Security Analysis

PassV

August 10, 2022

1 Assets

A set of descriptions concerning the functionality of the PassV application components.

1.1 Internally developed software

In this regard, Browser Extension as the main client interface, which will provide the entire login segment from the client and server side, and additional usability related to the usage of the vault and user data management. In addition, the single page website structure of the application, in terms of interface readability, general access to website functionality and its security mechanisms.

1.2 Central server deployment

The server is the core of PassV application. Server performs the functions of communication with data base, single-page website and web extension. Server validates user's credential before allowing access to logins. It is responsible for managing user accounts and storing vault data to enable seamless synchronisation between different client devices. User authentication is handled by the server using JSON Web tokens. The server is hosted, which may create certain threats such as server downtime, denial of service, described in the section below.

2 Threats

- Theft of users device - victims of laptop theft are at risk of losing hardware, software and important data that has not been backed up. Thieves can also gain access to sensitive data and personal information. If a user's device is stolen, all locally stored data is exposed. Web extension keeps confidential data locally.
- User impersonation - type of fraud where an attacker poses as a trusted person to steal sensitive information. Attacker might use Cross-Site Request Forgery (CSRF) attack that occurs when a malicious program causes a user's browser to perform an unwanted action on a trusted site when the user is authenticated. This attack can be thwarted if proper authentication is used.
- Rouge server instances - the general set of situations where a DHCP server is used outside the control of network administration. That is for example assigning invalid IP adresses, overall distruption of network connection, preventing other devices from accesing the network services.
- Unauthorized access to server - unauthorized access occurs when somebody gains access to a server using somebody else's account or other methods. For example, when someone guesses the password or username for an account that does not belong to them until they gain access, this is considered as unauthorised access.
- Denial of service - DOS occurs for example when somebody tries to send too large of a file for the server to handle so the service is temporarily unavailable.
- Programmer error - type of error done by programmer which can result in compromising the security of the system.

- Server downtime - a situation where the server is not online thus when user tries to connect to his online vault, it is not possible.
- Weak password requirements

3 Controls

3.1 Theft of users device

- Locally stored data is encrypted by the master password. Master password is never stored on the device, it is only known by the user.
- Storage encrypted locally (plaintext visible only when logged on)
- Secure cryptography standards (AES, Argon2)

3.2 User impersonation

- CSRF protection

3.3 Rouge server instances

- Server-specific logins (domain in hash), when authenticating to the server, web extension generates a password based on the domain
- Server only receives encrypted data
- Certs

3.4 Unauthorized access to server

- Server validates credentials before allowing access to logins
- User authentication and authorization via JWT
- Standard user limited privileges
- Local admin auth only

3.5 Denial of service (large data uploads)

- Per account quota
- Mail required for registration
- Active monitoring (data size) and automated response

3.6 Programmer error

- CI, testing pipeline

3.7 Server downtime

- Architecture enabling high availability, redundancy and load balancing

3.8 Weak password requirements

- Minimal security requirements imposed by the generator
- User data protection in PassV begins at the moment a user creates an account and a Master Password.
- PassV includes a Password Strength Meter as a guide that will assess and display the overall strength of the Master Password being entered to encourage for a stronger password.
- If user attempt to sign up with a weak password, PassV will be notifying that the Master Password chosen is weak. Best Practices for Password Management from NIST Special Publication 800-63B - Digital Identity Guidelines - Authentication and Lifecycle Management, we see a set of informative recommendations on password security.
- We offer additional measures, such as two-step login, to help the user maintaining the account's security, but the content of the account and its security are up to the user.
- After creating your account and specifying your Master Password, PassV next generates several keys that are used in protecting your account's data.
- protection via hard memory function

