CS 1653: Applied Cryptography and Network Security
Term Project, Phase 1

Lindsey Bieda leb35@pitt.edu Tucker Trainor tmt33@pitt.edu

January 19, 2012

Section 1: Group Information

Lindsey Bieda leb35@pitt.edu
Tucker Trainor tmt33@pitt.edu

Section 2: Security Requirements

General Properties of Secure File Sharing

A bulleted list of properties that should apply to *any* such file sharing system.

- **Property 1: Correctness.** Correctness implies that if file *f* is shared with members of group *g*, only members of group g should be able to access *f*. The notion of "access entails the creation, modification, and deletion of *f*, as well as the ability to see that *f* even exists. Without this requirement, any user could access any file, which is contrary to the notion of group-based file sharing.
- **Property 2: Open verified software.** Open verified software implies that the software installed on the system will be open source and heavily validated and supported by the community in order to ensure both correctness and security. Open verified software provides transparency in source code and by extension software, allowing enhanced security over black box software.
- **Property 3: User verification.**
- **Property 4: Strong login protocols.**
- **Property 5: Physical system protections.**
- **Property 6: Connection restrictions.**
- **Property 7: User roles.**

- **Property 8: Permission levels.**
- **Property 9: Password integrity (and authentication).**
- **Property 10: User/group uniqueness.**
- **Property 11: Filename uniqueness.**
- **Property 12: File integrity.**
- **Property 13: File restrictions.**
- **Property 14: download integrity.**

System Assumptions & Threat Models

A paragraph informally describing the trust assumptions that you are making regarding the players in the system. This could, for example, be a description of the system model in which you envision your application being deployed.

- A
- B
- C