- Deposit-and-clear
 - All parties need to have necessary infra.
- Cash-and-transfer
 - Payee bank is unable to process eCheck
- Lockbox
 - Payee is unable to receive eCheck
 - Lockbox is used on behalf of payee
- Transfer order
 - Neither payee nor his bank is able to process eCheck

© Jaehong Park 2005

19

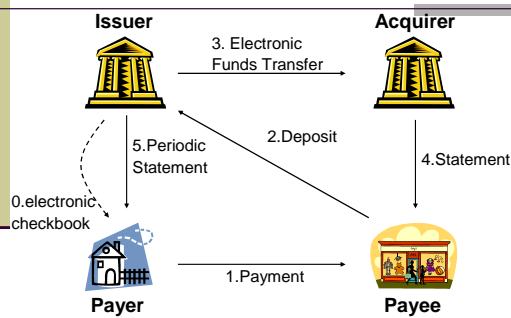
eCheck: Deposit-and-Clear Scenario



© Jaehong Park 2005

20

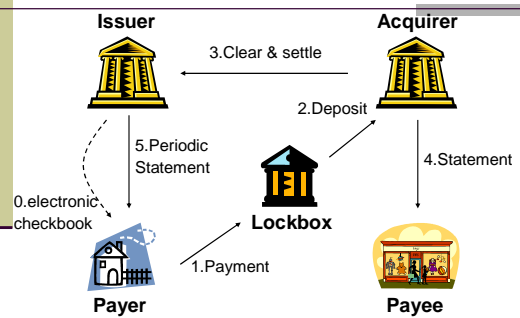
eCheck: Cash-and-Transfer Scenario



© Jaehong Park 2005

21

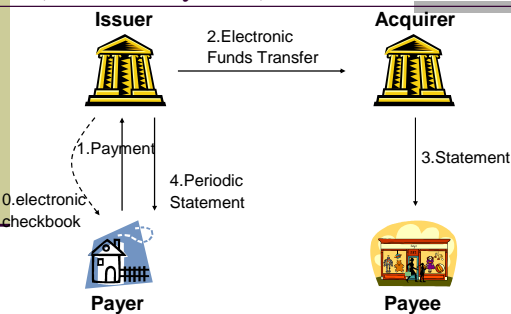
eCheck: Lockbox Scenario



© Jaehong Park 2005

22

eCheck: Transfer Order Scenario (Indirect Payment)



© Jaehong Park 2005

23

Online Credit Card Payment Systems

- Close to MOTO (mail order telephone order)
 - Card not present (CNP) transaction
 - No hand signed agreement
 - Customer repudiation problem
- Not for small transactions
 - Merchant costs (3% of purchase + transaction fee of 20 to 30 cents + other setup fees).
 - One solution is to charge in the aggregate (Micropayment)
- Not for everybody

© Jaehong Park 2005

24

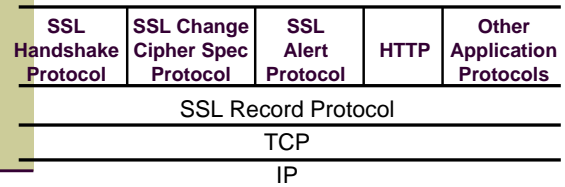
Online Credit Card Payment Systems

- Threats on the transmission of the card number over open networks like Internet
 - Eavesdropping
 - Tampering
 - Impersonating
- Two approaches
 - Securing communication protocols
 - E.g., SSL (Secure Socket Layer)
 - Securing payment protocols
 - E.g., SET (Secure Electronic Transaction)

© Jaehong Park 2005

25

Secure Socket Layer (SSL) Architecture

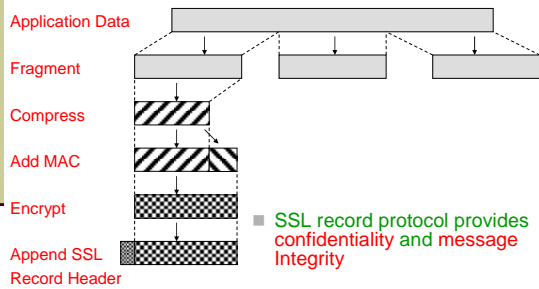


- SSL record protocol provides basic security services to various higher-layer protocols
- Three higher layer protocols are defined as part of SSL

© Jaehong Park 2005

26

SSL Record Protocol



© Jaehong Park 2005

27

SSL Handshake Protocol

- A series of message exchanges by client and server
- Allows server and client
 - to authenticate each other and
 - to negotiate an encryption and MAC algorithm and cryptographic keys
- Used before any application data are transmitted

