King Saud University
College of Computer and Information Sciences
Department of Software Engineering

SWE 314 – SOFTWARE SECURITY ENGINEERING 3(3–0–1)
Third Term, 2022–2023

Assignment #2 – Security requirements and Misuse Cases

(Same groups as in assignment #1)

Consider the basic functionalities of a customer banking system that allows users to:

- Login to the system using (username and password) and open their bank account online (customers can connect from a desktop, laptop, smart phone …)
- View whatever information they want from their account (transactions, profile information, remaining amount …)
- Perform transactions online (payments, Transfer to other local, national, or international accounts …)
- Send messages, enquiries, or requests to the bank
- Print Account statements for a given period of time
- Security is of utmost importance in such system. The bank owning the system must handle the following security threats:

  - The System must be made available all the time; otherwise, customers might be unhappy and change to another bank.
  - Identity theft must be avoided; otherwise a malicious user can access the system and do bad things.
  - The system must guarantee the confidentiality of at least the sensitive information in the system such as card numbers, accounts' amounts,

transactions' amounts, passwords themselves; otherwise, the loss of confidentiality of sensitive data can result in lawsuits against the bank.

- Information integrity must be preserved in all cases; otherwise, customers will lose their trust in the bank.
- Anonymity must be guaranteed to customers who desire to remain anonymous. In this case, the information that identify these customers (name, identity number…) must be handled differently.

You are required to do the followings:

1. List the functional requirements of the system.
2. Analyze each requirement using the "Requirement, Fail case, Consequence of failure, Associated risks/threats" approach by identifying the potential security requirements associated with each requirement.
3. For each identified risk/threat, indicate what solutions you will consider to reduce/overcome the said risk/threat. Indicate whether the solution will be implemented as part of the system or it will be an external solution.
4. Produce a use case diagram of the system (only the diagram, no use case descriptions).
5. Based on the analysis done in points 2. and 3. above, modify the use case diagram to make it a misuse case diagram by adding misuse cases, mitigation use cases, misusers, "threatens" and "mitigates" relationships.
6. Describe the misuse cases and (the mitigation use cases) using the template seen in class.
7. Discuss the choices you will make in terms of software architecture and design in order to produce a secure software product.

Deliverable:

A short report containing:

- Cover page

- Summary
- Introduction
- List of functional requirements
- Analysis of each requirement using "Requirement, Fail case, Consequence of failure, Associated risks/threats" approach
- Proposed solutions to the identified threats/risks
- Use Case Diagram
- Misuse Case Diagram
- Misuse case descriptions
- Design Choices
- Conclusion

Deadline: The report must be delivered as a printed report on Wednesday, June 7th, 2023, at 4:00 PM at latest.