CS-255

Project Two Speaker Notes

Mark Rossmiller

**[SLIDE 1]**

DriverPass System Analysis:

In this presentation, I will review some of the software requirements for the DriverPass system we have modeled in order to realize your vision to help future drivers to pass their DMV exams.

**[SLIDE 2]**

System Requirements:

Usability: our system for DriverPass is designed to be functional from an end-user standpoint. The GUI is meant to be intuitive and not cluttered with an overwhelming number of options. We did this by including only the bare minimum of system requirements and lessening the feature set.

Reliability: we suggest implementing the system server on an ISP with limited downtime in order to keep the system online as often as possible and not to be affected by too many system updates and server maintenance. Possibly the server should be implemented under AWS or a similar cloud service provider to limit the amount of downtime the system may experience.

Authentication: The system will authenticate users via password with 2-Factor Authentication using SMS on a mobile phone to help validate user login. This increased security feature will help keep attackers from accessing accounts or the payment information associated with them.

Audit Tracking: The owner of the DriverPass system will have complete access to changes made and who made them in an Excel spreadsheet available on-demand.

**[SLIDE 3]**

Use Case Diagram:

In this diagram, you can see the users of the DriverPass system and the actions they are able to take within that system. The actors involved in creating a working system are the client, the administrator, the secretary, the instructors, and the owner of DriverPass. Within the system are labeled such actions as loggin in, verifying credentials as well as scheduling and downloading reports. There are lines between actors involved and the actions they can take within the system.

**[SLIDE 4]**

Activity Diagram:

In this activity diagram, you can see the login sequence in action and the steps taken during a session mainly with the login sequence. If the user is not yet registered, they will be given a chance to register an account and enter in the personal information required for the secretary to activate their account. If a user already has an account and enters the correct login information, they are presented with a menu where they can implement functions using the GUI.

**[SLIDE 5]**

Security:

SSL, or Secure Sockets Layer, has been chosen to disallow eavesdropping of the connection between users of the DriverPass system and its server-side code. We use HTTPS, Hypertext Transport Protocol over SSL to keep transactions private and to help during authentication. Secure password creation will be enforced during new user registration. 2FA, 2-Factor Authentication, will be implemented using SMS on a mobile phone in order to help verify the authenticity of a user login attempt.

**[SLIDE 6]**

System Limitations:

The budget provided by DriverPass does not support long-term updates and modifications to the system, which may be required to keep the system up-to-date. The number of developers working on the project is limited, which may in turn limit the amount of work we can reliably dedicate to the developmental process. An Agile workforce is unavailable to us with our small development team, which may hamper our ability to create a product with user needs in mind. The system will not be scalable if DriverPass grows too much.