© Jaehong Park 2005

28

SSL Session

- SSL session created/negotiated by handshake protocol
 - session ID
 - chosen by server
 - X.509 public-key certificate of peer
 - possibly null
 - compression algorithm
 - cipher spec
 - encryption algorithm
 - message digest algorithm
 - master secret
 - 48 byte shared secret
 - is resumable flag
 - can be used to initiate new connections

© Jaehong Park 2005

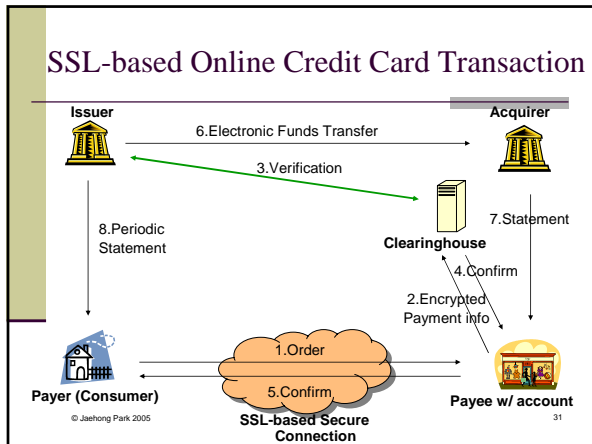
29

SSL Services

- Peer entity authentication
- Data confidentiality
- Data authentication and integrity
- Compression/decompression
- Generation/distribution of session keys
 - integrated into protocol
- Security parameter negotiation
 - Cipher suite (key exchange method and cipher spec), compression algorithm

© Jaehong Park 2005

30

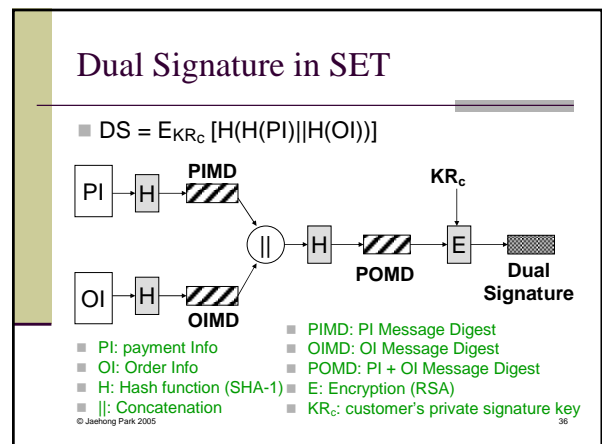


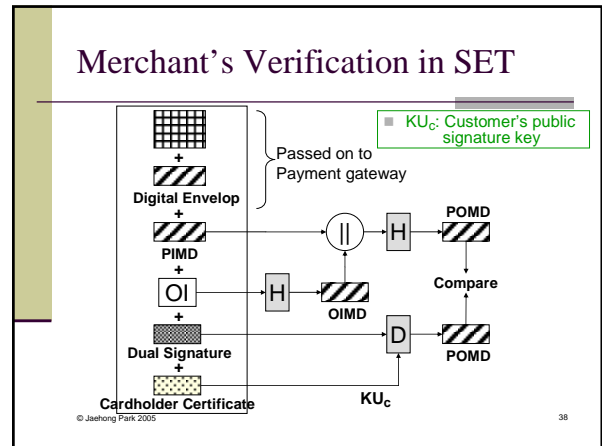
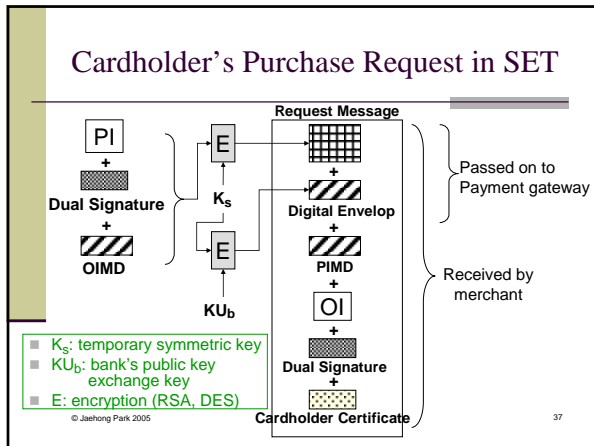
- ### Secure Electronic Transaction (SET)
- Designed to protect credit card transactions on Internet by MasterCard and Visa in 1996
 - Not a payment system
 - A set of security protocols and formats that enables users to employ the existing credit card payment system on Internet in a secure manner
 - Services
 - Provide a secure communications channel among involved parties
 - Provide trust by the use of X.509v3 digital certificate
 - Ensures privacy
 - Facts
 - 3 books, a total of 971 pages of specifications (compare to 63 pages of SSLv3 and 71 pages of TLS)
- © Jaehong Park 2005 32

