SET YOUR TITLE USING \title

I. Methodology

1.1 Problem/Objective

This research aims to demonstrate how data leakage in smart home environments enable an eavesdropper to classify internet of things (IoT) devices, track user's movements, map networks, and identify events within the smart home. It also seeks to show how a smart home user can defend against these attacks. These goals are enabled through the implementation of the Classification, Identification, and Tracking of IoT (CITIoT) and Mitigation of IoT Leakage (MIoTL) tools respectively. The experiment presented in this section functions as an evaluation of these tools in a realistic smart home environment, testing how accurately the CITIoT tool operates against the Smart Home Automation Architecture (SHAA) and how well MIoTL mitigates these attacks. Specifically, the experimentation attempts to accomplish four objectives:

1. Determine the ability of an observer to accurately classify smart home devices.*
2. Examine with what success rate events can be identified.*
3. Measure the capability to track when users are in the smart home.*
4. Evaluate processing time and storage requirements.

* Objective is fulfilled in two states: when the MIoTL tool is activated and when it is not.

The evaluation results will provide consumers with an understanding of data leakage in smart home environments and a method to defend against these vulnerabilities.

1.2 System Under Test

Figure 1 displays the System Under Test (SUT) and Component Under Test (CUT) diagram. Section 1.7.3 describes the experiment treatments which include a user performing actions from a script to interact with the smart home environment and the operation of the MIoTL tool. Section 1.6 discusses the constant factors that do not change throughout the experiment such as computing parameters and the number of devices. The actual Wi-Fi and Bluetooth Low Energy (BLE) traffic collected by the CITIoT tool is considered uncontrolled and is examined in Section 1.5. The components tested include the preprocessor, Media Access Control (MAC) tracker, classifier, and network mapper. Response variables, or metrics, described in Section 1.3, consist of classified devices, identified events, user tracking, processing time, and storage requirements.

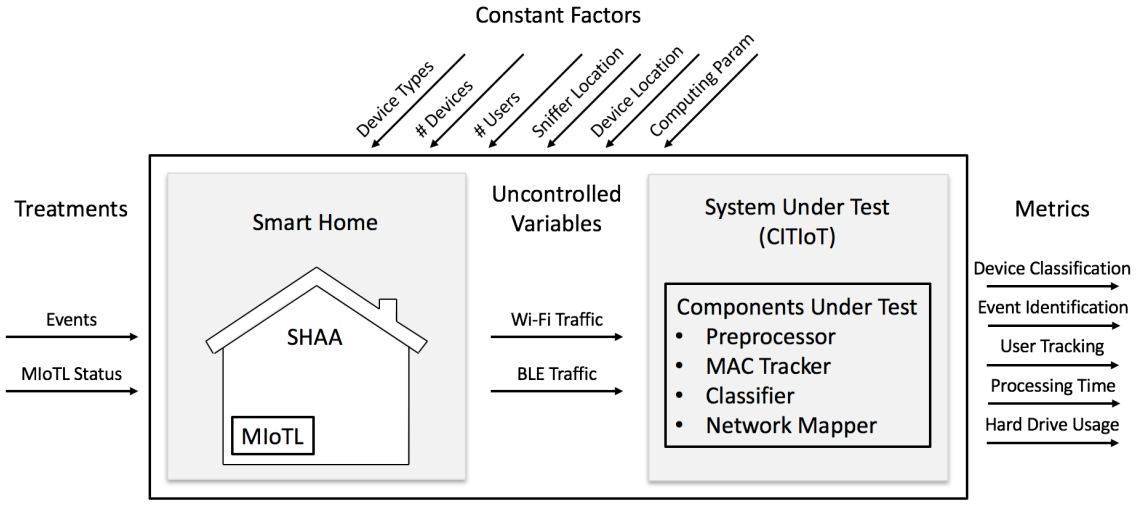

Figure 1. System Under Test (SUT) and Component Under Test (CUT) diagram

1.2.1 Assumptions.

The following assumptions are made when designing and executing experiments for the CITIoT tool:

1. The actions performed within SHAA are representative of a real smart home environment.

2. The eavesdropper has already accomplished reconnaissance and scanning and has the required parameters to run the CITIoT tool.

