Acceptance Test Plan

for

Smart Security

Version 2.0

Prepared By:

Tiffany Wong, Helen Hua, Josie Spencer, Aruna Srinivasiah, Connie Diu, Dericka Logan

Advisor:

Yuan An

Stakeholders:

Tiffany Wong, Helen Hua, Josie Spencer, Aruna Srinivasiah, Connie Diu, Dericka Logan

Table of Contents

1 Document History

Name	Date	Reason	Version
Tiffany Wong, Helen Hua, Josie Spencer, Aruna Srinivasiah, Connie Diu, Dericka Logan	February 26th, 2018	Initial draft	1.0
Tiffany Wong, Helen Hua, Josie Spencer, Aruna Srinivasiah, Connie Diu, Dericka Logan	April 4, 2018	Updated requirements number	2.0

2 Introduction

2.1 Purpose

Our team will be working on a senior design project that involves utilizing a smart home device (Google Home and/or Google Home Mini) and turning it into a cheap, multifunctional, and transportable security alarm system. The target demographic would be college students or recent graduates who do not have a lot of disposable income and are renting an apartment. Combining a smart home device with a smartphone will allow users to monitor their home wherever they are.

2.2 Definitions

Alarm - the mode of the system during which the user is alerted to unauthorized entrants.

Authorized - an authorized entrant can disarm the alarm for a certain amount of time.

Entrant - a person who enters the home. An entrant may be authorized or unauthorized. The user is a permanently authorized entrant.

Home - the Google Home or Google Home Mini device incorporated in the system.

Residence - the apartment or other living space that the user is protecting using the system.

Unauthorized - an unauthorized entrant will cause the alarm to sound.

User - the primary owner of the device.

3 Test Approach and Constraints

3.1 Test Objectives

The following test cases ensure that the Smart Security system fulfills the requirements put forth in the Software Requirements Specification. The Smart Security System will be considered ready for deployment if it passes all of the tests included in this Acceptance Test Plan.

3.2 Test Structures

The tests in this document are based on the requirements from the SRS. Each test case description includes an identifying number, a name, a description of the functionality being tested, and references to the related specifications in the SRS. The test cases also include preconditions, actions, and postconditions that describe the beginning state of the system at the start of the test, the steps to be taken, and the expected end state, respectively.

3.3 Test Constraints

This test plan only tests the functionality described in the SRS, and test only the top-level behavior expected from the system, as opposed to implementation or specific design.

4 Test Assumptions and Exclusions

This section provides in greater detail the functions and features of Smart Security. It covers those features and functions that are not talked about in the Acceptance Test Plan process.

4.1 Test Assumptions

The test cases in the Acceptance Test Plan are written under the assumption that the related issues are addressed by unit tests, integration test, and system tests for Smart Security.

The Acceptance Test Plan covers:

- Functional requirements listed in the Software Requirements Specification
- Usability of the system
- Consistency of user-related system documentation

4.2 Test Exclusions

The following areas will not be covered by the Acceptance Test Plan

The Acceptance Test Plan does not cover:

- Non-functional requirements listed in the Software Requirements Specification
- Requirements and functionality that is beyond the scope described in the Software Requirements Specification

5 Entry and Exit Criteria

The following list of criteria should be satisfied in order for the testing to be completed.

5.1 Entry Criteria

The following preconditions must be met for the acceptance testing to begin:

- Requirements are well defined
- Testable code is available
- Test cases are developed
- Test environment has been set-up

5.2 Exit Criteria

The following postconditions must be met for the acceptance testing to end:

- All Priority 1 requirements were tested and resulted in a success
- All Priority 1 requirement defects were identified and fixed
- Retesting and closing all Priority 1 requirement defects

6 Testing Participants

This section will describe the roles and responsibilities of all individuals in the Acceptance Test Plan. Also, the procedure for reporting test results and any subsequent issues.

6.1 Roles and Responsibilities

For the testing of the Smart Security project, we have divided the tasks and responsibilities to the different members for the rest of the terms. We have divided up the tasks and responsibilities as followed:

- Web Application: Tiffany
- Google Home: Connie, Dericka, and Josie
- Database: Helen
- Documentation: Aruna

6.2 Training Requirements

All parties involved in the testing should have a great understanding of Smart Security.

6.3 Problem Reporting

Any problems or issues found by any testers should be reported and documented by the documentation person. All problems should be reported and reviewed during the post testing meeting.

6.4 Progress Reporting

The Acceptance Test Plan Report should be completed and compiled by the documentation person once all testing have been completed.

7 Test Cases

7.1 Introduction

The test cases in this section test that the Smart Security system fulfills all the functionality described in the Software Requirement Specification (SRS). Each test case includes the following fields:

- ID - An identification code for the test case
- Name - A descriptive name for the test
- Requirement(s) - The requirement number(s) from the SRS for the requirements tested by the test
- Description - A brief overview of the test purpose
- Precondition(s) - The expected state of the software before the test is attempted
- Action(s) - The step(s) to be taken by the tester
- Postcondition(s) - The expected state of the software after the test has been completed

7.2 Test Cases

7.2.1 Login to Existing Account

ID	T7.2.1.1
Name	Login to existing account
Requirement(s)	R4.2.1
Description	The user opens the Smart Security web application and login to an existing account using Google Authentication API
Precondition(s)	● The user has a Google account
Action(s)	1. The user opens a web browser and navigates to the Smart Security web application 2. The user clicks on the “Sign in with Google” button on the upper right corner 3. The user selects their Google account to use as their login information
Postcondition(s)	● The user is directed to the alarms page

