Milestone 2 Requirements

Personnel

Mitchell Vogel, mjv58
Kyle Donahue, kjd88
Chie Shu, cs794
Kenta Labur, kl459

System Purpose

Our system will be a password manager targeted for individual users. Users will use it to securely store their usernames and passwords for other websites and services (hereafter referred to as “stored credentials”) in a way which removes the burden from them of remembering a large number of unique passwords, while also having the security associated with using strong and unique passwords for all of their accounts. Users’ stored passwords will be associated with a single account accessed through a username and master password (together referred to as the “master credentials”). After authentication with that set of master credentials, users can view, modify, or delete the stored information associated with their account.

System Backlog

User Types: Personal User, Admin User
Assets: Master credentials(user/admin level), Stored credentials, system logs, user logs
User Story:

User Type	Assets	Imp.	User Story	Complete?
Personal	Master Credentials	M	The user enters the master credentials on a desktop client. If this set of credentials is verified as correct by the server, they are able to retrieve their stored account credentials.	Yes
Personal	Stored Credentials	C	When the user has already entered the master credentials, their stored credentials are automatically filled out while they visit websites using their browser.	No
Personal	Account	M	Anyone with the appropriate client software can create an account.	Yes
Personal or Admin	Master Credentials	M	A user can change his master password (not the username) after authenticating with the old master credentials.	Yes
Personal or Admin	Master Credentials	S	If the user forgets his master password he can reset it to a new master password after a multi-factor authentication process	No
Personal	Stored Credentials	M	An authenticated user can update a password associated with any of his current stored credentials	Yes

Personal	Stored Credentials	M	An authenticated user can add a new account credential	Yes
Personal	Stored Credentials	C	A user may choose to secure certain stored credentials with another master password, different from their main master password	No
Administrative	System Event Logs	M	The admin can view changes, deletions, or removal of users' stored passwords and changes to their master passwords.	Yes

Threat Analysis

Malicious Admins

A malicious admin has a server which is running our software or a version of our software. They are able to view the data stored and make arbitrary manipulations to it. In addition, they have considerable computing power at their disposal. They are motivated by the desire to steal account credentials from unsuspecting users, by convincing them that their server is a secure installation of our software and then obtaining plaintexts from the client's usage of the system. We assume that the Malicious Admin does not control the client-side software: this would give them the ability to completely control the operation of the system, which negates any threat analysis. A second case which is considered Malicious Admin is that where the server is compromised by an attacker who assumes full or partial ability to read its files and control its activity or by gaining access to an administrative account.

Dolev-Yao Attacker

A Dolev-Yao attacker has access and privilege to all intervening networks but not the server or the client software/hardware. They can view, store, and modify any data transferred over the network, and they may have access to considerable computing power. They have a motive to retrieve and/or modify stored/master credentials stored on the server, because these credentials can be used for financial or personal gain.

User-Side Social Engineering

A social engineering attack will most likely take the form of an attacker sending an email or somehow otherwise contacting the owner of an account in our system. In this contact, the attacker will attempt to impersonate an administrator of the system and will request the user's master credentials. The attack can also take the form of an attacker pretending to be the owner of a particular account and request a change in the master password. This type of attacker will focus on single users, in contrast to the previous two who cast a wide net.

Security Goals

1. Stored credentials shall not be disclosed to any entities other than the owner of the credentials. In particular, the server admin should not be able to read them in plaintext. (Confidentiality).

2. Stored credentials shall not be modified by any entities other than the owner of the credentials or the admin (Integrity).

3. Changes to stored credentials should be detectable by the user, and associated with a specific record in their user log (Accountability).

4. Only users will have access to their own master credentials (Confidentiality).

5. System logs should not be readable by users (Confidentiality).

6. Only the owner of an account (user or administrator) can reset or change the master password for that account. If the user forgets their password, they should be able to reset it to some new password so they can continue to access their account. No other entity should be able to deny access to the account by changing its password (Confidentiality, Integrity, Availability).

Essential Security Elements

1. Authentication: In order to view, modify, or delete account data, users or administrators must be properly authenticated with their master account credentials. Otherwise, any user could change data that does not belong to them.

2. Authorization: Users are authorized to view, modify, or delete only the data associated with their accounts. Administrators are authorized to perform those actions and to view the system logs.

3. Audit: Administrators are able to track accesses/changes to users' master and stored credentials. Administrator actions (viewing/modifying accounts and credentials) are also tracked in a log.

4. Confidentiality: The data stored in the system is information that provides access to users' other accounts, be they credentials for online banking or for Netflix. If the confidentiality of this information is breached then attackers can access any of these accounts and cause extensive harm to those accounts.

5. Integrity: If the data stored by the system (i.e. the stored credentials) are modified on our server, it becomes likely that the user can no longer access many of the accounts for other services, such as Facebook, Netflix, or their online banking information. If users are relying on our system as the only way to remember a multitude of credentials, then any modification of these credentials could deny users access to other services. If logs are modified, then a system administrator trying to restore user data or detect attacks would be working off of false data and accountability would be lost.