امنیت تجارت الکترونیکی

محمد مهدی گیلانیان صادقی
دانشگاه آزاد اسلامی قزوین

Electronic Payment Systems

- An introduction to electronic commerce and electronic payment systems
- An overview of the payment instruments
- To discusses the major issues of electronic payment security

Electronic Commerce

- E-commerce can be defined as any transaction involving some exchange of value over a communication network.
- This broad definition includes
  - Business-to-business transactions, such as EDI (electronic data interchange)
  - Customer-to-business transactions, such as online shops on the Web
  - Customer-to-customer transactions, such as transfer of value between electronic wallets
  - Customers/businesses-to-public administration transactions, such as filing of electronic tax returns

Electronic Commerce (2)

- Business-to-business transactions are usually referred to as **e-business**
- Customer-to-bank transactions are as **e-banking**
- Transactions involving public administration as **e-government**

Electronic Commerce (3)

- A communication network for e-commerce can be a private network (such as an interbank), an intranet, the Internet, or even a mobile telephone network
- The focus is on customer-to-business transactions over the Internet and on the electronic payment systems that provide a secure way to exchange value between customers and businesses

Requirements for e-payments

- Atomicity
  - Money is not lost or created during a transfer
- Good atomicity
  - Money and good are exchanged atomically
- Non-repudiation
  - No party can deny its role in the transaction
  - Digital signatures

Electronic Payment Systems

- Electronic payment systems have evolved from traditional payment systems
- Electronic payment systems are much more powerful, however, especially because of the advanced security techniques that have no analogs in traditional payment systems.
- An electronic payment system in general denotes any kind of network (e.g., Internet) service that includes the exchange of money for goods or services
- The goods can be physical goods, such as books or CDs, or electronic goods, such as electronic documents, images, or music

Electronic Payment Systems (2)

