Purpose

To discuss design choices to be made based on a distributed version of your game, with particular emphasis on the security design principles.

Scenarios

The following scenarios may be discussed in class.

1. Assume that your game (either Cosmic Wipeout or Tunk) is going be designed as a multi-player game where each player may participate in a game from anywhere, as long as they have access to the Internet.

   a. Will this change your model-view-controller design?
      i. If so, what are the significant changes you would need to make?

   b. Think about the security design principles listed on page 2.
      i. Which of these principles need to be addressed in your design?
      ii. How would your design change to accommodate the principles that should now be included in your design?
      iii. What ideas do you have for implementing each of the principles identified in 1.b.i and 1.b.ii?

2. Assume that your multi-player distributed game (as described in 1) is also going to charge each player a fee to play the game. This will require players to provide credit card information.

   a. Will this change your model-view-controller design?
      i. If so, what are the significant changes you would need to make?

   b. Think about the security design principles listed on page 2.
      i. Which of these principles need to be addressed in your design?
      ii. How would your design change to accommodate the principles that should now be included in your design?
      iii. What ideas do you have for implementing each of the principles identified in 2.b.i and 2.b.ii?

3. Assume that your multi-player distributed game has been in use for a few years. Suddenly, a malicious user has attacked your system and gained access to customer data that should have been kept private.

   a. Think about the security design principles listed on page 2.
      i. Which of these principles should now be addressed in your design?
      ii. How would your design change to accommodate the principles that should now be included in your design?
      iii. What ideas do you have for implementing each of the principles identified in 3.a.i and 3.a.ii?

Security Design Principles

Security Design Principle	Description
• Economy of mechanism	Keep your design as simple as possible. Allows quality assurance methods the greatest chance of finding security vulnerabilities.
• Fail-safe defaults	Default setting/action should be to favor security over usability. When in doubt, deny access.
• Complete mediation	Every request to access data/system should be checked for adherence to a protection scheme. Strike a balance with performance (e.g., speed, power usage) and usability requirements.
• Open design	Publish your design for anyone to review. No one person is an expert in all things security-related!
• Separation of privilege	Separate components of a system to reduce damage when a security breach occurs in any one component.
• Least privilege	Each user and program should operate with minimum set of privileges necessary to accomplish the job. Every user should not have “admin” rights.
• Least common mechanism	Minimize security mechanisms being shared/used by more than one user or system.
• Psychological acceptability	User interfaces related to security mechanisms should be designed based on what a user expects.
• Work factor	Cost of compromising a security mechanism should be compared with the resources of an attacker when designing a security scheme.
• Compromise recording	It may be more desirable to record the details of an intrusion rather than designing more sophisticated prevention mechanisms.
• Secure the weakest link	Suite of security mechanisms being used are only as good as the weakest security mechanism being used.
• Defend in depth	Your design should include redundancy and layers of defense.
• Be reluctant to trust	Be skeptical of security protections that are not within your software system (i.e., trust but verify).
• Promote privacy	Your design needs to consider types of personal information you are collecting from a user. Do you really need to persistently store this data? Do you really need to send this data over a network?
• Use your resources	Talk to others about design choices you are making. Have experts with different backgrounds review your design.