Software Testing Specification Plan

for

IoT Sensor Blinding

Version 1.0 not approved yet

Prepared by Jeremy Gluck, Todd St. Onge, Xuchao 'Steven' Jiang, Cole Clements, and Alex Winstead

September 2019

Project Name: IoT Sensor Blinding

Software Quality Assurance Plan

Version: (n)	**Date: (mm/dd/yyyy)**
Version (1.0)	9/30/19

Document History and Distribution

1. Revision History

Revision # () if not approved	**Revision Date**	**Description of Change**	**Author**
(0)	9/28/19	Created	Team #1

2. Distribution

Recipient Name	**Recipient Organization**	**Distribution Method**
Dr. Chan	Sr. Design	email

TABLE OF CONTENTS

1. INTRODUCTION

(NOTE 1: THE SOFTWARE TEST PLAN GUIDELINES WERE DERIVED AND DEVELOPED FROM IEEE STANDARD FOR SOFTWARE TEST DOCUMENTATION (829-1998)).

The project entails acquiring labeled frames of network traffic from Internet of Things devices for building models to classify IoT device network traffic for the purpose of penetration testing the devices. The team members will collect the machine learning data in a controlled lab environment until October 28th. Between October 28th and November 25th the team will label unlabeled data as well as extract features from the data for potential models. Between November 25th and February 3rd the team will explore different models of the data in order to maximize accuracy and generality. Between the date of March 2nd and April 6th the team will attempt to utilize the models to affect the devices. After April 6th the team will begin work on a research paper for publishing results. In order to build the knowledge base for the model team members will use software and hardware to sniff network frames from active devices, eventually to label them with the corresponding device name as well as the content of the communication. For the purpose of showcasing the project a device titled the "Raspberry Jam" will be developed with our models loaded onto it.

1.1 Objectives

The team will generate data in order to build a model of IoT device networks frames. The accuracy of this model will be tested and it will be the team's goal to maximize this accuracy. A research paper will be written detailing results and a small computer will be prepared to showcase the model working in a real world environment. Due to the number of devices and communications to be tested team members will need to be in the lab multiple times per week to collect data/ label data/ research models/test model accuracy.

1.2 Testing Strategy

Multiple model types will be researched and implemented and then their accuracy in classifying novel network traffic will be tested. A classification model works in the following fashion: given a set of input classes , a set of labeled data (data of the type of the input, paired with the correct label for that point), and an input, the model outputs a prediction for the class of the input. The model can be either right or wrong. Given a set of test data, we define the model's accuracy as the ratio of its correct predictions to its

incorrect predictions. Models will be researched in order to maximize accuracy (avoiding overfitting). The generality of the model is the ability for it to retain its accuracy in novel (possibly noisy) environments; the team will attempt to construct the most general model that still functions accurately.

1.3 Scope

The following IoT devices will be used to generate data and model:

Amazon - All-New Echo Dot Kids Edition Smart Speaker with Alexa - Rainbow
Amazon - Echo Dot (3rd Gen) - Smart Speaker with Alexa - Charcoal
Amazon - Echo Show 5 Smart Display with Alexa - Charcoal
Arlo - Pro 2-Camera Indoor/Outdoor Wireless 720p Security Camera System - White
August - Smart Lock Pro + Connect - Dark gray
Blink - Wireless Home Security System - White
Geeni - Indoor Wi-Fi Wireless Network Surveillance Cameras (2-Pack) - Black
Geeni - Pan and Tilt Indoor Wi-Fi Wireless Network Surveillance Camera - White
Geeni - Smart Wi-Fi Video Doorbell - Wired - Black
Google - Home Mini - Smart Speaker with Google Assistant - Charcoal
Google - Nest Cam IQ Indoor Full HD Wi-Fi Home Security Camera - White
Google - Nest Hello Smart Wi-Fi Video Doorbell
Google - Nest Secure Alarm System - White
Kwikset - SmartCode Z-Wave Deadbolt Lock - Polished Brass
Night Owl - Smart Wi-Fi Video Doorbell - Wired - Black
Philips - Hue Color 3pk Starter Kit with Lightswitch - Multicolor
Philips - Hue Play White & Color Ambiance Smart LED Bar Light (2-Pack) - Multicolor
Ring - Alarm Motion Detector - White
Ring - Alarm Starter Home Security Kit - White
Ring - Motion Sensor - White
Ring - Spotlight Indoor/Outdoor 1080p Wi-Fi Wireless Security Camera - Black
Ring - Video Doorbell Pro and Chime Pro Bundle - Satin Nickel
Ring - Wi-Fi Smart Video Doorbell - Multi
Samsung - Button - White

