Homework 2: Threat Model of Online Banking

General Directions

This is intended to be a group homework, since threat modeling typically is a cooperative effort, although you can do it individually if you wish. Part of the assignment is to email the instructor the names of those in your group, and the rest of the assignment is related to threat modeling.

What to turn in

For the first problem, you will send an email to the instructor. The remaining parts are to be turned in on Webcourses as file uploads (a Word document or PDF file).

The Assignment

1. (6 points) Send a list of the names of your group members for this homework by email to the instructor (with a cc to all group members). The subject of this email must be "CIS 6614 Group membership for homework 2" and it must be sent by email (not on webcourses or by some other means).
2. [Plan] In this question you will be considering the design of an online banking system, which would be accessible from a computer or smart phone owned by a customer.
   (a) (5 points) For such an online banking system, describe its business purpose. That is, what benefits would a business hope to obtain by operating such a system?
   (b) (5 points) Name at least one regulation or compliance issue that such a system needs to enforce or be designed to not violate.
3. [Plan] In this question you will consider the high-level design of an online banking system.
   (a) (10 points) Describe, at a high level, the design of the system, including: the kinds of data it would handle or store, any servers or services it would contain, and any network devices it would contain.
   (b) (10 points) List the assets that the system contains that the bank that builds and runs the system would want to protect.
   (c) (20 points) Produce a data flow diagram of the system's design that contains users, data stores, active components (e.g., servers or processes), and the data that flows between them, as well as any trust boundaries. Hint: the diagram can be produced by a tool such as the Microsoft Threat Modeling Tool or the OWASP Threat Dragon tool.
   (d) (10 points) Briefly describe the trust boundaries of the system.
   (e) (5 points) Briefly describe the system's attack surface.
   (f) (5 points) Briefly describe any implicit trust relationships in the system's design. (If there are none, say that.)
   (g) (10 points) List the actors or roles that should be part of the system and the permissions that they would need.
4. (20 points) [Plan] Briefly describe the 10 most important threats to the system's security and why they are real and credible.
5. [Architect] Supposing you are directing the implementation of the security mitigations for this system.
   (a) (20 points) List the procedures and policies you would have developers use to mitigate the 10 most important threats described in the previous question.

(b) (20 points) For each mitigation, list each of the threats that your procedures and policies would help prevent, along with a brief justification as to why those mitigations should work.

6. (15 points) Taking into account the mitigations, briefly describe the residual risk of the design.