Teaching Security Lesson 2: Authentication

Activity: Threat Modeling
Online Banking Authentication

In Lesson 1, you learned how to threat model a system. Now you'll apply that to the creation of an online bank account.

Start by drawing a diagram on the next page. Here's what's supposed to happen:

1. When the customer opens a bank account, xe signs up for online banking, and chooses a username and password.
2. The bank verifies that the username is unique and the password meets the minimum requirements.
3. The bank stores the password and tells the customer that the account was successfully created.
4. The customer installs the bank's mobile app and uses it to connect to the bank.
5. The customer uses xir username and password to log in and set up a payment to xir cell phone provider.

Your diagram should **show how information moves through the system** during the steps listed above.

Now: What could go wrong with this scenario? What are the weak points?

Draw in on the diagram some things that might go wrong at the different steps in the process. Also **draw in any protections** you know of that the bank could implement to prevent those things from going wrong.

Remember to use the threat modeling questions. **Jot down some notes** to use as a guide:

a. What needs to be protected in this system? What's the impact if it fails?

b. Who do you need to protect against? What are their motivations and goals?

c. What resources do any potential attackers have for getting what they're after? What strategies could they use?

d. What resources and strategies do you have for protecting against attacks?
    i. What resources and strategies does the *user* have?

    ii. What resources and strategies does the *bank* have?

System Diagram:

Key:

Provide labels here for any symbols you use!