3. During experimentation, the CITIoT tool is positioned within SHAA, whereas in real-world operation it would be outside of the smart home. It is assumed that a directional antenna aimed at the smart home would have similar results to an omnidirectional antenna within the smart home. This assumption is substantiated through Rose, et al.'s work cracking a gun safe from a quarter mile away [2].

4. The degree of precision for an identified event is one minute. This level of precision provides enough accuracy for the problem presented in this thesis and allows for signal propagation and sniffer delays to be ignored.

1.3 Response Variables

The objectives of this experiment influence the response variables used in measuring the performance of the CITIoT tool. While not directly measured, the performance of MIoTL is quantified via the observed decrease in the CITIoT tool's operation when the mitigation tool is operating. Therefore, response variables (or performance metric) tied to the four objectives help consider the overall performance of the CITIoT tool in either state:

- **Objective 1:** Determine the ability of an observer to accurately classify smart home devices.

  Device Classification Success Rate (DCSR): Since the number of devices within SHAA is controlled, and the CITIoT tool attempts to classify

each device, the DCSR response variable can measure the tool's ability to accurately classify devices. The DCSR metric can be expressed by the simple ratio measurement

$$DCSR = \frac{DC}{TD} \tag{1}$$

where DC represents the number of successfully classified devices and TD represents the total number of devices within SHAA.

- **Objective 2:** Examine with what success rate events can be identified.

  Event Identification Success Rate (EISR): The EISR response variable measures the tool's ability to accurately identify events. An event is considered successfully identified if the time and device of the event recognized by the CITIoT tool matches an event in the log. The degree of precision for an identified event is one minute. The EISR metric can be expressed by the simple ratio measurement

$$EISR = \frac{TP}{TE} \tag{2}$$

where TP represents the number of true positives, or successfully identified events, and TE represents the total number of events per test trial.

  Event Identification False Positives (EIFP): The EIFP response variable measures the rate at which the CITIoT tool falsely identifies events that did not actually occur. The EIFP metric can be expressed by the simple ratio measurement

$$EIFP = \frac{FP}{EI} \tag{3}$$

where FP represents the number of false positives, or identified events that did not occur, and EI represents the total number of events identified by the CITIoT tool.

Event Identification False Negatives (EIFN): The EIFN response variable measures the rate at which the CITIoT tool fails to identify events that did actually occur. The EIFN metric can be expressed by the simple ratio measurement

$$EIFN = \frac{FN}{TE} \tag{4}$$

where FN represents the total number of false negatives, or events the tool failed to identify, and TE represents the total number events per test trial. The EIFN metric can be simplified to

$$EIFN = 1 - EISR \tag{5}$$

- **Objective 3:** Measure the capability to track when users are in the smart home.

  User Location Success Rate (ULSR): The ULSR response variable measures the rate at which a user's location is accurately identified as home or away via Wi-Fi devices. The ULSR metric can be expressed by the simple ratio measurement

$$ULSR = \frac{ST}{TT} \tag{6}$$

  where ST represents the total time (minutes) which the location of the user is successfully tracked and TT is the total time (minutes) of the experiment.

- **Objective 4:** Evaluate processing time and storage requirements.

  Processing Time (PT): The PT metric is the average wall-clock processing time across all trials for each separate unit and the CITIoT tool as a whole. Each unit and experimental trial analyzes a different number of packets, therefore, the PT is normalized by taking the average PT of a single trial over

25,000 packets. Next, all of the trial's normalized PT values are averaged to provide the average tool and unit PT respectively. The average CITIoT tool PT metric can be expressed by the equation

$$CITIoTPT = \frac{\sum_{n=1}^{NumTrials} 25000 \times \frac{T_n}{TP_n}}{NumTrials} \tag{7}$$

where $NumTrials$ represents the number of trials, T_n is the total time of a given trial, and TP_n is the total number of packets in a given trial.

