Section 1: Group Information

Mark Shanoudy

- mhs38@pitt.edu

Rich Mau

- rim20@pitt.edu

Section 2: Security Requirements

- Create/delete users
- Create/delete group
- Add/remove user *u* to/from group *g*
- Upload/overwrite file *f* to be shared with members of group *g*
- Download file *f*
- Delete file *f*
- Unique accounts which consist of ID's and passwords
- Group administers to manage groups on group server
- Upload/overwrite file *f* to be private to unique user
- User identity validation to access system and any groups/files
- User login information is encrypted
- 2-step validation required to log in to group server by administrator *a*
- Channels between client application and group servers are encrypted
- Group server and Files servers are not accessible directly from the internet
- Client application has a timeout function
- Only one user can be logged into client application on any given machine
- User cannot be logged into multiple client applications at the same time
- User *u* cannot add/remove other users in the same group *g* without administrative privileges
- Users required to have strong passwords (8-12 characters, at least 1 special character, and at least 1 number)
- Limited amount of login attempts per user account
- User account creation is done by administer
- Administrator can restrict what File Servers users can view

Threat Model #1: Group Spoofing

In this threat model, it is assumed that malicious users will attempt unauthorized access to files on the file server via spoofing. In this case, a malicious user will attempt to use the same group name from a different group server on a file server or even from the same group server.

- **Property 1: Connection**. Connection refers to the unique connection between a group server to file server. For example, group server *A* cannot connect to file server *Z* if file server Z already contains a unique addressing to group server *B*. This is important because different group servers manage different groups, so if group server *A* was hosted by a malicious user, then the malicious user can use the same group authentication to freely access all files on the file server.

- **Property 2: Uniqueness**. Uniqueness implies that groups on the group server are unique such that no two group names are the same. This will reduce confusion among users and prevent unauthorized access of files on the file server. This goes hand and hand with Correctness, though different in that this property addresses conflicting groups on the file server. Without Uniqueness, unintentional tampering of files on the file server will dramatically reduce system effectiveness. For example, if this file called 'project_1.doc' were uploaded on a file server under the group name 'Rich and Mark', another group name (although not likely) named 'Rich and Mark' will inadvertently tamper with the file, thereby losing file integrity.
- **Property 3: Renewal.** Renewal refers to the property of updating membership of groups on the group server in order to prevent "ex-group" members from maliciously tampering with group files. For example, if Alice was kicked out of the group then Alice should not have access to the group files on the file server, for this, a state of membership must be thoroughly maintained-- otherwise, Alice may tamper or disclose information and distribute the group files.

Threat Model #2: Tampering of Data Sent to Server

In this threat model, it is assumed that a malicious user will attempt to capture and modify legitimate user data while it is being sent to and from the server via the client application. In this case, an attacker could either capture the data and modify it in a way that corrupts the data or replace the data with malicious code.

- **Property 1: Authentication**. Authentication refers to the ability for both the client application and the servers to confirm that network traffic is both legitimate and correct. Legitimacy and correctness refers to the notions that files may become corrupted through network jitter/failures or malicious attacks and must therefore be checked through a system similar to tcp. Without this requirement, files could potentially be corrupted or manipulated through the network.
- **Property 2: Cryptography**. Cryptography refers to the notion that data sent over the network will be encrypted. The attacker may be able to capture information as it is being transmitted over the network from the client application to the servers. However, if the data being intercepted is encrypted then the attacker will be unable to modify or even read it. Without this requirement, attackers could intercept and manipulate data.
- **Property 3: Data Masking**. Data masking refers to the notion of masking sensitive data from users in the system -- especially during data transfer. Sensitive data can include things like ssn, bank accounts, etc. For instance, if a malicious user should intercept and decrypt data during transfer over a network, that malicious user would not have access to sensitive data that could then be manipulated in the message. Without this requirement, sensitive data could potentially be vulnerable to tampering.

Section 3: References

http://msdn.microsoft.com/en-us/library/ff648644.aspx#c03618429_005
http://msdn.microsoft.com/en-us/library/ff648641.aspx
https://www.owasp.org/index.php/Threat_Risk_Modeling
http://en.wikipedia.org/wiki/Data_security