- ### Key Features of SET
- Confidentiality of cardholder account and payment information
 - DES
 - Integrity of payment information
 - RSA digital signature, SHA-1 hash codes
 - Cardholder account authentication
 - X.509v3 digital certificates with RSA signatures
 - Merchant authentication
 - X.509v3 digital certificates with RSA signatures
- © Jaehong Park 2005 33

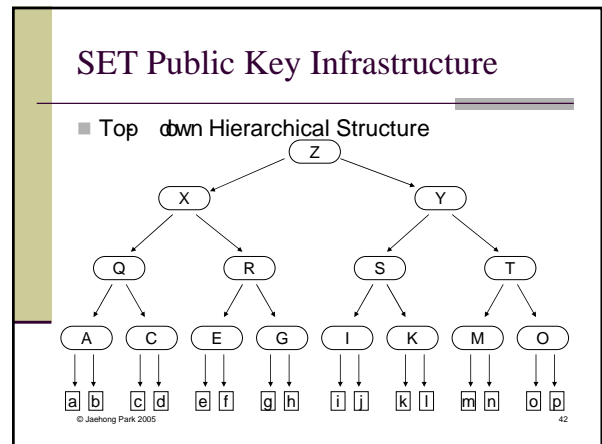
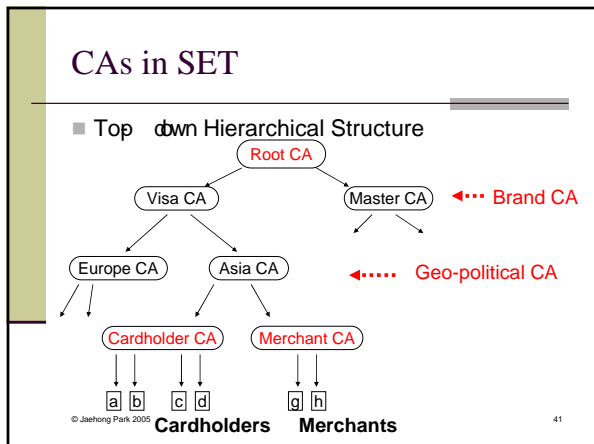
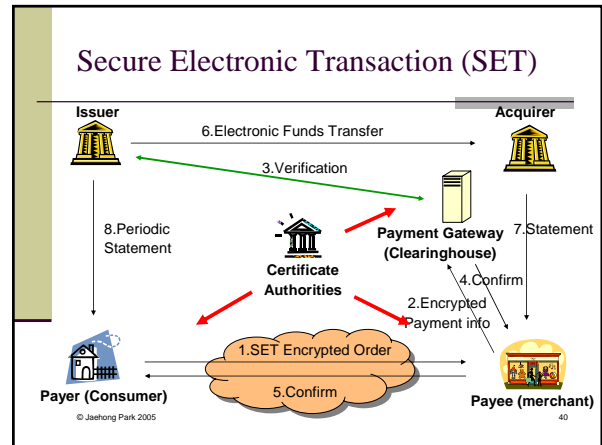
- ### SET Participants
- Cardholder (payer, customer, purchaser)
 - Merchant (payee, service provider)
 - Issuer (payer's card issuing bank)
 - Acquirer (payee's bank)
 - Payment Gateway
 - A function operated by either acquirer or designated third-party that processes merchant payment message
 - Interface between SET and existing credit card network
 - Internet connection to merchant, direct connection to acquirer
 - Certificate Authority
 - Issue certificates for cardholders, merchants, and payment gateways
- © Jaehong Park 2005 34

- ### Dual Signature in SET
- Designed to link two messages that are intended for two different recipients
 - Order Information (OI) to the merchant
 - Payment Information (PI) to the bank
 - Privacy protection by keeping two messages separate
 - Two messages must be linkable
- © Jaehong Park 2005 35



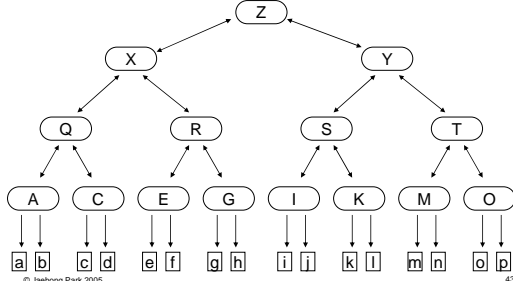


- ### Payment Authorization
- Between merchant and payment gateway
 - Authorization request
 - Purchase info (received from cardholder)
 - Authorization-related info
 - Transaction ID signed with merchant's private signature key and encrypted with a one-time symmetric key generated by merchant
 - A digital envelope: one-time key encrypted with payment gateway's public key-exchange key
 - Cardholder signature key certificate, merchant signature key certificate, merchant key-exchange certificate
- © Jaehong Park 2005 39