The timing of a given unit is calculated a little differently as multiple units run simultaneously with shared processing time. A unit's PT, then, only accounts for time used to assist in that unit's purpose and not other units. For example, the preprocessor and MAC tracker both require the packet capture to be read into a list. Therefore, the time taken to parse the capture is accounted for in both unit's PT, but the time used to track MAC addresses is not added to the preprocessor's PT. Only two units operate at a time, so a unit's PT can be expressed by the equation

$$UnitPT = \frac{\sum_{n=1}^{NumTrials} 25000 \times \frac{T_n - T_b}{TP_n}}{NumTrials} \tag{8}$$

where T_b represents the total processing time exclusive to the other unit's operation.

Hard Drive Usage (HDU): The HDU metric is the amount of hard drive space used by all components of the CITIoT tool after operation.

Table 1 defines each performance metric's units of measurement, accepted range value, and expected range value. Objectives one through three and corresponding response variables are also observed while the MIoTL tool is operating.

Table 1. Performance Metrics

Metric	Units	Accepted Range	Expected Value
DCSR (Device Classification Success Rate)	%	0 to 100	$> 75\%$
EISR (Event Identification Success Rate)	%	0 to 100	$> 75\%$
EIFP (Event Identification False Positives)	%	0 to 100	$> 75\%$
EIFN (Event Identification False Negatives)	%	0 to 100	$> 75\%$
ULSR (User Location Success Rate)	%	0 to 100	$> 75\%$
CT (Completion Time)	minutes	0 to ∞	< 120 minutes
HDU (Hard Drive Usage)	bytes	0 to ∞	< 20 GB

1.4 Control Variables

A primary goal of this experiment is to observe how the CITIoT tool operates in a realistic smart home environment. Using commercial off-the-shelf (COTS) components restricts the number of factors that can be altered during experimentation. Event type and timing are the primary factors, and are the main treatments in the experiment. A scripted number of events are performed in a random order and time interval throughout a trial. Additionally, the operating status of the MIoTL tool is used to evaluate the CITIoT tool's operation during mitigation.

1.5 Uncontrolled Variables

Another consequence of testing the CITIoT tool against a realistic smart home environment is the introduction of uncontrollable factors. The use of COTS components and an open environment introduces wireless noise and the occurrence of unscripted events. This is beneficial to the evaluation of the CITIoT tool as it is meant to operate among real-world interference.

1.6 Constant Factors

Throughout the course of experimentation, several factors will be held constant to limit the scope of the experiment:

- **Type of Devices:** The type of devices in the smart home does not change throughout the experiment.
- **Number of Devices:** The number of devices in the smart home does not change throughout the experiment.
- **Number of Users:** The number of smart home occupants does not change throughout the experiment.
- **Location of Sniffers:** The location of the sniffers relative to the smart home devices does not change throughout the experiment.
- **Location of Devices:** The location of the devices relative to the sniffers does not change throughout the experiment.
- **Computing Parameters:** The operating systems, resources (memory, CPU, and disk space), script languages, and hardware are held constant.

1.7 Experimental Design

The purpose of this experiment is to meet the four objectives listed above. The experiment scenario is defined by a user performing actions from a script to interact with the smart home environment. These events occur while the user is both in and away from the smart home environment. Data logging occurs to provide truth data used to evaluate the CITIoT tool's operation.

1.7.1 Smart Home Automation Architecture (SHAA).

Figure 2 depicts how the devices, CITIoT tool, and MIoTL tool are laid out within SHAA. To provide consistency between trials, all devices, excluding the iPhone, are not moved throughout experimentation. Proximity between the devices and CITIoT tool provides greater chances of packet capture for testing.