Samsung - Motion Sensor - White
Samsung - Multipurpose Sensor - White
Samsung - SmartThings Arrival Sensor - White
Samsung - SmartThings Hub - White
Samsung - SmartThings Indoor 1080p Wi-Fi Wireless Security Camera - White
Samsung - SmartThings Item Tracker - White
Samsung - SmartThings Smart Outlet - White
Samsung - SmartThings White A19 Smart LED Bulb - White
Samsung - Water Leak Sensor
Schlage - Encode Wi-Fi Touch Screen Deadbolt - Matte Black
SimpliSafe - Entry Sensor - White
SimpliSafe - Glassbreak Sensor - White
SimpliSafe - Motion Sensor - White
SimpliSafe - Pro Smart Wi-Fi Video Doorbell - Wired - White
SimpliSafe - Smart Lock Black + Black PIN Pad - Black/Black
SimpliSafe - Wireless Home Security System - Black
Swann - Indoor/Outdoor 1080p Wi-Fi Wireless Security Camera - White
TP-Link - Kasa Spot Indoor 1080p Wi-Fi Wireless Security Camera - Black/White
Yale - Assure Lock Touch Screen Smart Lock - Satin Nickel
Yale - T1L Z-Wave Touchscreen Deadbolt Replacement Smart Lock - Nickel

1.4 Reference Material

1) https://github.com/FloridaTech-IOT-Security-SProject-19-20/Project-Plan?organization=FloridaTech-IOT-Security-SProject-19-20&organization=FloridaTech-IOT-Security-SProject-19-20

2) https://enck.org/pubs/oconnor-wisec19b.pdf

   T. Oconnor, W. Enck, and B. Reaves, “Blinded and confused,” *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks - WiSec 19*, May 2019.

3) https://dl.acm.org/citation.cfm?id=3323409

T. Oconnor, R. Mohamed, M. Miettinen, W. Enck, B. Reaves, and A.-R. Sadeghi, "HomeSnitch," *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks - WiSec 19*, May 2019.

1.5 Definitions and Acronyms

(Specify definitions of all terms and agency acronyms required to properly interpret the Software Test Plan. Reference may be made to the Glossary of Terms on the IRMC web page.)

Acronym/Definition	**Meaning**
IEEE	Institute of Electrical and Electronics Engineers
RF	Radio Frequency
WiFi, Wi-Fi	Wireless Fidelity
IoT	Internet of Things

2. FEATURES TO BE TESTED

(Note: features and numbers referenced are from Design Document and are numbered accordingly.)

- 4.1 Detect WiFi packets
- 4.2 Parse WiFi packets
- 4.4.0 Test Model created in 4.3
- 4.5 Blind WiFi packets
- 4.6 Send WiFi packets

3. FEATURES NOT TO BE TESTED

(Note: features referenced are from Design Document and are numbered accordingly.)

- 3.3 Use Data to Train Model
    - Because this is just the training of the model testing will not be necessary.

4. APPROACH

The Below Testing procedures will be used with the designated features to ensure said features meet the PASS/FAIL Criteria.

4.1 Component Testing

Each feature being tested will be treated as a unit and will go through and comply with basic unit testing procedures.

4.2 Integration Testing

Features 4.1 Detect WiFi packets, 4.5 Blind WiFi packets, 4.6 Send WiFi packets, will all be tested using the supported hardware mentioned in the design document to test verification and validation.

4.8 Performance Testing

Feature 4.4.0 Test Model created in 4.3 will need to undergo performance testing to identify with an eighty percent accuracy the type of packet being transferred.

4.10 Acceptance Testing

Acceptance testing will be done on the product as a whole by Dr.O'Connor, he will decide the pass fail criteria.

5. PASS / FAIL CRITERIA

Tests that have Passed will have achieved the desired goal as stated by the tester in accordance with the test document and will be able to show documented proof of completion and success. If no Criteria are stated the tester will create criteria to be approved by the team. FAIL Criteria is the inability for the program to complete the PASS criteria.