7.2.2 Arm Alarm

ID	T7.2.2.1
Name	Arming alarm
Requirement(s)	R4.2.3
Description	The user arms the alarm through Google Home
Precondition(s)	● Google Home is linked to user's Google account ● Application is on the Google Home ● Google Home is on
Action(s)	1. User says "set alarm [passcode]" to Google Home
Postcondition(s)	● The Google Home alarm is armed (activated) ● Passcode is recorded on database

7.2.3 Disarm Alarm

ID	T7.2.3.1
Name	Disarming alarm
Requirement(s)	R4.2.4
Description	The user disarms the alarm through Google Home
Precondition(s)	● Google Home is linked to user's Google account ● Application is on the Google Home ● Google Home is on ● Google Home is armed
Action(s)	1. User says "Disarm alarm [passcode]" to Google Home
Postcondition(s)	● The Google Home is disarmed (deactivated) ● Correct passcode was used

7.2.4 Trip Alarm

ID	T7.2.4.1
Name	Tripped Alarms
Requirement(s)	R4.2.5
Description	Alarm shall be tripped when Google Home picks up invasive sounds
Precondition(s)	● Alarm is armed
Action(s)	1. Text message shall ask user to approve or deny entrance 2. User sends approve 3. Alarm shall disarm
Postcondition(s)	● Alarm shall immediately play a loud alarm sound for a minute ● Text message shall ask user to approve or deny entrance

7.2.5 Notify User

ID	T7.2.5.1
Name	Notify user
Requirement(s)	R4.2.5.2, R4.2.7
Description	User will be notified when alarm is tripped by an approved user
Precondition(s)	● Alarm is tripped ● Text message is sent to user
Action(s)	1. User replies to text message with APPROVED
Postcondition(s)	● Alarm is disarmed ● Information of tripped alarm is added to Alarms list

ID	T7.2.5.2
Name	Notify user
Requirement(s)	R4.2.5.2, R4.2.7
Description	User will be notified when alarm is tripped by an unapproved user

Precondition(s)	● Alarm is tripped ● Text message is sent to user
Action(s)	1. User replies to text message with DENY
Postcondition(s)	● Alarm plays an obnoxious sound for one minute ● Information of tripped alarm is added to Alarms list ● Alarm is still armed

7.2.6 Sound Alarm

ID	T7.2.6.1
Name	Sound alarm
Requirement(s)	R4.2.5.2.1.2.1
Description	Alarm will play an invasion sound when tripped
Precondition(s)	● Alarm is tripped ● Text message is sent to user ● User denied entrant
Action(s)	1. The Google Home play an obnoxious sound for one minute
Postcondition(s)	● After one minute, the sound is stopped ● Alarm is still armed

7.2.7 View Alarm Log

ID	T7.2.7.1
Name	Viewing alarm log
Requirement(s)	R4.2.7
Description	The user views alarm log
Precondition(s)	● The user is logged into Smart Security
Action(s)	1. The user login to Smart Security
Postcondition(s)	● The Alarms page appears on the screen ● The page shows the list of alarms

ID	T7.2.7.2
Name	Viewing alarm log
Requirement(s)	R4.2.7
Description	The user views alarm log from another page on Smart Security
Precondition(s)	● The user is logged into Smart Security ● The user is on another page on Smart Security
Action(s)	1. The user clicks on the Alarms button on the upper right corner
Postcondition(s)	● The Alarms page appears on the screen ● The page shows the list of alarms

7.2.8 Add Entrant

ID	T7.2.8.1
Name	Add Entrants
Requirement(s)	R4.2.6.1
Description	User can add authorized entrant(s) who shouldn't trip the alarm when the alarm is set
Precondition(s)	● The user is logged into Smart Security
Action(s)	1. The user clicks on the Entrants button on the upper right corner 2. The user clicks on the Add button on the Approved Entrants page 3. The user enters the name, email address, and phone number for the entrant being added 4. The user clicks on the Add New Entrant button
Postcondition(s)	● User is directed to the Approved Entrants page ● User can see the name of the entrant that was just added ● Entrant's information is recorded on database

7.2.9 Delete Entrant

ID	T7.2.9.1
Name	Delete Entrants
Requirement(s)	R4.2.6.2
Description	User can add delete authorized entrant(s)
Precondition(s)	● The user is logged into Smart Security ● The user is on the Approved Entrants page
Action(s)	1. The user click on the Delete button next to the entrant name
Postcondition(s)	● User cannot see the name of the entrant that was just deleted ● Deleted entrant's information is removed from database

8 Traceability Matrix

Requirement	Description	Test Cases
R4.2.1	Logging into Smart Security	T7.2.1.1
R4.2.2	Creating Arm/Disarm Alarm Code	T7.2.2.1, T7.2.3.1
R4.2.3	User Arming Alarm	T7.2.2.1
R4.2.4	User Disarming Alarm	T7.2.3.1
R4.2.5	Tripped Alarms	T7.2.4.1, T7.2.6.1
R4.2.6.1	Creating Entrants List	T7.2.8.1, T7.2.9.1
R4.2.6.2	Deleting Entrants	T7.2.9.1
R4.2.7	Report of Tripped Alarms	T7.2.7.1