Hazard Analysis
Sayyara

Team 3, Tiny Coders
Arkin Modi
Joy Xiao
Leon So
Timothy Choy

October 18, 2022

Table 1: Revision History

Date	**Developer(s)**	**Change**
October 13, 2022	Arkin Modi	Create Failure Mode and Effect Analysis table
October 14, 2022	Joy Xiao	Introduction
October 15, 2022	Leon So	Update Failure Mode and Effect Analysis table
October 16, 2022	Arkin Modi	Fill in FMEA table for Work Orders, Shop Profile, Services, and Shop Employees
October 17, 2022	Timothy Choy	Add Safety and Security Requirements

Contents

1 Introduction

This document outlines the hazard analysis of Sayyara. The definition of hazard is any property or condition in the system along with conditions in the environment that may cause harm or damage. This definition is from Nancy Leveson's work. The hazards for Sayyara include security and usage hazards such as protecting personal information, database failures, and having no internet connection.

2 Scope and Purpose of Hazard Analysis

The scope of the hazard analysis is to identify any hazards that may arise when using the application, their causes, coming up with steps to eliminate or mitigate the effect of the hazard. The purpose of the hazard analysis is to pinpoint areas where hazards may arise and their effects and come up with mitigation steps. Through completing the hazard analysis, safety and security requirements will be developed early in the design process to minimize the risk of having hazards occur without plans in place to reduce or mitigate the effects.

3 System Boundaries and Components

The system consists of:

1. The application's front-end and back-end components in the major categories:
    - Authentication
    - Appointments
    - Quotes
    - Work Orders
    - Shop Profile
    - Services
    - Shop Employees
2. The database being used which will store all of application's data

4 Critical Assumptions

- Assume the users of the application are not intentionally trying to misuse it
- Assume that the user will follow cybersecurity best practices

5 Failure Mode and Effect Analysis

Table 2: Failure Mode and Effect Analysis Table

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref.
General	Loss or theft of Personal Identifiable Information (PII)	Legal consequences	a. Malicious internal or external actors gains access to the system b. SQL inject attack	a. Encryption of PII data at rest and in transit	a. SR1	H1-1
Authentication	User cannot login	User is unable to access their account and application features requiring login	a. User inputted login credentials do not match the credentials in the database	a. Allow user to reset password	a. SR2	H2-1
	User account is hacked	Unauthorized actions may be performed from the hacked account	a. Malicious internal or external actors gains access to the user account	a. Allow user to reset password b. System administrators to undo/revert unauthorized changes	a. SR2	H2-2
Appointments	Multiple appointments are scheduled for the same time	Conflict in scheduling and availability	a. Two or more users attempt to schedule an appointment for the same time slot at the same time	a. The shop owner or employee will accept one of the appointments	a. SR3	H3-1
Quotes	Chat is disconnected	Loss of chat history, new messages sent may not be received	a. Loss of internet b. Inactive or stale connection c. Web socket failure	a. Notify user of chat disconnection b. Cache latest messages, disable send button	a. SR4 b. SR5	H4-1

Work Orders	Work Order is missing	Customer and Employees will not know any of the work that has been done for a specific job	a. Database failure	a. Regular and automatic database backups/snapshots and allow shop owners to request rollbacks	a. SR6	H5-1
	Work Order is missing detailed information	Customer and Employees will not know all of the work that has been done for a specific job	a. Database failure	a. Refer to H5-1a	a. SR6	H5-2
Shop Profile	Unable to find details of a shop	Customers will not be able to see the information about a specific shop (e.g., address, phone number, etc.)	a. Database failure	a. Refer to H5-1a	a. SR6	H6-1
Services	Unable to find a service	Customers and Employees will not be able to see what services are offered by the shop	a. Database failure b. Client-side network failure	a. Refer to H5-1a b. Display a message to the user informing them that they are offline	a. SR4 b. SR6	H7-1
	Unable to find details of a service	Customers and Employees will not be able to see the details of a service (e.g., price, estimated time, etc.)	a. Database failure b. Client-side network failure	a. Refer to H5-1a b. Refer to H7-1b	a. SR4 b. SR6	H7-2
Shop Employees	A former employee joins the shop account	The former employee can view sensitive information and perform unauthorized actions	a. A former employee accepts their invite link to join the shop as an employee after their employment has been terminated	a. Invite links should expire after a set period of time b. Invite links should only be able to be accepts once c. Shop owners should be able to revoke access to any employee	a. SR7	H8-1

	An employee of the shop cannot be found	Shop owners will not be able view employee's details; Effected employee will not be able to be assigned to work orders or view their profile details	a. Database failure b. Client-side network failure	a. Refer to H5-1a b. Refer to H7-1b c. Employees should be able to be reinvited to a shop	a. SR6 b. SR8	H8-2

6 Safety and Security Requirements

SR1. The system shall protect personally identifiable information (PII) by encrypting information both at rest and in transit

Rationale: There are legal consequences associated with losing people's PPI.

Associated Hazards: H1-1

SR2. The system shall allow the user to reset their password

Rationale: If a user forgets their password, they will be unable to access information regarding their work. Furthermore, losing access to their account due to a malicious actor would allow unauthorized people access to components that require a level of authorization.

Associated Hazards: H2-1, H2-2

SR3. The system shall allow the shop owner or employee to accept appointments before they are finalized

Rationale: As the application is run in real time with multiple users, scheduling conflicts can occur if multiple users fill in a time slot at the same time. Allowing the shop owner or employees to accept would remove the hazard of conflicting schedules.

Associated Hazards: H3-1

SR4. The system shall notify the user if there is no network connection, and prevent the user from using functions that require a connection when they have no connection

Rationale: A web socket connection cannot be made if there is no network connection. Letting the user know that they have no connection and disabling methods for them to use connections would prevent any hazards.

Associated Hazards: H4-1, H7-1, H7-2

SR5. The system shall cache recent chat messages

Rationale: Caching recent chat messages allows the user to keep reading their conversations, even without access to a network.

Associated Hazards: H4-1

SR6. The system shall take periodic backups and snapshots of the database and allow shop owners to request rollbacks

Rationale: It would be catastrophic to lose critical data in the case of a database failure. Having backups and snapshots would alleviate this hazard.

Associated Hazards: H5-1, H5-2, H6-1, H7-1, H7-2, H8-2

SR7. The system shall disable invite links to employees after they have been used, after a set period of time, or if the shop owner revokes access

Rationale: Having an invite link stay after its intended duration would cause problems, such as accidentally allowing former employees back into the shop.

Associated Hazards: H8-1

SR8. The system shall allow multiple invite links to a single employee, though only one invite link can be valid at any given time

Rationale: There could be a situation where a database failure, or human error cause an employee to be unable to accept their first invitation. Allowing multiple invite links to the same employee

would resolve this hazard. Allowing only one valid link at any time would prevent malicious actors from using links that were not meant to be used.

Associated Hazards: H8-2

7 Roadmap

[Which safety requirements will be implemented as part of the capstone timeline? Which requirements will be implemented in the future? —SS]

[The Roadmap is where you can explain which safety requirements will be implemented during the course, and which will be "postponed" until after the course. —SS]