6. TESTING PROCESS

(Identify the methods and criteria used in performing test activities. Define the specific methods and procedures for each type of test. Define the detailed criteria for evaluating test results.)

6.1 Test Deliverables

All Tests will come with a list of inputs and actual outputs along with a date and a signature by the tester. In the case of performance testing any requested data that was printed into a log or other output should be included. Finally a PASS/FAIL result should be written down. This should include a reason the tester made this decision.

6.2 Testing Tasks

6.2.1 Testing form shall look like:

Tester:
Date:
Tests run:
Type:
Input:
Output:
Result: Pass/Fail
Reason:
Tester Signature:

6.2.2
Testing on each component

	Component Testing	Integration Testing	Performance Testing	Acceptance Testing
4.1 Detect Wifi Packets	YES	YES	NO	NO
4.2 Parse Wifi Packets	YES	NO	NO	NO
4.3 Use Data to Train Model	YES	NO	YES	NO
4.4 Input Data into Model to decipher packet type	YES	NO	YES	NO
4.5 Blind Wifi Packets	YES	YES	NO	NO
4.6 Send Wifi Packets	YES	YES	NO	NO
Project as a whole	NO	NO	NO	YES

6.3 Responsibilities

Member	Main Role/Task
Jeremy Gluck	Data Science (Machine Learning)
Alex Winstead	Data Science (Machine Learning), Scrum-Master
Cole Clements	Testing
Steven Jiang	Testing, Firmware-Software Specialist
Todd St. Onge	Firmware/Hardware Specialist

6.4 Resources

6.4.1 Responsibilities

Testers will be responsible for all tests they begin unless otherwise stated. Testers are individuals assigned to Testing in section 7.3 Responsibilities.

6.4.2 Tools

Tools and software used in the lab environment will be the tools used for fulfilling the required tests A detailed list can be found in 7 Environmental requirements which defines the lab setting.

6.5 Schedule table will be updated after values added in sheets

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	
8:00 AM								Jeremy Gluck
9:00 AM					Alex Winstead			Xuchao Jiang
10:00 AM	Xuchao Jiang		Xuchao Jiang					Alex Winstead
11:00 AM		Alex Winstead		Alex Winstead				Todd St. Onge
12:00 PM	Alex Winstead		Alex Winstead					Cole Clements
1:00 PM					Jeremy Gluck, Xuchao Jiang			
2:00 PM		Todd St.		Todd St.	Alex			

		Onge		Onge	Winstead, Xuchao Jiang			
3:00 PM	Jeremy Gluck, Todd St. Onge		Jeremy Gluck, Todd St. Onge					
4:00 PM		Alex Winstead Cole Clements		Alex Winstead Cole Clements				
5:00 PM					Alex Winstead Cole Clements			
6:00 PM								
7:00 PM								
8:00 PM								
9:00 PM								
10:00 PM								
11:00 PM								
12:00 AM								

7. ENVIRONMENTAL REQUIREMENTS

7.1 Hardware

- Raspberry Pi 4
- Various IoT Devices running Z-Wave, Zigbee, and IEEE 802.11 Protocols
- Wifi Pineapple
- Wireless Access Point Device
- RF Hacking Field Kit
- Bus Pirate
- Oscilloscope
- Z-Wave usb stick

7.2 Software

- Aircrack-ng
- Wireshark
- OpenSSH
- Curl

7.3 Publications

- Blinded and Confused: Uncovering Systemic Flaws in Device Telemetry for Smart-Home Internet of Things
- Homesnitch: Behavior Transparency and Control for Smart Home IoT Devices

7.4 Risks and Assumptions

Major Risks to testing.

7.4.1

Risk: Our Lab is not set up in time.
Solution: Set up a lab at a team member's house.

7.4.2

Risk: Equipment is not delivered on time
Solution: Wait until the equipment delivers.

8. CHANGE MANAGEMENT PROCEDURES

8.1 Changes to the test plan can be made by a majority vote of the team members only.

9. PLAN APPROVALS

9.1 This plan is approved by the entire team upon creation.

9.2 Approvals for change

Effective Date	**Change Made**	**Team Vote (for/against)**	**Sponsor Signature**