Daryl Blancaflor
Raymond Chin
Benjamin Guerrero
Carlos Lomeli

1. Introduction

Purpose: The purpose of this document is to define and analyze the features of our senior project. It focuses on providing an overall security package for a user's mobile device. The user will be able to auto-generate passwords for particular applications with filter options for special characters. The user will be able to easily manage passwords and set schedules for future password creation. In the event that the user's mobile device is stolen, they will be able to encrypt their device which cannot be uninstalled without 2-way verification. General use of the mobile application can only be accessed with a password and fingerprint authentication. The mobile application will also have geolocation to possibly locate the missing device.

Scope: This project will be a platform broken into a desktop and version with different user options depending on what device they are using. The logic will be in Java with the user interface and other visual elements will use HTML, CSS and JavaScript.

Definitions, acronyms and abbreviations:
Encryption: the process of converting information or data into a code, especially to prevent unauthorized access
Decryption: the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.

Overview: This document will first address an issue that would be remedied by the creation of this platform. Then it would envision the possible users and scenarios that this platform and application would be most effective for. It will go into greater detail of the features that will be created.

References:
Making files smaller/ overall app file smaller/ sending files to the cloud
http://www.hongkiat.com/blog/manage-cloud-files-on-android/

https://nexus5.gadgethacks.com/how-to/easiest-way-transfer-files-between-different-cloud-service-accounts-android-0155124/

https://quickblox.com/developers/Android

https://github.com/markets/awesome-ruby#cloud

https://rpgmaker.net/forums/topics/20754/

https://cloud.google.com/storage/transfer/

http://www.makeuseof.com/tag/free-storage-space-android-device/

https://developers.google.com/web/fundamentals/performance/optimizing-content-efficiency/optimize-encoding-and-transfer

https://developer.android.com/topic/performance/reduce-apk-size.html

https://android.jlelse.eu/put-your-apks-on-diet-cc3f40843c84

https://medium.com/@kevalpatel2106/how-you-can-decrease-application-size-by-60-in-only-5-minutes-47eff3e7874e

Password salting and hashing
https://crackstation.net/hashing-security.htm
Algorithms for Password hashing
http://security.blogoverflow.com/2013/09/about-secure-password-hashing/
More Alternative Password Hashing in Different Languages.
https://paragonie.com/blog/2016/02/how-safely-store-password-in-2016

Enable Geolocation Permissions:
https://stackoverflow.com/questions/34740547/how-to-enable-geolocation-permissions-for-a-website-in-firefox-profile-using-sel
Or Without Requesting Permission:
https://stackoverflow.com/questions/15017854/geolocation-without-requesting-permission
Fingerprint Authentication
http://www.androidauthority.com/how-to-add-fingerprint-authentication-to-your-android-app-747304/
Detecting Device Type for Mobile/Desktop Specific Features
https://stackoverflow.com/questions/8515161/detecting-device-type-in-a-web-application
Encrypt/Decrypt Files
https://stackoverflow.com/questions/5632658/how-to-encrypt-or-decrypt-a-file-in-java
"lock-now" files on Android
https://developer.android.com/reference/java/nio/channels/FileLock.html
Generating Passwords With Restrictions
http://theopentutorials.com/tutorials/java/util/generating-a-random-password-with-restriction-in-java/

Overwriting Passwords
https://stackoverflow.com/questions/15025502/change-password-button-how-to-overwrite-current-user-password
Creating a Website and its Database
https://msdn.microsoft.com/en-us/library/879kf95c.aspx

2. Positioning

Business Opportunity: Security is an ever present issue and in a growing digital age, the contents of a person's mobile device may contain sensitive information that can be exploited. With security being a necessity for a growing population that uses mobile devices, a security mobile application is becoming a requirement, unlike social or entertainment apps whose shelf life depends on how long they can keep a consumer interested.

Problem Statement: Almost anytime an individual is out in a public place, there is the threat of having the sensitive information on their phone stolen when the device is stolen.

The the threat of having a mobile device stolen affects everyone who is out in a public space. The impact of the problem is having the sensitive information on their device stolen. A successful solution would include the protection of the user's passwords and other information as well as the possibility of reacquiring the user's stolen or missing mobile device.

Product Position Statement: For the everyday mobile device user, the need for security becomes present once they enter a public space, especially a crowded area. This platform is a security package that provides another layer protection for their mobile device without significantly sacrificing convenience.

