FINAL PROJECT REPORT

OPERATING SYSTEMS (CS 5204)

THE ELECTRONIC COMMERCE SYSTEM

PROJECT BY-

Ashwini Pande. (900 - 16 - 0518)

Subhag Oak. (627 - 70 - 0055)
Abstract of the project:

We are developing a basic electronic commerce system as a project for the operating systems course. The basic aim of this project was to understand the nature of distributed computing and to study the functionality and implementation of JAVA RMI.

The fundamental design of the project is as follows.

The system contains 2 stores with which the client can do online shopping and 1 bank server, which will be used to validate the transaction done by the client with any of the stores. The stores will forward the information entered by the client to the bank for validation. The important point here is that all the transactions should be asynchronous i.e. the client does not block when the store sends the validation request to the bank. This would enable the client to conduct the several stores simultaneously. After the bank validates the client information such as valid credit card number and the available credit, the bank sends an email confirmation to the client giving him the status of his transaction with the store i.e. failure or success of the transaction.

Here we have used the security features such as PKI (public key infrastructure) for secure data communication between the stores and the bank. The security between the client and the bank will be taken care of by the Java Security Manager.

Underlying Technology and concepts:

- JAVA RMI - for communication.
- JAVA Swing – for GUI development.
- JAVA Security – implementing security mechanism.
- PKI Infrastructure – implementing security mechanism.
- Callback Feature (for Server to Client Communication) – adding client objects.
- JDBC – for database connectivity
- SMTP – email
Communication Diagram:

Here is the basic communication diagram of the project, which explains the flow of the entire system.

This diagram explains the working of the system with only one store in the picture. But since the system is designed for transaction with multiple stores, same work flow diagram can be drawn with multiple stores in the picture.

The communication between the client and store is independent of communication between the store and the bank. Multiple clients can communicate with the store simultaneously. Similarly the client can conduct the business with multiple stores simultaneously.
**Workflow:**

The workflow of the system is as follows:

Client decides from which store he wants to do shopping. At this point in the project he will be presented with the screen, which will give him the option of doing shopping from either store1 or store2. He selects the store for transaction by clicking on any of them.

The client is required to login to the store database in order to carry out the transaction. The client also passes its own object to the store so that the store can use it for callback implementations. Each store has the client database available with it. The database will contain the client specific information such as user name, password, Email -id. The client will be presented with the login screen where he will enter the required information. The communication between the client and the store is implemented using the RMI mechanism.

When the store receives this information, it will be validated against the information present in the database with the store. The database available with the store has the username, password and some other information related to the client. The store will authenticate the client against the information provided. If authenticated the store will display the shopping cart to the user.

The client will then select the items to buy from the available list of items. After he has done with the selection, for the purchasing purpose he will enter the required information such as credit card type, credit card number and expiry date. This information will be passed on to the store.

The store will not do the validation of this information but it will forward this to the bank for validation of the credit. The credit database is available with the bank. This database contains information such as credit card number, credit available with the client and the email-id of the client. The communication between the store and the bank is implemented using the RMI mechanism.

The bank will validate the credit information provided by the client and check if a particular transaction can be carried out or not. Firstly the bank will validate the credit card number. If the number is valid then the amount of the purchase done by the client will be verified against the available credit. If everything is proper then the bank will send a confirmation email to the client giving him the summary of his transaction.

So in total there are 3 servers:
- Store1 server
- Store2 server
- Bank server
Security aspect of the system:

The communication between the client and the store takes place using the RMI mechanism and underlying security mechanism used by this communication is implemented using the JAVA security manager.

The communication between the store and the bank also takes place using the RMI mechanism but here the underlying security mechanism is implemented using PKI (Public Key Infrastructure). This will be used only in case of the bank. This is implemented as follows:

We first run the RSA algorithm to generate the pair of keys for the communication. These keys are nothing but the public and the private keys for the bank server. Once these keys are generated, we store them in files, namely bank_pubic_key and bank_private_key. When the store server wants to send in the credit information to the bank server, it will use the public key of the bank server to encrypt the information such as credit card number in this particular case and will pass on that encrypted information to the bank server. When the bank server receives this information as a part of the message sent to by the store, it will use its own private key to decrypt the message. This will give bank server the original credit number of the client.

Since the bank only knows the private key of the bank server, it is the only one who is capable of decrypting the information. Thus the credit card number of the client is securely passed on to the bank server by the store server.

Summary:

Thus we have successfully implemented an electronic commerce system in the process of learning and understanding the fundamental working of JAVA RMI. It was very interesting to watch how the communication takes place between different machines using RMI. This made the concept of client-server architecture more clear. The security aspect of implementation gave us more insight into the security in the distributed systems; especially the PKI explained the functionality of the public and private key infrastructure.