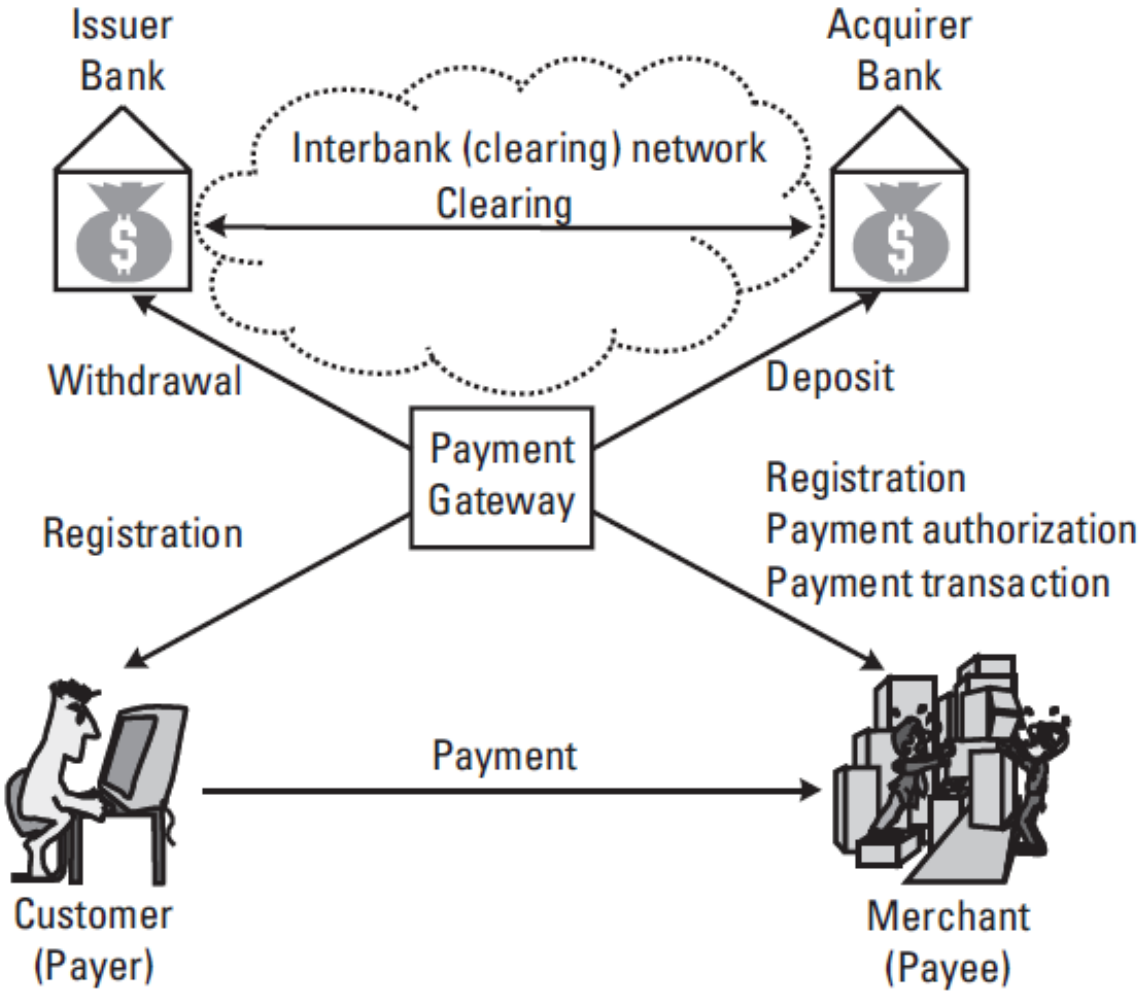

Figure 4.1 A typical electronic payment system.

Electronic Payment Systems (3)

- Electronic Payment Systems divides into three parts:
  - Off-line Versus Online
  - Debit Versus Credit
  - Macro Versus Micro

Off-line Versus Online

- **Off-line system:** a payer and a payee are online to each other during a payment transaction, but they have no electronic connection to their respective banks.
- The payee has no possibility to request an authorization from the issuer bank (via the payment gateway), so he cannot be sure that he is really going to receive his money.
- Without an authorization, it is difficult to prevent a payer from spending more money than he actually possesses.

Off-line Versus Online (2)

- **Online system:** requires the online presence of an authorization server, which can be a part of the issuer or the acquirer bank
- Clearly, an online system requires more communication, but it is more secure than off-line systems
- Most proposed Internet payment systems are online

Debit Versus Credit

- An electronic payment system can be **credit based** or **debit based**
- In a *credit based system* (e.g., credit cards) the charges are posted to the payer's account. The payer later pays the accumulated amounts to the payment service
- In a *debit based system* (e.g., debit cards, checks) the payer's account is debited immediately, that is, as soon as the transaction is processed

Macro Versus Micro

- An electronic payment system in which relatively large amounts of money can be exchanged is usually referred to as a **macropayment** system
- An electronic payment system which is designed for small payments (e.g., up to 5 euros), it is called a **micropayment** system

Payment Instruments

- Payment instruments are any means of payment
- Traditional payment instruments: Paper money, credit cards and checks
- Electronic payment systems have introduced two new payment instruments: *electronic money* (also called digital money) and *electronic checks*
- Payment instruments can in general be divided into two main groups: *cash-like* payment systems and *check-like* payment systems

Payment Instruments (2)

- **A cash-like system:** The payer withdraws a certain amount of money (e.g., paper money, electronic money) from his account and uses that money whenever he wants to make a payment
- **In a check-like system:** the money stays in the payer's account until a purchase is made. The payer sends a payment order to the payee, on the basis of which the money will be withdrawn from the payer's account and deposited in the payee's account. The payment order can be a piece of paper (e.g., a bank-transfer slip) or an electronic document (e.g., an electronic check)

Payment Instruments-Credit cards

- The first credit cards were introduced decades ago (Diner's Club in 1949, American Express in 1958)
- For a long time, credit cards have been produced with magnetic stripes containing unencrypted, read-only information. Today, more and more cards are "smart cards" containing hardware devices (chips) offering encryption and far greater storage capacity