3. Stakeholder and User Descriptions

Market Demographics:

In a time where virtually everyone owns a smartphone, the safety of our devices has become increasingly threatened. In 2011, 33 percent of all robberies involved a stolen phone. Even more alarming, are the low rates at which those stolen phones get back to their original owners. The need for a solution gets higher everyday as phone prices continue to go up and we believe our platform has the ability to solve this crisis.
We will be able to provide a solution at little or no cost by making our software available to all phone users by providing a platform for keeping phones secure both online and in the real world. Our solution will be able to keep phones secure in a threatening world and help users with cybersecurity and locating their phone if it is lost or stolen.

Stakeholder Summary

Name	Description	Responsibilities
Software Developers	This is the individual(s) who will develop the code for the platform	Implement the platform using software. Debug software if needed
Q/A Testers	This is the individual(s) who will put the platform through it's paces and find any bugs.	Use the application and try to "break" it. Report on any found bugs.

User Summary

Name	Description	Responsibilities
New Users	End User/ Potential Primary End User	Create an account and enable certain features
Regular Users	Primary End User	Regularly use app to manually change and manage passwords

Emergency Users	Primary End User /The user's phone is stolen	Encrypt device and use GPS to attempt to track it down.

User Environment: A particular mobile device encompasses the working environment of the application with the number of users depending who is registered on the application for that particular advice. The mobile application is designed to not be too inconvenient, therefore completing a task must be swift. A user should be able to log in, quickly adjust security measures, then log out. Certain features such as geolocation may be slowed or suspended depending on internet connection.

3.5 Stakeholder Profiles:

Software Developers

Description	A content creator capable of making functional applications
Type	Basic programming language comprehension with mobile application experience
Responsibilities	● Creating product's functions ● Creating product's user interface ● Storing user information in a database ● Deploying product onto a device ● Handling user permissions
Success Criteria	Creating a finished product
Involvement	Event handling
Deliverables	
Comments/Issues	

Q/A Testers

Description	A content creator who can ensure that the product upholds particular requirements
Type	Basic programming language comprehension with mobile application experience

Responsibilities	● Using the application and trying all its features on a mobile device ● Using the application and trying all its features on a desktop/laptop ● Creating a user profile and checking its relation to the database ● Simulating a stolen mobile device by trying its emergency features
Success Criteria	The finished product does not have any issues and all actions work perfectly within a certain time limit
Involvement	Requirements reviewing
Deliverables	User data
Comments/Issues	

3.6 User Profiles

New Users

Description	A person who is downloading the application
Type	New user, minimal technical experience required
Responsibilities	● Creates an account/logs in, get user data ● Enable 2-way verification ● Enable geolocation ● install on mobile device, connect account
Success Criteria	● Installing application ● Successfully connecting account with mobile device
Involvement	● Uses the application’s features
Deliverables	● Provides confidential information to be stored into the database for future authentication ● Indicate which features will be active or inactive ● Indicate which applications will have auto-generate passwords

Comments/Issues	● Weak master password ● Unidentifiable fingerprint

Regular Users

Description	A registered user of the application
Type	Regular/casual user, minimal technical experience required
Responsibilities	● Fingerprint and PIN
Success Criteria	● Passwords are not obtainable by anyone other than the registered user
Involvement	● Uses the application's features
Deliverables	● Provides confidential information to be stored into the database for future authentication ● Indicate which features will be active or inactive ● Indicate which applications will have auto-generate passwords
Comments/Issues	● Weak master password ● Unidentifiable fingerprint

Emergency Users

Description	A user whose mobile device is stolen are now undergoing countermeasures on their desktop
Type	Regular/casual user, minimal technical experience required
Responsibilities	● Logging onto account on desktop
Success Criteria	● Passwords are not obtainable by anyone other than the registered user ● Phone is encrypted
Involvement	● Encrypt device

Deliverables	● Provides confidential information for authentication ● Give permission to encrypt mobile device
Comments/Issues	● Wifi not working for geolocation

3.7 Key stakeholder/User needs

Need	**Priority**	**Concerns**	**Current Solution**	**Proposed Solution**
Easy to Navigate and Manage	Low	Ability of users to understand how our platform works. App should be available in a way that most people can use it	UI/UX testing	Help website and help section in our app
Easy to Access	Medium	Ability to use the application quickly. App should be convenient to use.		Platform available on the web and through an app
Passwords are Auto-generated Correctly	High	Generated passwords meets security and custom filter requirements		Find and test and existing algorithm
User Meets Authentication Requirements	High	Only the registered user can log on to their account	Security questions, 2-way verification, fingerprint authentication	Secure form creation
Geolocation is Accurate	Medium	User will be able to accurately locate phone	Google Maps API	Progressive Web App properties allowing a page to load instantly

