Homework 1: Threat Modeling

See Webcourses and the syllabus for due dates.
This homework is about threat modeling. The main reference we have for this is the article by Myagmar, Lee, and Yurcik [MLY05], which was passed out in class.

General Directions

This homework can be done in groups. You should form a "group" in webcourses for it, even if it consists of yourself only.
Answers to English questions should be in your own words; don't just quote from articles or books.

What to turn in

For problems that require an English answer, please paste the text of your answer into the text box on webcourses. If the problem may benefit from formatting support, we will instead have you upload a word document or a PDF file.

Problems

1. [SecurelyConstruct] Consider an electronic bill paying system (such as Quicken Bill Pay see `http://quicken.intuit.com/personal-finance-tools/online-bill-pay-software.jsp`). The key features of this system is that a customer using Quicken (on their own computer) can pay bills using their computer's an app (the Quicken program). Paying a bill with such a system directs the customer's bank to send money electronically to pay the bill. You can imagine that the bank just sends a check instead of the person writing the check themselves, but the payments are actually done electronically between the customer's bank and the payee's bank (and that transaction is outside the scope of our analysis).

   To make communication between customers and the service more efficient, the service itself maintains an account for each customer. Also, for each customer the service maintains records of the customer's bank, and the customer's accounts for each payee. Such records include the customer's own account number for that payee and the local address of the payee.

   (a) (7 points) Draw a network model of the Quicken Bill Pay service. This can be done either by hand (and then scanned or photographed) or with powerpoint or some other drawing tool, but however this is done it should be part of the document you hand in.

   (b) (10 points) From the point of view of the Quicken Bill Pay service, what are the assets to be protected in such a system? Note: in this problem we will only consider the part of the service that allows bill payments and queries about bill payments by customers (not other services such as transferring money between accounts).

   (c) (12 points) From the point of view of the Quicken Bill Pay service, what are the threats for the service? (Recall that threats are the goals of an attacker. We are not looking for the attacks themselves, just what an attacker's goals might be.) Note: Again, for this problem we are only considering the part of the service that allows bill payments and queries about bill payments by customers (not other services such as transferring money between accounts).

2. [SecurelyConstruct] Perform a threat analysis for an online backup service, such as Carbonite's personal backup service (see `http://www.carbonite.com/online-backup/personal/how-it-works`). Note that part of the service is "customer support" Your analysis should include the following parts.

   (a) (7 points) Make a network model of the backup service.

(b) (12 points) Enumerate the assets of the backup service, from the point of view of the backup service itself.

(c) (6 points) List the access points into the backup service.

(d) (12 points) Enumerate the possible threats to the backup service.

(e) (30 points) Enumerate the possible attacks to the backup service, and for each attack rate the risk of that attack on a scale of 1-10 (10 being the highest risk).

Points

This homework's total points: 96.

References

[MLY05] Suvda Myagmar, Adam J. Lee, and William Yurcik. Threat modeling as a basis for security requirements. In *IEEE Symposium on requirements engineering for information security (SREIS)*, volume 2005. IEEE, 2005.