Payment Instruments-Credit cards

- The next Figure illustrates a typical payment transaction with a credit card as the payment instrument
- The customer gives his credit card information (i.e., issuer, expiry date, number) to the merchant (1). The merchant asks the acquirer bank for authorization (2)
- The acquirer bank sends a message over the interbank network to the issuer bank asking for authorization (3). The issuer bank sends an authorization response (3)
- If the response is positive, the acquirer bank notifies the merchant that the charge has been approved. Now the merchant can send the ordered goods or services to the customer (4), and then present the charge (or a batch of charges representing several transactions) to the acquirer bank (5 up)
- The acquirer bank sends a settlement request to the issuer bank (6 to the left). The issuer bank places the money into an interbank settlement account (6 to the right) and charges the amount of sale to the customer's credit card account.
- At regular intervals (e.g., monthly) the issuer bank notifies the customer of the transactions and their accumulated charges (7).

Payment Instruments-Credit cards

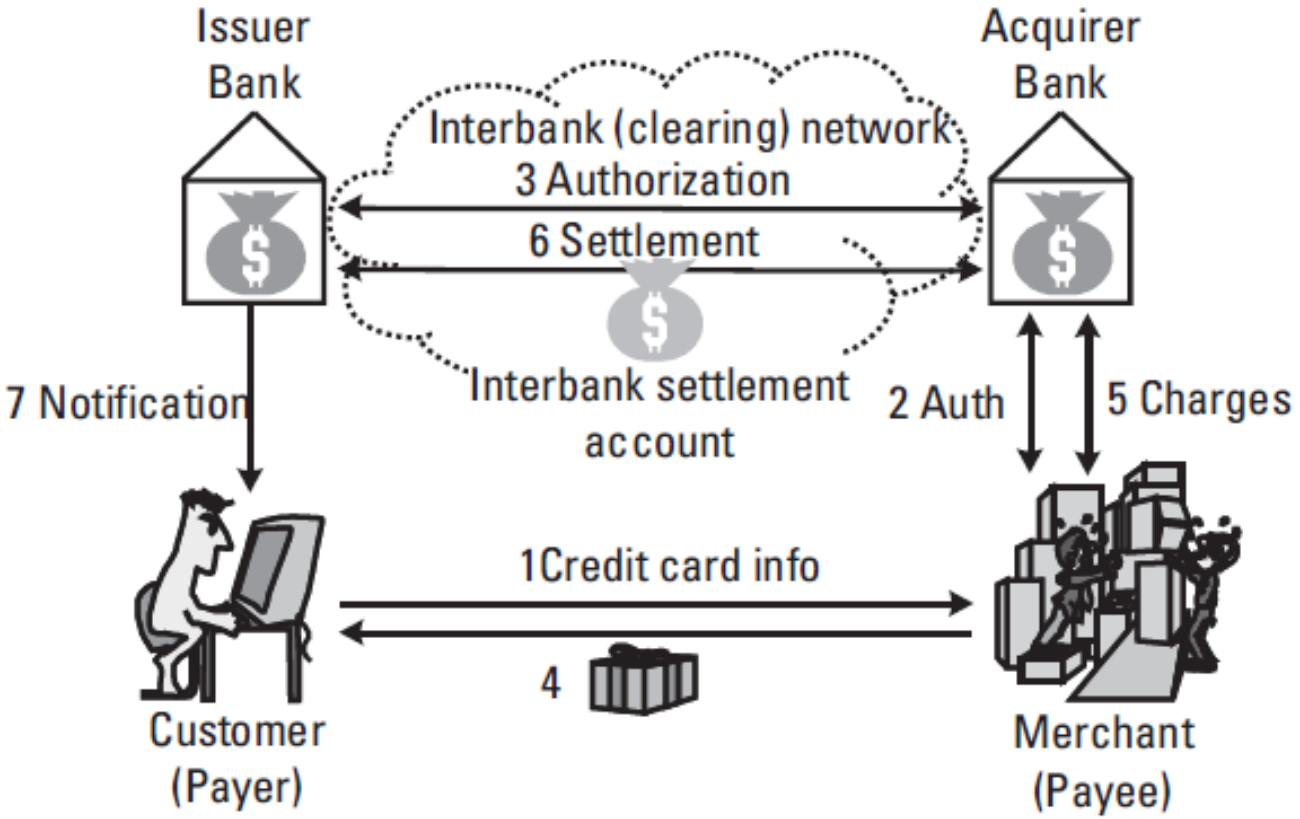

Figure 4.2 A credit card payment transaction.

The credit card numbers can steal by *eavesdroppers* and *dishonest merchants*

Payment Instruments-Electronic Money

- Electronic money is the electronic representation of traditional money
- A unit of electronic money is usually referred to as an *electronic* or *digital coin*
- For the following discussion, the actual value of a digital coin in units of traditional money is irrelevant. Digital coins are ‘minted’ (i.e., generated) by brokers
- The next Figure illustrates a typical electronic money transaction