Encryption is Strong	High	An unauthorized user will not be able use the encrypted phone		Find and test and existing encryption algorithm

3.8 Alternatives and competition

Alternative to our product include Fastpass, Dashlane, and Apple's Find my Phone.Fastpass and Dashlane help users manage and create passwords but are hindered by charging people to use this app. Find my Phone influences our platform, but since it is only available on Iphone, we believe our app can do better by making a service like it available on Android as well. While these products are excellent to use on their own, we believe that our platform can beat them out in overall customer satisfaction by providing what they do on one app and also building on top of that. Our idea will take concepts thats are fragmented across multiple platforms and unify them under a single platform that will be universally compatible on smartphones instead of being exclusive to the type of phone the user has. By doing so, we expect to get many users because it will be more accepted as we will provide a service for those who do not have security on their phone as well as save them space by creating a single platform.

4. Product Overview

Product Perspective: The product will be accessible by any Android mobile device that meets our system requirements. The product must be installed on the user's mobile device. The product can also be used through a computer (must also have the product installed) for 2 way verification. Our product will not be completely independent or self contained, but the only limiting factor will be the user's device or computer.

Summary of Capabilities:

Customer Benefit	**Supporting Features**
A safe place to store all your passwords	-Auto-generated passwords -2 way verification
Encrypt all information on your phone	-Protected by Blowfish for its speed and overall effectiveness
Access from your computer	-2 way verification -Extra security. (Ex. User loses access to their phone) -Geolocation so user may locate their phone.

Assumptions and Dependencies:

1. User's devices meet the minimum requirements for our product.
2. The only language supported will be US English.
3. It is assumed the game will be run on Android 4.0.3 or higher. For PC users we are assuming it will be run on a Windows OS computer.

Cost and Pricing:

Our product will be free to download and use. However we will need to get a domain for our users to use when they are on a PC. If users enjoy our app and want to support us they may send us donations.

Licensing and Installation:

There will be no licensing requirements for V1.0 of our app except for a end-user license agreement. Which includes: limitation of liability of the software vendor, disclaimer of warranties, choice of law applicable to that contractual relationship, venue for possible disputes, and so on. Installation details will be included on the readme.

5. Product Features

System Features

1. Accept touch/mouse input
2. Keyboard input (Mobile and PC)
3. Exit App

Mobile App Features

1. Connect to account
2. Master Password will be safely stored using Bcrypt (salted and hashing)
3. 2 way verification using phone and PC
4. Geolocation
5. Dashboard
6. Auto-generate passwords which can be auto-generated periodically.
7. Encrypt all important information on the phone.
8. Option to turn on encryption/master key on mobile device

PC Platform Features

1. Creates an account/logs in = get user data
2. Send notification to install on mobile device
3. Option to track phone with geolocation
4. 2 way verification
5. Option to override master key on desktop
6. Option to uninstall app
7. Option to turn off GPS
8. Options to modify security measures

Menu Features(Mobile)

1. View Passwords
2. Auto-Generate Passwords
3. Encrypt Device

Menu Features(PC)

1. Create Account
2. Manage Account
    a. Change Password
    b. Send Notification to install on mobile device
    c. Uninstall App

    d. Modify other security measures
3. Manage Mobile Device
    a. Turn off GPS
    b. Geolocation
    c. Override Master Key
4. Logout

6. Constraints

Performance:

-Quick response time our product should run smoothly as long as the device fits the system requirements. This also applies to the PC version.

-Minimum actions the app should be simple to use it shouldn't be too complicated.

-Must be able to connect to WiFi to use the app.

Clearness:

-Ease of Use

-Clear and intuitive UI Design

Permissions:

-User must allow:

- Encrypting Mobile Device
- Geolocation
- Security measures that people allow. Each account will have different features allowed for more security. Therefore each phone will have a different level of security.

7. Quality Ranges

This mobile APP uses the most up to date API 26: Android 8.0 (O). We know not every customer will not meet certain standards depending on their phone, so the minimum API will be API 15: Android 4.0.3 (IceCreamSandwich). There will be no need to use fingerprint scan with phones that are not able to do it. Two way verification along with main computer verification are enough for them.In order to prevent passwords from being hacked, we are implementing features that makes it harder for hackers to get into your info like: Two way verification, encryption, fingerprint scanning, and main computer verification.

