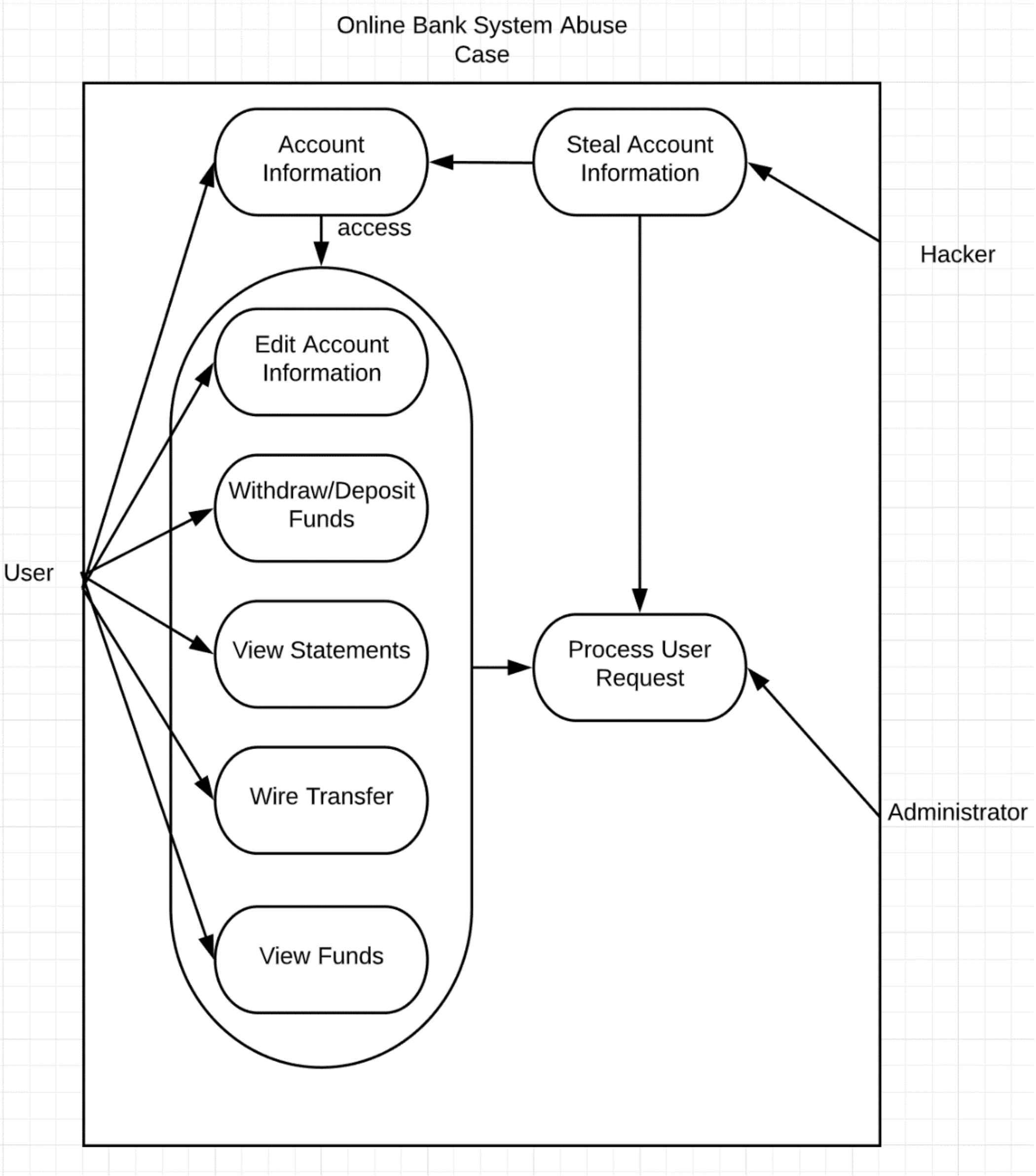
CIS 4930 - Software Security - Spring 2020

Mini-Project 1 Use/Abuse Case Diagram

Members:

Stalim Rivero
Amanda Gonzalez
Rafael Gonzalez
Tyler Allan

Use/Abuse Case Diagram:



Description:

The diagram above illustrates the different interactions between the online bank system, a registered user, the administrator and a malicious attacker. In order to strengthen the security features of the system, this will show us where the potential vulnerabilities lie and what the system should not do in the presence of an attacker.

Our usage scenario is that a registered user utilizes their account information to gain access to the account to make any of the changes that are shown in the diagram, then that request gets sent to an administrator which then processes that request. The potential exploits lie in the steps of becoming a registered user, using maliciously obtained information, where the hacker can then access the account and make any desired changes.

When making a risk analysis of the potential vulnerabilities, the risk exposure is determined by the probability of the occurrence of said risk, times the impact of the loss to the product should the risk take place. The probability of the occurrence is dependent of the level of security of the personal account information storage, sharing an inversely proportional relationship. In the scenario where this information is acquired by the attacker, as the diagram shows, the damage could be permanent and could cause closure of a legitimate account.

One security policy that is violated, which this diagram shows, is that a user's bank account balance should not be read by or modified by any other user. In this case, if a malicious attacker can obtain the account information of another user, he/she could have access to the account's balance, therefore violating this policy.