4 Cryptography overview

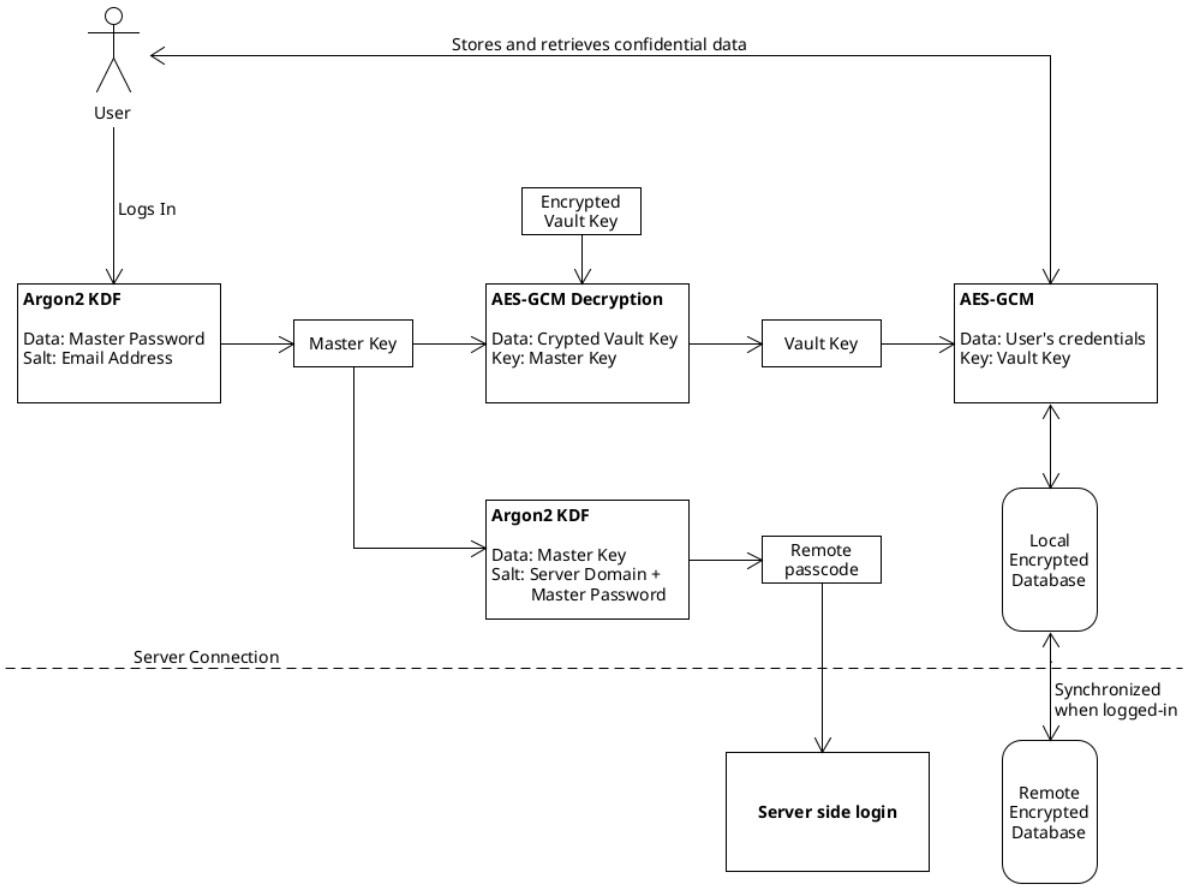
The below diagram is a short overview of password and data handling within PassV components. On the client side Argon 2 key derivation function is used to derive individual keys, while AES-GCM with 256-bit keys is used for actual encryption and decryption of both the vault key as well as all user supplied passwords and data.

The entire system relies on a single, strong master password created by the user initially during sign-in.

The master password combined with the user's email address are then used to derive both the intermediate vault encryption key as well as the server passcode. For additional security server passcode is also derived from server's domain name. This prevents secret reuse when multiple servers are accessed by the user.

To enable storage and retrieval of data on the client side an encrypted, random vault key is decrypted using the previously derived intermediate key. This key is used for encryption of the majority of data contained in each database entry apart from the unique identifier as well as the access time.

Since no unencrypted confidential information is stored by the client on disk, entries shared with the server during synchronisation are largely identical to those stored in the persistent localstorage-based database.


User
Stores and retrieves confidential data
Logs In
Encrypted Vault Key
Argon2 KDF
Data: Master Password
Salt: Email Address
Master Key
AES-GCM Decryption
Data: Crypted Vault Key
Key: Master Key
Vault Key
AES-GCM
Data: User's credentials
Key: Vault Key
Argon2 KDF
Data: Master Key
Salt: Server Domain + Master Password
Remote passcode
Local Encrypted Database
Server Connection
Synchronized when logged-in
Server side login
Remote Encrypted Database