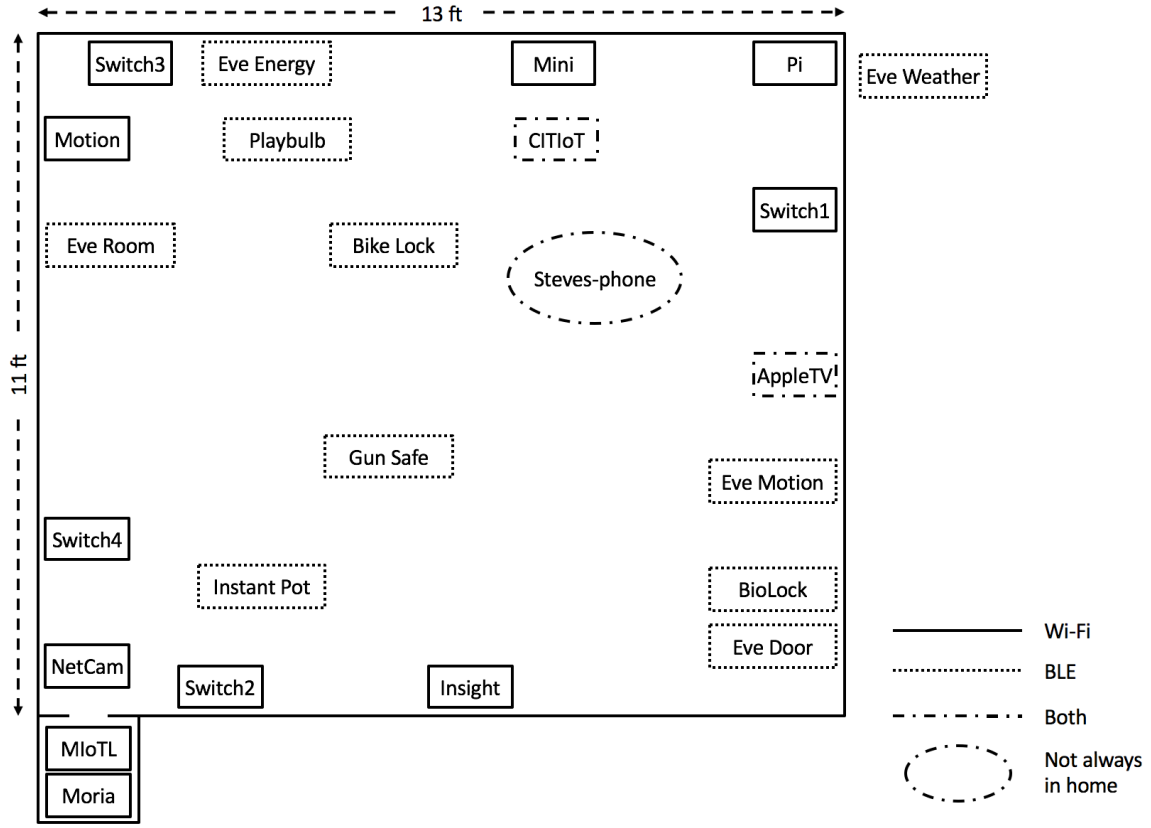

Figure 2. Approximate layout of devices within SHAA for experimentation (not to scale)

1.7.2 CITIoT.

Figure 2 shows where the CITIoT tool is placed within SHAA. Each sniffer operates in the 2.4 GHz band and must be horizontally isolated to avoid interference. The distance between antennae, d, to provide horizontal isolation can be expressed

by the equation

$$d \geq 2\frac{D^2}{\lambda} \tag{9}$$

where D is the length of the antenna in meters and λ is the wavelength of the device frequency band in Hz [1].

The Ubertooth One antennae are 3.5 inches long and operate with an average wavelength of 2441 MHz, while the Alfa Card antenna is 6.5 inches long and operates with an average wavelength of 2412 MHz. Plugging these values into the equation provides a separation value of about 5 inches for the Ubertooth One antennae and 17 inches for the Alfa Card antenna. Figure 3 shows how the individual sniffers are setup to avoid horizontal interference. The Ubertooth One sniffers are separated by 11 inches, while the Alfa Card is 20 to 23 inches from each of the Ubertooth One sniffers.

1.7.3 Treatments.

Table 2 lists the thirty-one events used during experimentation which occur randomly during trials. Events happen multiple times during a trial at random intervals. Each event allows the CITIoT tool to be evaluated against different devices and actions.

The events are administered with SHAA operating in two states: with and without the MIoTL tool activated. Table 3 describes how the treatments are administered among trials.