PKI- Other Structures

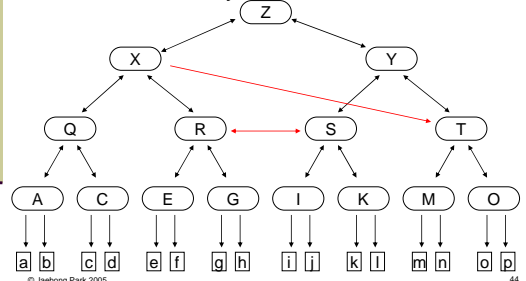
General Hierarchical Structure



© Jaehong Park 2005 43

PKI- Other Structures

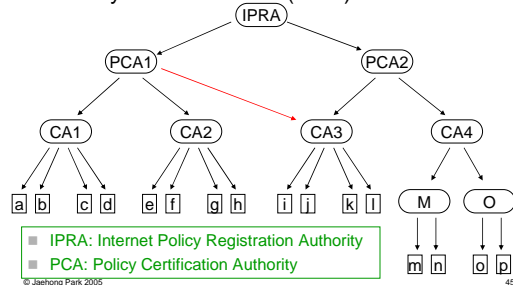
General Hierarchy w/ Additional Links



© Jaehong Park 2005 44

PKI- Other Structures

Privacy Enhanced Mail (PEM) Structure



- IPRA: Internet Policy Registration Authority
- PCA: Policy Certification Authority

© Jaehong Park 2005 45

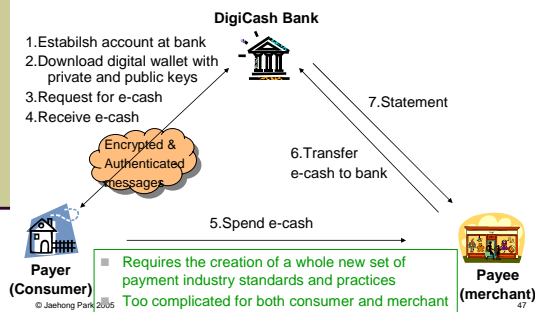
E-Money or Digital Dash

Cash vs. Digital Cash

- Cash
 - Legal tender (currency) by national authority
 - Instantly convertible to other value forms,
 - no intermediary
- Digital Cash
 - Misnomer
 - No legal tender by government exists
 - Limited convertibility
 - Requires intermediaries to convert
 - Some survived in P2P payment systems

© Jaehong Park 2005 46

Original DigiCash – not successful

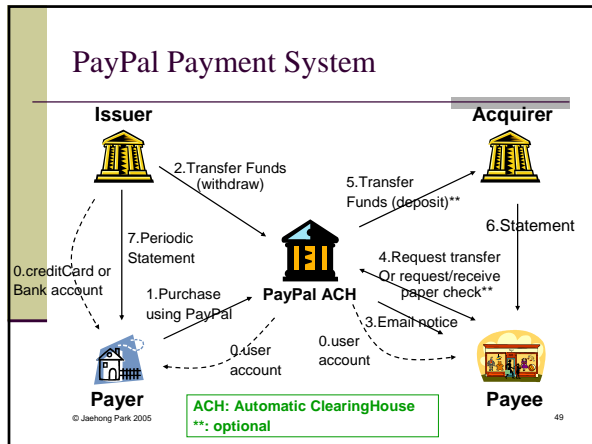


© Jaehong Park 2005 47

P2P Payment Systems

- The growth of eBay → PayPal
 - Millions of peer to peer e-commerce
 - A demand for e-payment services
 - A demand of micropayment services
- PayPal as a form of cash
 - Limitation
 - Need intermediary
 - Payment can be accepted only by people with email account
 - Nevertheless, it has a cash-like quality
 - Other similar services
 - Yahoo's PayDirect, AOL's QuickCash, etc.

© Jaehong Park 2005 48



- ### PayPal Payment System
- Provide **convenience for individual fund transfer** (compare to mailing check/MO)
 - Payment system **for small business** who cannot afford credit card payment system
 - No need to have merchant's account
 - Simple system using existing credit card and checking payment systems
 - The more people use, the greater the benefit to the user
 - Facts (2003)
 - 17 million accounts, \$5 billion in transactions per year
 - Now owned by eBay (acquired at \$1.5 billion in 2002)
 - Revenue model
 - Seller pays transaction fee of 3% of the transaction
 - Collecting interests on consumer funds in PayPal system₅₀
- © Jaehong Park 2005

- ### M (mobile) –Payment System
- **E** Payment using wireless and mobile devices such as cell phone.
 - Accumulating Balance Payment System
 - More popular in Western Europe and Asia, less popular in US
- © Jaehong Park 2005
- 51