Homework 6

Due by 7:00 p.m. Tuesday, 12/9/14

In this assignment, you are asked to contemplate descriptions of hypothetical systems and identify the following.

1. What security properties might we expect the system to enforce?
2. For each such security property, label it with one of: *confidentiality*, *integrity*, or *availability* and list some control(s) that might be used to ensure it?

Note, in order to answer (2), your answers to (1) are necessarily somewhat restricted. For example the security property "Cannot be attacked" is not suitable as one of the properties you list for (1) because it is not one of: confidentiality, integrity, or availability.

As an example of what we would like you to produce, consider the following system description.

> The *stork baby delivery system* allows an autonomous aircraft (a *stork*) to deliver a payload (a *baby*) to a geographic location (given in some coordinate system, such as latitude and longitude) prespecified by some higher authority (herein called *providence*). Prior to take-off, providence programs a stork with the geographic location describing where the baby should be delivered. Throughout the mission, the stork transmits back to providence a video of the landscape (labeled with geographic location coordinates) that the stork flies over. While a stork is in flight, providence may issue commands to that stork and change the location for the delivery, alter the path being followed to that location, or abort the mission.
>
> **Threat model**: The adversary desires to prevent baby deliveries. The adversary has access to radio equipment that transmits and receives on the same frequencies that providence uses for communication with a stork. The adversary also controls weapons systems that can destroy a stork in flight.

Here is the list of security properties, each identified with a type, that you might submit as an answer.

1. Integrity: Prior to take-off, the delivery location can be programmed into the stork by providence but not by the adversary.
2. Integrity: While in flight, the delivery location, trajectory of the stork, and mission abort can be changed by providence but not by the adversary.
3. Availability: If a delivery has not yet been made then providence is able to program the delivery location, trajectory of the stork, and/or abort the mission.
4. Confidentiality: The adversary is not able to view the video images transmitted by the stork while the stork is in flight.
5. Availability: Providence is able to view the video images of the stork while the stork is in flight.
6. Integrity: The video images seen by providence are accurate depictions of what the stork sees while in flight.
7. Confidentiality: Prior to a delivery, the adversary is not able to learn the location of the delivery.
8. Confidentiality: While in flight, the adversary is not able to learn the location of the stork except by direct visual observations from the ground.

System 1: A Web-based Mail System. Users login by visiting a prespecified URL for the system and then entering both an identifier (i.e., a name) and a password. This starts a session that is associated with the specified identity. The system then displays in a *preview frame* a list of messages that have been sent to that identity and have not been deleted during this or some prior session associated with that identity. Here, for each message, the name of the sender and the contents of the message are displayed.

During a session, a user can:

a. Click on an icon to generate a reply to the message the user is currently viewing. The user then types the body of the reply. That reply later becomes a message that will be available for viewing by the sender of the original message to which this serves as a reply.
b. Click on an icon to generate a new message. The user then enters an identity of some receiver and enters a body for the message. That body is incorporated into a message that will be available for later viewing by the intended receiver.
c. Click on an icon to delete the message that the user is currently viewing.
d. Click on an icon to end the session.

Threat model: The adversary is a user who desires to read email, generate bogus email, and/or alter email that has been generated by bona fide users. The adversary has access to the URL for the mail system and also can read, delete, and/or update network packets in transit. The adversary cannot physically access or run programs on a user's machine that is running a browser to access the mail system. And the adversary cannot physically access or run programs on the mail system server.

System 2: A Grade Management System. This information system allows users to enter grades and access grades associated with assignments. A user is granted access to the system by providing a role (professor, TA, grader, or student) along with an SFSU ID and associated password. Permissible roles for each user are specified at the time a new course is added to the information system. Grades are assigned by graders. Regrades are done by teaching assistants when a student requests a regrade or when the TA notices a grade that seems anomalous. And a professor can perform any and/or all of these actions, but a professor's updates can only be changed by the professor. A student, in addition to learning about his or her grades on individual assignments, is entitled to learn the average and median grade for any given assignment.

Threat model: The adversary is a user who desires to learn grades, change grades, or prevent others from learning or changing grades. The adversary has access to the information system and also can read, delete, and/or update network messages in transit. The adversary cannot physically access or run programs on a user's machine that is running a browser to access the information system. And the adversary cannot physically access or run programs on the server hosting the information system.