Vault 5431 - Requirements

Alicia Wu, Britney Wong, Chang Yang Jiao, Paul Chesnaisa

March 17, 2016

1 Personel

Alicia Wu (yw344), Britney Wong (bmw227), Chang Yang Jiao (cj285), Paul Chesnais (pmc85)

2 System Purpose

Signing into services is one of the most common security features for keeping the confidentiality of the user on the Internet. However, for security purposes, passwords ought to be both hard to discover and used only once for each service. In order to increase user psychological acceptability, this system provides a "vault" for the users to both generate more complex passwords and to confidently store all passwords in a secure manner, both of which may be accessed from anywhere and any device.

3 Functional Requirements

3.1 User Types

User User of Vault5431 with the ability to view, add, modify, and/or delete existing passwords, to view application logs, to change his/her vault's master password, change vault settings, and to securely delete his/her personal vault.

3.2 Assets

- Passwords
- Master Passwords
- Phone Number
- Vault settings
- Vault Event Log
  - User actions
  - Changes in password vault
  - Changes in settings
  - Login IPs
- User identity
  - User first and last name
  - Email
  - Billing address
  - Credit card information

3.3 Function Requirements

Please refer to to Table **??** for user stories.

4 Threat Analysis

- Disgruntled employees (Internal Threat) - This kind of threat is motivated by personal vendettas against the company (or in this case the system since there is no company). The employee is likely to want to see this system fail and will have access to either the source code or the server. They will have moderate to high skill level, as well as the number of resources.
- Personal enemies (External Threat) - This kind of threat is motivated by personal vendettas. They seek to obtain or modify the passwords of people they know. By doing so, they can get all kinds of information on their enemies, limited only by what kinds of passwords are stored in the vault (e.g. bank account password, email password, etc). They will have low to moderate skill level and a limited number of resources.
- Organized crime group (External Threat) - This kind of threat is often motivated by personal gain. They seek to obtain the passwords of all users of this system. With those passwords, they can access all online accounts that are stored in the manager. This could cause damage in all levels of the harm spectrum, ranging from stealing someones money to sending a bad email. They will have high skill level and moderate number of resources.

5 Security Requirements

5.1 Asset Analysis

Asset	Stakeholder	Value
Master Password	User	Allows user to log into the vault and get access to stored passwords, settings, etc
Stored Password	User	The main assets of the user. allows user to log into other online accounts
Setting - Phone Number	User (Privileged Mode)	Allows user to use 2-factor authentication
Setting - Notification	User (Privileged Mode)	Allows user to be notified of suspicious activity, change paranoia level, and unfreeze my own vault if it got frozen by a hacker
Vault Event Log	User (Privileged Mode)	Allows user to view event log of actions made under his own account. this is useful for checking suspicious activity
Secure Notes	User	Allows user to store things other than passwords, such as bank account number

Table 1: Asset Analysis

5.2 Harm Analysis

Master Password

- Unauthorized changes of the master password will cause the user to lose access to the entire vault, thereby rendering all of his online accounts useless and compromised.
- The user would also lose confidentiality would be damaged because sensitive information stored in the vault, such as phone number, credit card, and IP addresses will be revealed (event log).

Stored Password

- Unauthorized viewing of the stored passwords will cause all services stored user information to be compromised.
- Unauthorized changes of the stored passwords will cause the user to lose access to the accounts to which the passwords belong.

Setting - Phone Number

- Unauthorized viewing of the a users phone number will cause the users identity to be compromised.

Setting - Notification

- Unauthorized changes to a users notification settings will cause user to lose control over his vault. For example, if the user prefers a certain paranoia level, which controls the amount of simultaneous accesses and number of mistakes allowed, and an unauthorized user changes the level to less secure, the user becomes more likely to lose access to their vault.

Vault Event Log

- Unauthorized viewing of the vault event log will cause the users location to be revealed. The log will most likely contain the IP addresses of users, which could be exploited by malicious parties and lead to physical danger to the users.
- Unauthorized viewing of the vault event log will cause the users usage and habits to be revealed.

Secure Notes (Optional)

- Unauthorized viewing of secure notes such as bank account numbers will cause the user to lose confidentiality of his secure notes, which could cause other harm such as money theft.
- Unauthorized modification of secure notes such as bank account numbers will cause the user to lose access to his own bank account.

5.3 Feasibility Analysis

The security goals documented below are important aspects of our system and therefore the goals defined should be feasible against threats with limited resources and skill level. For now, we are not guaranteeing security against availability attacks (like DDOS) attacks, though we would want to in the future.

