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

System Assumptions & Threat Models

Preventing malicious users from accessing the system or authorized users from defacing existing data.

1. **Property 3: User verification.**
2. **Property 10: User/group uniqueness.**
3. **Property 4: Strong login protocols.**
4. **Property 6: Connection restrictions.**
5. **Property 9: Password integrity (and authentication).**
6. **Property 11: Filename uniqueness.**
7. **Property 5: Physical system protections.**

Privacy and isolation of files must be ensured if users are to trust the file sharing system.

1. **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.

2. **Property 8: Permission levels.**

3. **Property 12: File integrity.**

4. **Property 13: File restrictions.**

5. **Property 7: User roles.**

6. **Property 14: download integrity.**

7. **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.