8. Precedence and Priority

1. Encryption
2. UI
3. Two way Verification
4. Fingerprint Scan
7. Cloud Capabilities
6. GPS location
7. Platform

9. Applicable Standards

Because we are an app that stores and changes your passwords, it is of utmost importance that we are able to protect our users data from individuals looking to steal it. In order to use our APP, a user must have an Android phone. To access our platform they can use any OS like Linux, Windows, or macOS. Certain features require certain hardware and software. New phones will be able to use fingerprint scan, while older phones cannot because of their hardware limitations.

10. Documentation Requirements

This section describes the documentation that will be worked on or developed over time to support the project we are building.

10.1 Release Notes (Patch Notes) - These notes will be included in a text file to keep new releases up to date. Each version of these notes will have new features that are added/ removed and explain what we have done to improve on the app.

10.2 Online Help - While our app will be mainly used on mobile devices, we will also have a platform where users can access additional features. One of these features will be the option of a online resource guide featuring commonly asked questions and information about our product.

10.3 Installation Guide - Download app and user will be able to access from platform on a PC as well.

11. Appendix 1 - Feature attributes

This is a basic overview of our most important features. While not all features will be listed here, we believe that these are our core features that are essential to the app performing how we want it to.

11.1 Status of Key Features

Proposed Features: 1. Geo-location Monitoring / Mapping
2. Auto- Generate Passwords
3. Phone Encryption/ More secure log-in
4. Emergency User / Safe user

Approved Features: All of the proposed features have been accepted by the engineering team, but are under consideration from Supervisor. They are waiting to approved and further worked on.

Incorporated Features: The incorporated features so far are file encryption and geo-location mapping to ensure that users and their information will be safe no matter what we decide to do

11.2 Benefits

Critical : Auto-Generated Passwords, Phone encryption

These features will be available to users at all times and prove to be the most helpful in keeping our users safe on the web and from potential thieves in real life. These features are sure to be our biggest selling point as we will be able to ensure users that their phone will be safe both online and in the real world.

Important: Emergency Mode/ Normal Mode

This feature is key to keeping user's phones safe in case it gets stolen. It will let users lock their phone from a PC by logging on to our platform while also getting GPS location if available.

Useful: GPS Mapping

This feature is useful because it will allow other users that the primary user sets access to the GPS location of the primary user. This will keep the User safe and also prove helpful in case the user needs to access the exact location of their phone in case it gets stolen or lost.

11.3 Effort

Auto - Generate Passwords / Phone Encryption/ Safety

These features will take up a big chunk of time both in coding and research. When dealing with safety online, it is imperative to make sure that user's information will never be in peril because of a weak password or bad encryption. Therefore, a lot of research will go into algorithms and safe encryption methods so users will always be safe, making this step very time consuming but essential to the success of our project.

The Emergency Mode aspect of our project will also take a considerable amount of time since we have to build the platform that the users will use to lock their phone and access other features. We will also have to figure out how to communicate in between our platform and app in an efficient and quick manner.

GPS services will most likely take less time to code and research as there are many resources online we could use to accelerate our progress in this feature. However, GPS services will have to incorporated into some other parts of the project so that time might be factored into those project timelines.

11.4 Risk

The biggest risk this project faces is running out of time. This project requires a lot of research and coding to come out in a presentable way. Extensive research and coding will have to done and the project still might not completely done.

Another risk that the project faces is that it will be working with the data of others since a big chunk of the project requires users to input their personal data and entrusting it to us to keep it safe. We have to accept the risk that if our product is not good, we will be putting the information of others at risk.

11.5 Stability

While some base features have been laid out, we estimate that one might have to be cut out because of the short period of time we have to do the project. It is possible that the project gets done completely, but some features might require more time or might not work completely and will have to be released in a beta version of the final project.

11.6 Target Release

Our Target release for the final app is roughly a year from now (9/22/2017). While our final product should be ready by that time, features will roll out at a quicker pace and be implemented into the project as they are complete. Implementing features will be done in the second phase somewhere at the start of next year and will continue until the end of the 2018 Spring Semester.

Note: Incorporated features should include all of the base features waiting to be approved by the advisor. Once approved, vision document will be revised accordingly.

11.7 Assignments

These features are too big to tackle as a single programmer and therefore assignments are not yet determined for each task. However, we plan to work on these tasks by committee while also working on assigned team roles in order to keep on track to release by the end of phase 2.

11.8 Reason

The Reason that we decided to incorporate these features are to make having a phone and using the internet more secure. We live in a day and age where theft of electronic devices and information online is incredibly common due to bad passwords or hardware that does not include theft protection. By using this app, the everyday person will gain access to both as they will be able to generate passwords for safety online as well as have a resource to use in case their phone gets stolen or lost. Therefore, the main reason for these features is to keep users information secure both digitally and physically.