1.7.4 Logging.

A user log is used to record the time, device name, and action of each event carried out in SHAA during experimentation. Events recorded include turning on and off loggers, starting and stopping sniffers, arriving or leaving the smart home,

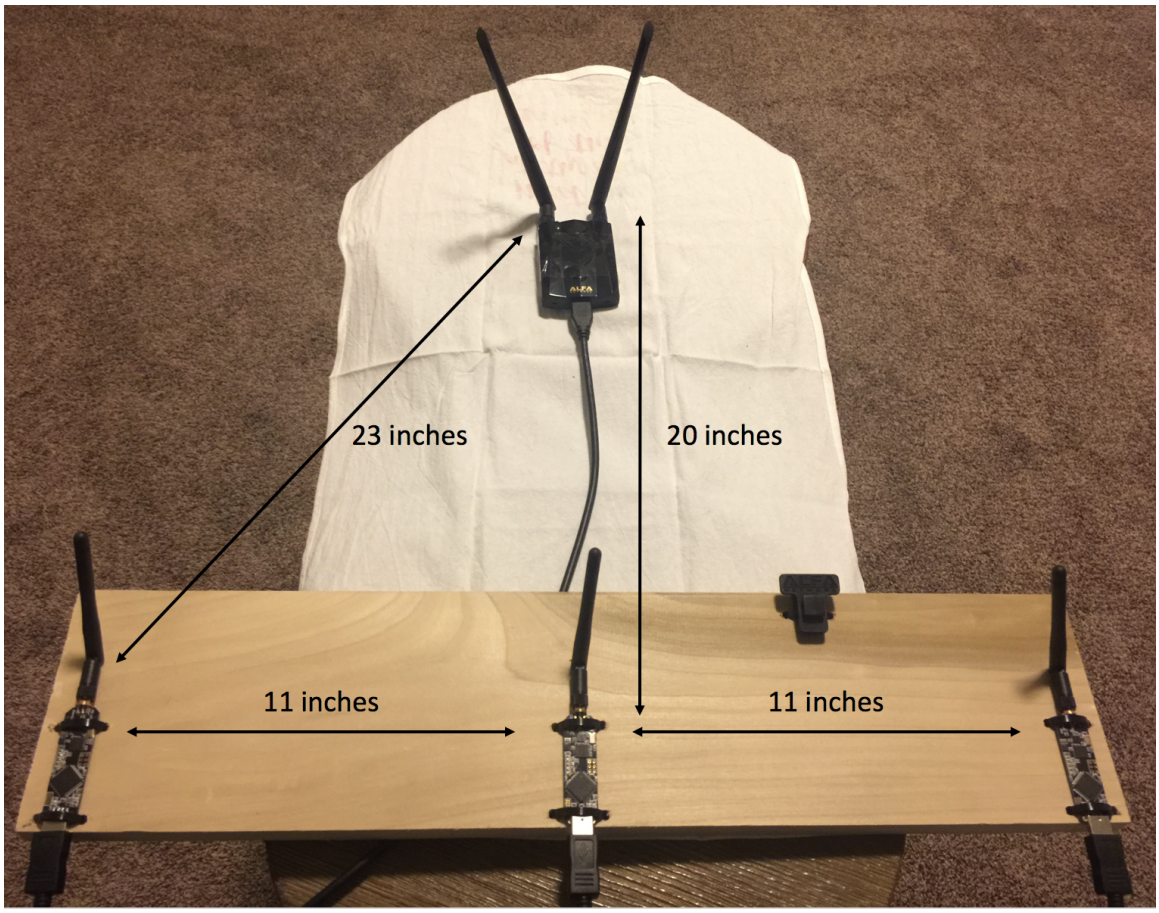

Figure 3. Layout of sniffer antennae for experimentation

computer errors, and activating devices. Additionally, the Raspberry Pi records each Wi-Fi event processed by the Homebridge server. These two logs are considered truth data and used to calculate the DCSR, EISR, EIFP, and EIFN response variables.

