CSE 345/545 Foundations to Computer Security

Course Project

A Secure Banking System

1. Introduction

A secure banking system (SBS) is a software system developed primarily to facilitate secure banking transactions and user account management through the Internet. A banking organization often needs to track various operations performed by both the internal and external users using the organization's banking infrastructure.

The focus of this project is to develop a SBS to facilitate secure banking transactions and account management required by any banking organization. This document shall be used as a set of guidelines. You are allowed to make necessary additions and/or changes to the requirements with prior written approval from the professor or the TA.

2. Requirements

A user should be able to use this system any place and any time with the availability of Internet access and web browser.

2.1 Users

Users of this system can be categorized according to their roles. In this project, there are the following categories of users:

2.1.1 Internal Users

1. Regular employees: responsible for low priority banking operations.

2. System manager: responsible for higher priority banking operations and responsible for the authorization of critical transactional operations.

3. System administrators: maintain all the user accounts and the banking system.

2.1.2 External Users

1. Individual customers: Individuals having banking activities, each of whom have an user account for performing personal banking transactions such as personal fund transfer, debit and credit from personal user account.

2. Merchants/Organization: Users having specialized banking transaction processing requirements, such as client payment processing.

2.2 User Account Management

- Various user roles have different privileges. The following are the general rules:
    - A regular employee
        - can view, create, modify, delete and authorize transactions upon having necessary authorization from the users and/or merchants
        - does not have access privilege to view or modify any user account unless he/she has an authorization from the system manager.
        - can access transactions with necessary authorization from users/merchants or system administrator
    - A system manager
        - can authorize for critical transactions (Amount > Rs.100000)
        - can access transactions with necessary authorization from users/merchants or system administrator
    - A system administrator
        - can verify users' requests.
        - can add /modify /delete internal users' account.
        - can access the system log file
        - can access PII with necessary authorization/request from government agencies (no automatic PII access. A system may be designed to act as a higher authority)
        - can add/modify/delete external user accounts with necessary request from external user and respective regular employee/system manager
    - An individual user
        - can view, debit, credit and transfer money from his/her personal bank account
        - can initiate modification personal information change or transactional review
        - can authorize bank official requests to review transactions on accounts he/she is responsible for
    - A Merchant/Organization
        - can submit an individual users/merchants payment to the bank with proper authorization from users/merchants
        - can view, debit, credit and transfer money from merchants' bank

account

▪ can initiate modification personal information change or transactional review

▪ can authorize bank official requests to review transactions on accounts the merchant is responsible for

2.3 Secure Banking Functions

The system should provide at the least the following functions for customers' checking accounts or savings accounts, based on a user's assigned role after user authentication (all the functions can be performed by a user with proper privileges):

1. Debit and Credit Funds: Must provide external users (with proper privilege) an interface to debit and credit funds securely from the accounts they are responsible for. An external user can submit a debit/credit request to the system and an internal user(with proper privilege) can authorize or decline the request. If the request is authorized, the debit/credit is successful, and the external user's account should be changed accordingly. Otherwise, there shouldn't be any change for the external user's account.

2. Transfer Fund: Must provide external users (with proper privilege) an interface to move funds from one account to another personal and/or another external users' account. Transfer fund function should include both internal transfer and external transfer. An internal transfer is a transfer between one user's different accounts. An external transfer is a transfer between two users' accounts.

3. Payments: Must provide external users (with proper privilege) an interface to either make payments or submit payment on behalf of another user.

4. Technical Account Access: Must provide internal users (with proper privilege) an interface to access users' account to perform troubleshooting and/or perform maintenance operations

5. Transaction Locator: Must provide internal and external users (with proper privilege) an interface to search, locate and access appropriate transactions (for specific users)

6. Risky Transaction Authorization: Must provide internal users (with proper privilege) an interface to access and authorize "Risky" transactions (which require authorization)

2.4 Other Requirements

a. Public Key Certificates: The secure banking system must use public key infrastructure (PKI) in addition to using SSL/TSL (HTTPS) to enforce the security of the application. You can establish your own certificate issuing authority for purpose of this project (one way is to make the bank a certificate issuing authority to certify entities to authenticate users). A minimum of two functions must employ PKI, and you may decide the extent of the PKI applicability to the functions.

b. OTP: The secure banking system must employ OTP (One Time Password) technique with virtual keyboard feature to validate highly sensitive transactions for at least two of the functions in Section 2.3. You may decide the extent of the OTP applicability to the functions.

c. The SBS should allow multiple users to use the system simultaneously.

d. Secure transactions logging is required to enable external audits.

e. Must employ necessary security features to defend against attacks on the SBS system (project will be tested by the TA and students)

3. Programming Language & Framework

Each group can choose the programming language of their preference through consensus. Each group can use the following: OS: Windows (XP or any newer version) or Linux. DBMS: Microsoft SQL server, Oracle XE or MySQL. Web server: IIS or Apache. However, if you choose to use other types of OS, database system, or web server for the project, you need to discuss it with the TA since the TA may not be able to help you on the project.