

PC Building App
Design System Controls & Security
Keith Holcomb

Integrity Controls

1. Input Controls.

- Value Limit Controls.

Must limit controls will be during account creation.

Ex. Usernames should be between 8 and 32 characters in length, and not already be taken in the database.

Ex. Passwords should be between 8 and 100 characters in length, as well as contain an uppercase, lowercase and digit character.

- Completeness Controls.

For a PC Build Lists/Guide to be considered finished, it must actually have all the parts a PC requires (CPU, Motherboard, RAM, etc). A list/guide will provide a means of adding any necessary parts it's missing until they are all added.

- Data Validation Controls.

Ex. When creating a PC Build List, the type of the list must be either List or Guide. This input is validated via radio buttons, and an exception will be thrown if another input is listed.

- Field Combination Controls.

Ex. When creating a PC Build List, the date created should be the day the list was created. This value is not meant to be modified after creation. A modified date is instead changed whenever the list gets updated to show the last day the list was modified.

2. Access Controls.

PC Building App
Design System Controls & Security
Keith Holcomb

- User accounts are the primary access controls for the PC Building App. Users without an account don't have much access to the DB compared to those that do have an account.

- Unregistered Users Access.

All users, regardless of having an account in the DB, can view the PC part catalogue (table for PC Parts) as well as PC Build Guide viewing, but do not have access to editing any DB tables (outside of creating an account).

- Registered Users Access.

When a user is registered with an account, their account is stored in a DB table.

The registered user then can view the PC part catalogue, PC Build Guides and can create PC Build Lists (stored in a DB table), and can edit any PC Build Lists tied to their accountID.

3. Transaction Logging.

- Since the user only has access to editing one table in the DB, it isn't necessary to implement transaction logging within the DB, although PostgreSQL has some automatic transaction logging within the PGAdmin 4 interface.

4. Complex Update Controls.

- Since only a single user has access to their own PC Build Lists, there shouldn't be an instance where a PC Build List (the only updatable part of the DB) would be edited simultaneously. Assume that the user is only logged in on 1 instance at a time.
- Since accounts can be created simultaneously on multiple clients, a lock could be created when a user specifies to create an account. This lock could ensure that

PC Building App
Design System Controls & Security
Keith Holcomb

only one device is binding credentials to a single accountID. In the event another account is being created when there is a lock, that second account should be assigned a different accountID.

It is very unlikely that multiple accounts will be created at the exact same time, and PostgreSQL has some automatic checks to ensure some errors don't occur when this does happen.

5. Redundancy, Backup, and Recovery.

- Backups to the DB should be configured to be created every 24H, to ensure there is a way to recover the DB in case of an emergency. This backup would simply be on the device running the PostgreSQL server.

6. Output Controls.

- Since there isn't a product being outputted by the PC Building App, there aren't many output controls.
- Access Controls, such as user accounts, limit what info is available to unregistered clients, while providing registered clients with a way to view and edit their own PC Build Lists.

Security Controls

1. Access Controls.

- Authentication (user accounts). With the PC Building App, users will require a registered user account to create and edit PC Build Lists/Guides. User accounts require a username and password to login to. There is no multi-factor authentication with this application.

PC Building App
Design System Controls & Security
Keith Holcomb

- Access control list. The access control list for the PC Building App is very simple, in that there are only registered and unregistered clients. If a client is unregistered, the only access it has is to viewing the PC parts catalogue (table of PC parts). If a client is registered with an account, it has access to viewing the PC parts catalogue, as well as access to viewing and creating PC Build Lists/Guides that are tied to their account.
- Authorization. A user must be authorized with an account in order to create or edit PC Build Lists.
- Unauthorized, Registered, & Privileged Users. An unauthorized user is any client that does not have an account in the DB. A registered user is a client that has logged into an account in the DB. A privileged user would be someone able to access the physical computer running the MySQL server (myself).

For the scope of this project, there is another privileged user, which is the PC Building App. The app itself has the info needed to log into the database and have full read/write access.

2. Data Encryption.

- The only data that needs to be encrypted within the PC Building App is user created passwords. Account creation requires a password and a password confirmation from the user.

An encryption is necessary to ensure the user's password isn't compromised in any way.

The encryption uses SHA-256 byte conversion as well as Hexadecimal conversion. These conversions are run within the application and the final

PC Building App
Design System Controls & Security
Keith Holcomb

hexadecimal is sent to the DB. When logging in, the application will get the hexadecimal in the DB and compare it to the hexadecimal it creates from the user input, and if these match, the user logs in.

3. Digital Signatures and Certificates.

- The PC Building App doesn't have any need in having nor providing digital signatures or certificates.

4. Secure Transactions.

- Since there are no purchases made directly within the PC Building App, there is no need to provide details for secure transactions within the application or DB.
- A potential extension to the application could be providing affiliate links, which would need to be secure links that allows the user to visit a manufacturer's website or storepage.