Payment Instruments-Electronic Money

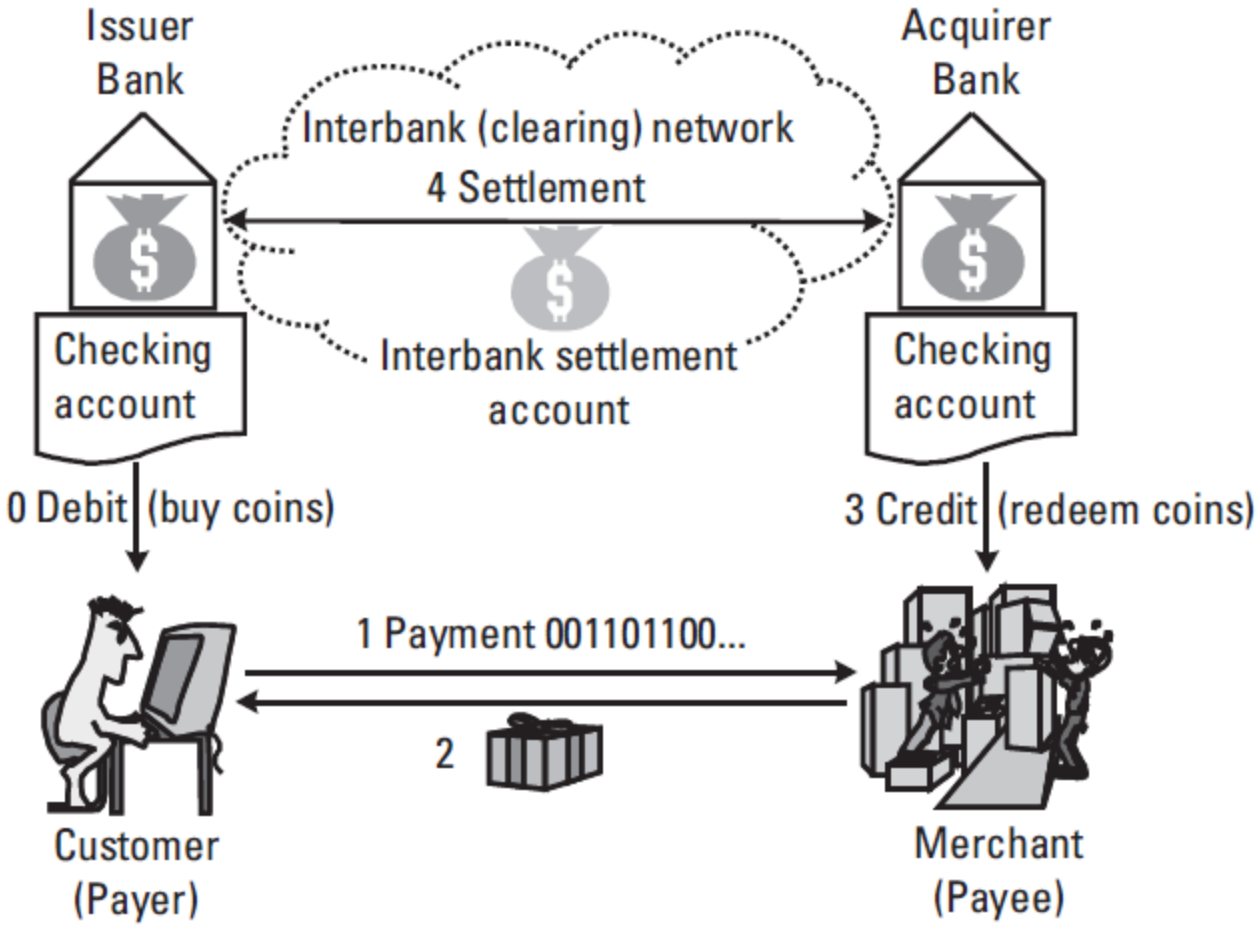

Figure 4.3 An electronic money payment transaction.

Payment Instruments-Electronic Check

- Electronic checks are electronic equivalents of traditional paper checks. An electronic check is an electronic document containing the following data:
  - Check number
  - Payer's name
  - Payer's account number and bank name
  - Payee's name
  - Amount to be paid
  - Currency unit used
  - Expiration date
  - Payer's electronic signature
  - Payee's electronic endorsement
- A typical payment transaction involving electronic checks is shown in the next Figure