The system will also not protect confidentiality violations made by the users themselves, such as distributing their passwords to their friends via other means.

5.4 Security Goals

- The system shall not reveal the master password of any account to unauthorized users. (Confidentiality)
- The system shall not reveal any stored passwords to unauthorized users. (Confidentiality)
- The system shall prevent unauthorized users from modifying the master password that would lead to locking out the authorized user from his own vault. (Availability)
- The system shall prevent unauthorized users from modifying any of the stored passwords in a vault. (Integrity)
- The system shall only allow the owner of the vault/account to modify any of the settings. (Integrity)
- The system shall only allow authorized users to view the vault event log. (Confidentiality)
- The system shall not allow any user to modify the vault event log. (Integrity)
- The system shall prevent unauthorized users from viewing the secure notes. (Confidentiality)
- The system shall prevent unauthorized users from modifying the secure notes. (Integrity).
- The system shall prevent unauthorized users from viewing a user's phone number. (Integrity)

6 Essential Security Elements

Authorization All users must be authorized to perform certain actions. Privileged users can get access to things such as event logs and special accounts settings like paranoia level. Regular users can access, modify, and delete stored passwords, as well as use the password generator. It is necessary to establish authorization in order to distinguish between the different privilege settings for different users.

Authentication All users are authenticated by logging into their vault with their username and master password. This is a necessary checkpoint that all users must pass in order to reach their vault.

Audit All user activities such as logins, password modifications, and settings changes, will be logged so that privileged users can view everything that occurs in their vault. This will help users catch unauthorized access to their vault by malicious principals.

Confidentiality This system must provide confidentiality to user information and passwords because the nature of the system is to store sensitive passwords that should only be accessed by those to whom the passwords belong. This password manager will address confidentiality in the following ways:

- All passwords being stored are kept confidential.
- Account settings can only be made known to the user himself.
- Event logs can only be read by the user.
- All user information, such as phone number, cannot be revealed.
- The algorithm for generating passwords is kept secret.
- The master password is not known to the password manager; only the user knows it.

Integrity This system must provide integrity to the stored user passwords, user settings, master encryption, and account information. The password manager will address will address integrity in the following ways:

- All passwords being stored cannot be modified except by authorized and authenticated users.
- Account settings cannot be changed except by authorized and authenticated users.
- Event logs cannot be modified by anyone.
- The master password and account information cannot be changed except by authorized and authenticated users.
- The encryption to get into the vault cannot be modified.

User Type	Assets	Importance	User Story
User	Master Password	M	As a user, I can access the vault using my master password.
User	Stored Password	M	As a user, I can view my stored username and passwords.
User	Stored Password	M	As a user, I can modify any stored username and password.
User	Stored Password	M	As a user, I can delete any stored username and password.
User	Stored Password	M	As a user, I can add new username and passwords to my vault.
User	Stored Password	S	As a user, I can randomly generate a password for use on a website.
User	Stored Password	C	As a user, I can check the strength of any stored password.
User	Setting - Phone Number	S	As a user in privileged mode, I can use my phone number as a secondary security feature.
User	Setting - Phone Number	S	As a user in privileged mode, I can change my phone number attached to the vault.
User	Setting - Notification	C	As a user in privileged mode, I can set notifications when unusual activiites are detected.
User	Setting - Notification	S	As a user in privileged mode, I can change the preset paranoia level.
User	Setting - Notification	S	As a user in privileged mode, I can unfreeze my vault if a hacker freezes it with too many login attempts.
User	Vault Event Log	M	As a user in privileged mode, I can view which passwords were accessed.
User	Vault Event Log	M	As a user in privileged mode, I can view which passwords were modified
User	Vault Event Log	M	As a user in privileged mode, I can view which passwords were deleted
User	Vault Event Log	C	As a user in privileged mode, I can view where my vault was accessed.
User	Vault Event Log	C	As a user in privileged mode, I can view when my vault was accessed.
User	Vault Event Log	M	As a user in privileged mode, I can view changes in my vault settings.
User	Stored Password	C	As a user, I can share passwords/secure notes with other users (e.g. family members)
User	Stored Password	W	As a user, I can generate pronouncable passwords
User	Secure Notes	C	As a user, I can store arbitrary information (bank account numbers, social security numbers etc)
User	Stored Password	W	As a user, I can track the password history for a given site

Table 2: Functional Requirements