|  |
| --- |
| **The Design and Implementation of Secure Transaction in iPay** |
|  |
|  |
| Team: popcorn |
|  |
| **Jianjun Liang** |
| **2011/9/1** |
|  |

# summary&introduction

## summary

Safety is an important part of e-commerce, and a good secure trading scheme ensures efficient and secure electronic transactions. At present, the mainstream of relevant security technologies has SET and SSL. SSl protocol is simpler, but there are some security risks; while the SET protocol has high safety, but it is more expensive to achieve them. Regardless of which technology to use, we should refer to the specific circumstances of the system, customize suitable safety program for the system. Ipay payment system references these two protocols, considering the actual situation (such as technical difficulties, development time, and hardware performance), designs and implements a secure trading system.

## introduction

Design of secure transactions involves the password hash algorithm, data encryption algorithms and asymmetric encryption algorithms and other techniques. Referring to SET and SSL protocols, we call the java class library that comes with part of the security library to implement secure payment. In addition to ensure the security of encryption, payment process should also avoid careless mistakes made by users of security vulnerabilities, taking into account the network environment and the efficiency of the algorithm.

# online payment security requirements

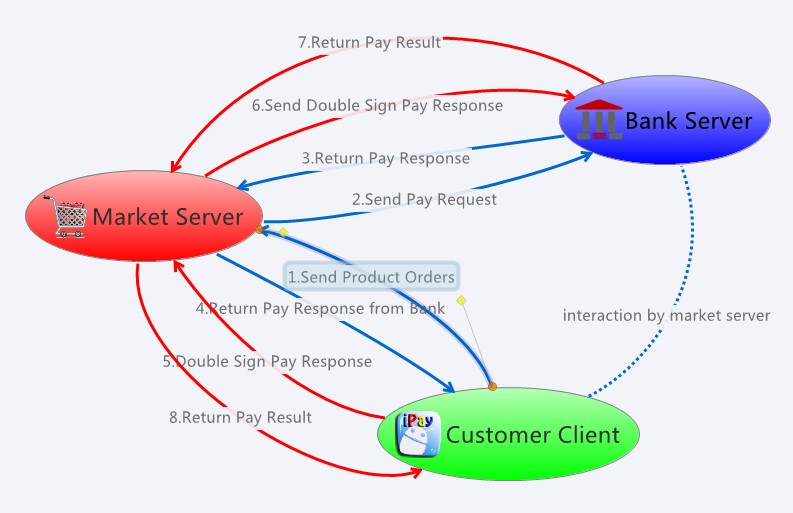
* Effectiveness: prevent and control computer hardware, software and network errors, to ensure that trade data in determining time and location is valid.
* Confidentiality: prevent illegal theft of information access and information during transmission by.
* Data integrity: prevent random generation, delete and modification of information. Prevent information loss and duplication and ensure the unity of the order of information transfer in data transfer.
* Reliability, non-repudiation: In the paperless e-commerce mode, through handwritten signatures and seals for identification of trading parties is impossible. Therefore, it’s necessary to provide reliable identification in the transaction process for the individuals involved in the transaction
* Review capacity. According to the requirements of confidentiality and integrity, data review results should be recorded.

# security measures

E-commerce in general takes the following safety measures:

* Data encryption to ensure data security.
* Certification to determine the identity of the sender.
* Anti-denial deal. The sender can’t deny that the information had sent to receiver, receiver can’t deny that the information has been received after receiving the information.
* Authorization. Determine whether the user is authorized to perform a particular special operation.

# ipay payment process design



* Registration stage

Individual client and server-side shopping centers have to go through the registration phase which will obtain related information and save them up.

1. Individual client need access to the bank's public key (open) and private key of you bank card encrypted by your payment password(secret)
2. Shopping malls need to obtain encrypted private key encryption of bank card, and re-encrypted, save it to the mall server. Bank database should contain all the bank cards information(including personal and shopping malls) ，public key and private key encrypted by the payment password

* Payment stage

Payment process uses https encrypted connections:

1. Individual client sends purchase orders (orders) to the mall server. The server calculates the costs required to pay.
2. Shopping mall encrypts credit card and fees need to pay by bank public key encryption and sign the information, then sends to the bank (RSAencrypt (market cardnum + amount) + RSAsign (market cardnum + amount)), bank verifies the information and generates number (tranid).
3. Banks uses the mall's public key to encrypt the payment number and the fees paid and send back to the mall, and return the data signature (RSAencrypt (tranId + amount) + RSAsign (tranId + amount)), the mall verifies the information
4. Shopping malls return the request back to the client (RSAencrypt (tranId + amount) + RSAsign (tranId + amount)). the client views and verifies the information, and then waits for user’s payment password, decrypt the private key, and use the private key to sign these information, confirm payment.
5. Individual client makes double signatures on payment data (RSAencrypt (OI) + RSAencrypt (PI) + RSAsign (OI) + RSAsign (PI) + RSAsign (OIMD + PIMD)), sends to the mall. The mall verifies the OI information inside.
6. Mall continues to send payment data of clients to banks, allowing banks to deal with. Banks verify the signature and data, and then save changes to the database.
7. Banks return the results and the signature of the results (RSAencrypt (result) + RSAencrypt (result) + RSAsign (result). Shopping malls save payment records based on the results.
8. Mall returns the payment results to the client. The client displays the prompt of the payment results to the user.

# payment process implementation

 Refer to the source code for the concrete realization. Tools used in encryption are in:

package com.ipay.server.security in project IpayMarketServer

package com.ipay.server.security in project IpayBankServer

package com.ipay.security in project IpayClient

# Other factors

* As the network instability, we should consider network interruption occurred during the payment processing. In addition to improve the hardware environment (such as enhancing WIFI hotspot load capacity), we should also increase validation of the data integrity and payment operations such as withdrawal
* Client providing users with automatic login and passwords save service should realize that there are many factors of insecurity, such as client poisoning, illegal program to steal data, mobile phone theft and other issues. It should add more to remind, inform the user of potential insecurity
* To protect the stability of the entire system, we can try to add more security measures, such as sending text messages to use paying temporary password when paying or freezing the account if inputting the wrong password three times

# references

1. 郭中华，徐飞 基于SSL协议的SET协议模拟实现
2. 吴波 易协议的网上支付系统的设计和实现
3. 黄元飞 信息安全与加密解密核心技术.

【4】 梁栋 Java加密与解密的艺术