CS 557: Software Secure Design and Analysis
Project Goals

Joshua D. Guttman
guttman@wpi.edu

Fuller Labs 311
Thursday 6–8:50

Each project will be spread over portions of three weeks. The first week, we will discuss the design goals in class.

Students may form into teams of two (three only if necessary), but do not use the same partner in two projects in a row. Each team will also serve as the *antiteam* for another team on this project.

The second week, each team will post its code, and submit its security design document. The security design document can be fairly short, but it must explain:

1. the adversary capabilities expected, and the goals of the adversary (his payoffs).
2. the system goals, briefly summarizing the intended functionality, and emphasizing the security goals you want to achieve.
3. user profile: What do you expect the user to do to keep your system secure, and why do you think the user will want to do that? Why do you think the user will know how to do that?
4. security mechanisms: What mechanisms does your project use to achieve its security goals?

At the end of the second week, each team will pass their code and description to their antiteam. The antiteam will prepare a critique for week three, which may include attacks on the system.

The third week, the antiteams will report:

1. problems about the security goals. Do they cover the important needs? Is the attacker model too weak (too optimistic for the designer)?

2. other mechanisms that could be used to achieve the goals.

3. problems with achieving the goals with the team's mechanisms.

4. attacks found, if any.

Grades for each team will reflect the quality of its work in the design/implementation phase, and as antiteam in the critique phase.

There will be four main projects. Topics will include:

1. An encrypted password wallet

2. A distributed filesystem using TLS

3. A network-accessible front end: authentication, access control, input validation

4. Final project: To be decided team-by-team