CSE 545 Software Security

Course Project Requirements

A Secure Banking System

Fall 2017

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 are allowed to make changes to the requirements only with prior written approval from the professor.

2. Requirements

A user 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 opening accounts, initiating fund deposit, etc. Tier 1 employee will do online operations like creating customer accounts, adding money to customer account (money deposit), etc.(mentioned later)
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.]
3. Administrators: create, maintain, change, and delete all the internal users' accounts and ensure smooth functioning of the banking system.[Internal accounts are handled by Tier 1 and 2 employees]

2.1.2 External Users

External users can be classified to the following two groups:

1. 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.
2. Merchants and organization: Users having specialized banking transaction processing requirements, such as client payment processing. Example: A merchant account (like Amazon) can initiate an incoming transaction if they have the customer credit card number and CVV number.

2.2 User Account Management

- Every external user must have at least one of the three types of account: 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 external users and tier 2 employee
    - can view, create and modify external users' accounts upon having authorization from external users and tier 2 employee
    - can authorize or decline external users' request
    - can initiate modification of personal account
  - Tier 2 employees
    - can view, create and authorize non-critical transactions
    - can view, create, modify, and delete external users' accounts
    - can view and modify internal users' accounts
    - can authorize critical transactions
    - can authorize or decline external users' request
    - can initiate modification of personal account
  - An administrator
    - can view, create, modify, and delete internal users' account.
    - can authorize or decline internal users' request.
    - can access the system log file. (System log file is only accessible to the administrator)
    - can access PII. (PII is only accessible to the administrator)
  - An individual user
    - can view, debit, credit and transfer money from his/her personal bank account

        - can initiate modification of personal account
        - can view, authorize and decline external users' transfer money requests

    - A merchant/organization
        - can view, debit, credit and transfer money from his/her personal bank account
        - can initiate modification of personal account
        - can view, authorize and decline external users' requests
        - can submit an external user's payment to the bank with proper authorization from the external user

2.3 Banking Functions (Required)

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 user's account. Must also provide an interface for approving or declining critical transactions on fund transfer. 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. **Email/phone transfer function:** An external user should be able to send money to other external users through their registered email addresses and/or phone numbers.

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

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

6. **Transactions Access:** Must provide internal users (with proper privilege) an interface to access and authorize all the transactions (with required authorization)

7. **Banking statements**: An external user should be able to download banking statements.

8. **Credit card function:** Your banking system should have credit card account management functions, which should at least include balance management, payment management, interest generation, late payment fee, and credit limit management.

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. You may decide the extent of the OTP applicability to the functions.

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. Implement trust management for end point devices

7. Session management

8. Email and/or text alert for critical transactions

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

10. Must employ data masking techniques and hashing algorithms to protect user sensitive fields in the database.

3. Technology & Tools

- Each group can choose one or more of the following languages: Java, Python, .NET, Ruby.
- 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.