CSE 545 Software Security

Course Project Requirements

A Secure Banking System

Spring 2020

1. Introduction

This course project is to develop a skeleton secure banking system (SBS) with limited functional, performance, and security requirements for secure banking transactions and user account management. You can make changes to the requirements only with prior written approval from the professor.

2. Requirements

Multiple users should be able to securely use this system from any place and at any time with the availability of Internet access and web browser.

2.1 Users Categories

The users of this system are classified in the following five categories according to their roles:

2.1.1 Internal Users

Internal users can be classified into 3 groups:

1. **Tier-1 employees:** Responsible for assisting the customer with various banking operations, such as initiating fund deposit, issuing cashier cheques and transferring money etc. Tier 1 employee will do online operations like adding money to customer account (money deposit), etc.

2. **Tier-2 employees:** Responsible for the authorization of critical transactional operations. Each bank has a threshold amount, which a customer can send in a day for a transaction. If a customer exceeds this threshold amount, the customer is notified that permission is needed from an internal employee (Tier 2 employee) to proceed. Transactions of this type are considered as critical transactions. The threshold amount for this project is $1,000 USD. A tier-2 employee must also be able to create, modify, and close customer's accounts.

3. **Tier-3 employees** (Administrators): create, maintain, change, and delete all the internal users' accounts and ensure smooth functioning of the banking system.

2.1.2 External Users

External users can be classified to the following two groups:

4. Individual customers: Individuals, each of them has at least one of the following three types of accounts: checking, saving and credit card with common functions, such as fund transfer, debit and credit from user accounts.

5. Merchants and organizations: Corporate customers

2.2 User Account Management

Every customer must have at least one of the three types of accounts: savings account, checking account and credit card account

Various user roles have different privileges. The following are the general rules:

⇒ **Tier 1 employees**

- can view, create and authorize non-critical transactions upon having authorization from the bank customer and tier-2 employee
- can view customers' accounts
- can issue cashier cheques as well as handle fund transfer
- can authorize or decline customer's request

⇒ **Tier 2 employees**

- can view, create, modify, and close customer' accounts
- can authorize transactions
- can initiate modification of accounts

⇒ **An administrator**

- can view, create, modify, and delete employees' account.
- can authorize or decline employees' request.
- can access the system log file. (System log file is only accessible to the administrator)

⇒ **An individual user (individual customer)**

- can view, debit, credit and transfer money from his/her bank account
- can initiate modification of personal account
- can view, authorize and decline customer's money transfer requests
- can initiate request for creation of an additional account

⇒ **A merchant/organization**

- can view, debit, credit and transfer money from their bank accounts with proper authorization.
- can initiate modification of personal account
- can view, authorize and decline other customer's requests

2.3 Banking Functions (Required)

The system should provide at the least the following functions for customers' checking accounts or savings accounts:

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

2. **Transfer Fund:** Must provide customers (with proper privilege) an interface to move funds from one account to another, or from one customer's account to another customer' account (all customers of the same bank). Must also provide an interface for approving or declining critical transactions on fund transfer. Transfer fund function should include being able to transfer between one customer's different accounts, as well as between two customers' accounts.

3. **Email/phone transfer function:** A customer should be able to send money to another bank's customer through their registered email addresses and/or phone numbers.

4. **Technical Account Access**: Must provide bank's employee (with proper privilege) an interface to access other employees' accounts to perform troubleshooting and/or perform maintenance operations

5. **Banking statements**: A bank customer should be able to download their banking statements.

6. **Opening additional account**: Banking system must provide an interface for a customer to request the creation of an additional account, after which the request is granted by a Tier 2 employee.

7. **Help & Support Center:** Banking system must also provide an interface for customer to update their contact information as well as schedule an appointment.

2.4 Security Designs (Required)

1. 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. There must be 2 applications of PKI:
   a. A certificate for the web application (self-signed or authorized by a Certification Authority)
   b. The group has the flexibility to choose the second application and how they want to use PKI in their system.

2. OTP: The secure banking system must employ One Time Password (OTP) technique with virtual keyboard feature to validate highly sensitive transactions for at least two of the functions in Section 2.3
3. The SBS should allow multiple users to use the system simultaneously.
4. The SBS must be available 24x7 for user access
5. Prevent malicious login controls
6. Session management
7. Must employ necessary security features to defend against attacks on the SBS system (project will be tested by the TA and students. Preventing DoS or DDoS attacks are out of scope for this project. Student will be penalized to deploy such attacks.)
8. Must employ data masking techniques and hashing algorithms to protect user sensitive fields in the database.
9. Must implement a sign-in history function in a manner that a log keeps history of date and time that a customer signs in into their account.
10. All the valid and approved transactions must be captured in Hyperledger blockchain platform.

2.5 Performance Requirement (Required)

1. Response time of the any event should not exceed standard response time for banking application (3 to 4 seconds).
2. System should withstand user load of approx.120 users per second and operate in 24*7 environment.

3. Technology & Tools

- Each group can choose one or more of the following languages: Java, Python.
- Each group can choose either Windows or Linux for OS.
- Web server: IIS or Apache.

If you want to use a technology/tool different from those above, you need to discuss it with the professor or TA and obtain a written permission. Note that the tool/technology you request to us for your course project must be available to the public for free.