COE817 The PROJECT: Secure Banking System

Design and implement security protocols for a banking system consisting of a bank server and three ATM client machines. The server establishes a socket listening for connection requests from ATM clients. For each request from an ATM client, the server creates a new thread that will authenticate the user of the ATM and process that user's transactions.

In this project, customers use ATM client machines to deposit, withdrawals, and balance inquiries from their accounts in the bank server. A client needs to register a new account on the server with his username and password. Customers then interact with the ATM client and work as below:

(1) The ATM client prompts the customer for username and a password which the customer enters at the ATM client for logging in.

(2) ATM client communicates with the bank by running an authenticated key distribution protocol (Assume client and server already have a shared key. This protocol will provide a second layer symmetric key based authentication) that satisfies the following requirements:

- It authenticates the customer to the bank server.
- It authenticates the bank server to the ATM.
- A new symmetric key called Master Secret is created and shared by ATM and the bank server.

Design and implement the authenticated key distribution protocol that meets the criteria outlined above.

(3) Design a key derivation approach that derives two keys from the Master Secret: one for data encryption, the other one is a MAC key (Message Authentication Code) for data integrity. Both ATM client and server will share and use these two keys for the following data transaction phase.

(4) Design security protocols for the following data transactions: deposits, withdrawals, and balance inquiries. The protocol preserves the integrity and confidentiality of data communications between the bank server and ATM client. No attacker should be able to modify or read the contents of the transactions, and, you need to generate and verify MAC to ensure data integrity of these transactions.

It also records information of clients deposits, withdraws and balance inquiries in an audit log file for later use in justifying its past actions to concerned customers.

The format of the audit information could be simply as below:

Customer ID	Action the client takes	The time the action is taken

In your program, whenever a customer takes an action (such as withdraw, deposit or balance inquiry), you need to create an audit information with the format described above and store it in an audit log file, so that it can be inspected afterwards. However, the bank server is potentially vulnerable to network attacks, thus data written to the log should be encrypted to prevent breach of confidentiality.

(5) Design GUI interfaces of clients and the server for project demo.

Maximum Group size

This is a group project. The maximum group size is 4.

Demonstration Requirements

The application you will develop should demonstrate the following functions:

(1) Customer logs on. Selects 2-3 actions, such as deposits, withdrawals, and balance inquiries. The bank server should perform the corresponding action on the account owned by the customer and respond the result to the customer. Also, check results in your audit log file.
(2) Pick up another client and do the same thing as in step (1) and check the audit log file results.
(3) Answer TA questions regarding details of your developed protocols.

Report

The report must be at least 10 pages long but no more than 20 pages. Use Times New Roman font size 12. Your report must include the following four parts:

Introduction:

Introduce the purpose and goals of the project. Provide any background material necessary. Discuss the scope and limitations of your project.

Design:

- Briefly describe how the project is implemented.
- Architecture Diagram: modules description and their functionalities.
- Detailed description of authenticated key distribution protocol, key derivation approach and security protocols for data transactions. Include any techniques/principles that you have used in your design.

Results:

Screenshots of GUI interfaces and results.

Conclusion:

What have you learnt from the project? Describe leadership experience received for each member from the project. Describe contribution of each member in your group.

The report will be assessed not only on their technical or academic merit, but also on the communication skills of the author as exhibited through the report.

Cheating

No copying is permitted. Cheating involves copying code or project from the web, other student's work, etc. The punishment for cheating is a zero in the project and will be subject to the university's academic dishonesty policy.

Submitting your project

Submit your project report and source code to D2L project submission folder by April 12, 2025.
You must provide the names and student ids of group members in your report.
.