Payment Instruments-Electronic Check

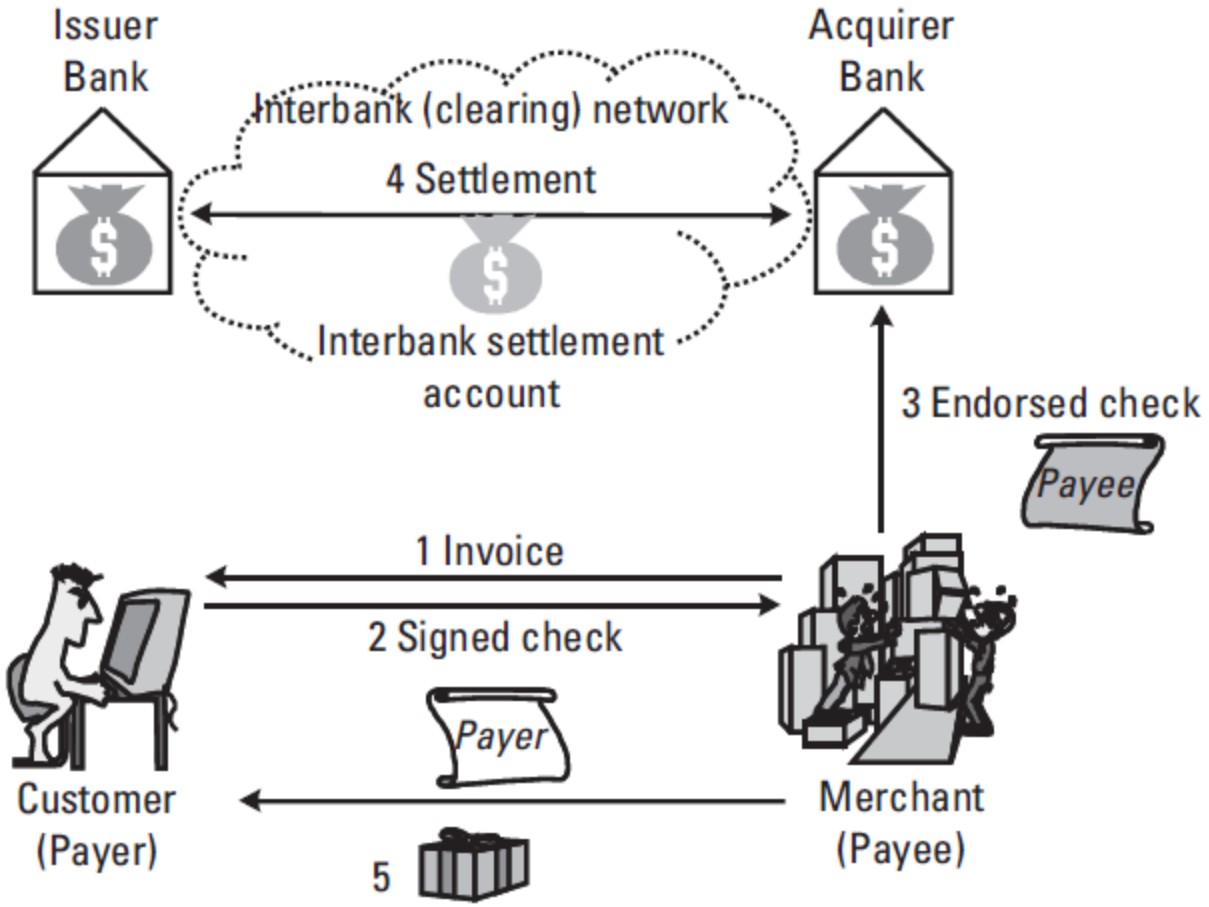

Figure 4.4 An electronic check payment transaction.

Payment Instruments-Electronic Wallet

- Electronic wallets are stored-value software or hardware devices
- They can be loaded with specific value either by increasing a currency counter or by storing bit strings representing electronic coins.
- The current technology trend is to produce electronic wallets in the smart card technology.
- Electronic money can be loaded into the wallets online and used for payments at point-of-sale (POS) terminals
- An electronic wallet: yahoo wallet

Payment Instruments-Smart Cards

- A smart card is a plastic card with an embedded microprocessor and memory
- Similar to electronic wallets, it introduces an additional piece of hardware and also a communication node into the payment system
- From the point of view of payment semantics, smart cards represent a technology, not a new payment instrument. In other words, a smart card can be used as either a credit card or a storage of electronic money or an electronic check device, or a combination of these

Assignment

Describe the following payment instruments?

- Mondex
- PayPal
- Agile Wallet
- eWallet
- Microsoft Wallet

Electronic Payment Security

- The security problems of traditional payment systems are well known:
  - Money can be counterfeited
  - Signatures can be forged
  - Checks can bounce
- Electronic payment systems have the same problems as traditional systems, and more:
  - Digital documents can be copied perfectly and arbitrarily often;
  - Digital signatures can be produced by anybody who knows the private key;
  - A payer's identity can be associated with every payment transaction.

Electronic Payment Security (2)