1.7.5 Testing Process.

Trials are carried out over six ten-hour days. The Homebridge logger and CITIoT sniffers are activated at the beginning of each trial. At least one minute is allowed before events occur to permit the logger and sniffers time to normalize. Then, each event from Table 2 is carried out in a random order in the morning and again in the evening. Also, devices are randomly activated throughout the day while the user is away. The time of each treatment is recorded in the user log. At the end of the day,

Table 2. Experiment Events

	Device Name	Action	Protocol
1	Bike Lock	Unlock	BLE
2	BioLock	Unlock	BLE
3	Instant Pot	Turn on	BLE
4	Instant Pot	Turn off	BLE
5	Gunsafe	Open	BLE
6	Gunsafe	Close	BLE
7	Eve Room	Get temperature in living room	BLE
8	Eve Weather	Get temperature on patio	BLE
9	Eve Door	Open	BLE
10	Eve Door	Close	BLE
11	Eve Energy	Turn on	BLE
12	Eve Energy	Turn off	BLE
13	Eve Motion	Activate motion sensor	BLE
14	Playbulb	Turn on	BLE
15	Playbulb	Turn off	BLE
16	Switch1	Turn on	Wi-Fi
17	Switch1	Turn off	Wi-Fi
18	Switch2	Turn on	Wi-Fi
19	Switch2	Turn off	Wi-Fi
20	Switch3	Turn on	Wi-Fi
21	Switch3	Turn off	Wi-Fi
22	Switch4	Turn on	Wi-Fi
23	Switch4	Turn off	Wi-Fi
24	Mini	Turn on	Wi-Fi
25	Mini	Turn off	Wi-Fi
26	Insight	Turn on	Wi-Fi
27	Insight	Turn off	Wi-Fi
28	NetCam	Activate motion	Wi-Fi
29	Motion	Activate motion sensor	Wi-Fi
30	Steves-phone	Leave house	Wi-Fi and BLE
31	Steves-phone	Arrive House	Wi-Fi and BLE

Table 3. Experiment Treatments

Trial #	Events Administered	MIoTL Status
1-5	1-31	Off
6	16-31	On

CITIoT sniffers and the Homebridge logger are deactivated and the processing unit of the CITIoT tool is started. When complete, the classifier, MAC tracker, and network mapper units are activated. Timing is built into the CITIoT tool using Python's time module for each unit to provide the wall-clock time for the response variable, PT. Results are stored for statistical analysis and evaluation.

The testing process is repeated during one trial with the MIoTL tool operating. As MIoTL only creates Wi-Fi traffic to impede with the CITIoT tool's operation, a subset of treatments only including Wi-Fi events are used. The MIoTL tool is activated at least five minutes prior to the Homebridge logger and the CITIoT Wi-Fi sniffer to allow for normalization. Wi-Fi devices are activate and the user log is maintained as in the first trials. At the end of the day, the CITIoT Wi-Fi sniffer, the Homebridge logger, and MIoTL are deactivated. The CITIoT tool operates similarly to previous trials after that.

1.8 Statistical Analysis

Data is collected through three main components: (i) results from the CITIoT tool, (ii) the logger on the Raspberry Pi recording events processed by the Homebridge server, and (iii) the user logs. This data is imported into the statistical analysis tool R, a GNU project language for statistical computing, and the CITIoT results are compared to the two truth data sources. The DCSR, EISR, ULSR, PT, and HDU data are tested for mean validity using a one-sample t-test, and computing the standard deviation, mean, and 95% confidence interval.

The comparison between the CITIoT tool's operation with and without the MIoTL tool running is accomplished using a paired t-test. If proven significant, the mean of the five trials without the MIoTL tool running is compared to the one trial with the tool operational.

1.9 Methodology Summary

This chapter describes the experimentation methodology used to measure the efficiency (PT and HDU) and accuracy (DCSR, EISR, and ULSR) of the CITIoT tool. The treatments allow for various devices and actions to determine the operational capabilities of the tool. The effectiveness of the MIoTL tool in mitigating some of the CITIoT tool's features is measured through the accuracy of the CITIoT tool while the MIoTL tool is operating.

Bibliography

1. Isolation between antennas of imt base stations in the land mobile service. Technical Report M.2244, International Telecommunication Union, 2011.

2. A. Rose and B. Ramsey. Picking bluetooth low energy locks from a quarter mile away. 2016. presented at DEF CON 24 *(media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/)*.