- In an electronic payment system, three types of adversaries can be encountered:
  - Outsiders eavesdropping on the communication line and misusing the collected data (e.g., credit card numbers)
  - Active attackers sending forged messages to authorized payment system participants in order either to prevent the system from functioning or to steal the assets exchanged (e.g., goods, money)
  - Dishonest payment system participants trying to obtain and misuse payment transaction data that they are not authorized to see or use

Electronic Payment Security (3)

- The basic security requirements for electronic payment systems can be summarized as:
  - Payment authentication
  - Payment integrity
  - Payment authorization
  - Payment confidentiality

Electronic Payment Security (4)

- **Payment authentication** implies that both payers and payees must prove their payment identities, which are not necessarily identical to their true identities
- **Payment integrity** requires that payment transaction data cannot be modifiable by unauthorized principals. Payment transaction data includes the payer's identity, the payee's identity, the content of the purchase, the amount, and possibly other information

Electronic Payment Security (5)

- **Payment authorization** ensures that no money can be taken from a customer's account or smart card without his explicit permission. It also means that the explicitly allowed amount can be withdrawn by the authorized principal only (access control)
- **Payment confidentiality** covers confidentiality of one or more pieces of payment transaction data. In the simplest case it can be achieved by using one of the communication confidentiality mechanisms

Summary

- Electronic Payment Systems
- Payment Instruments
- Electronic Payment Security