Research Proposal

Title: Black Box State Change Identification Through Side Channel Analysis

Author: Johnathan DiMatteo

Supervisor: Sebastian Fischmeister

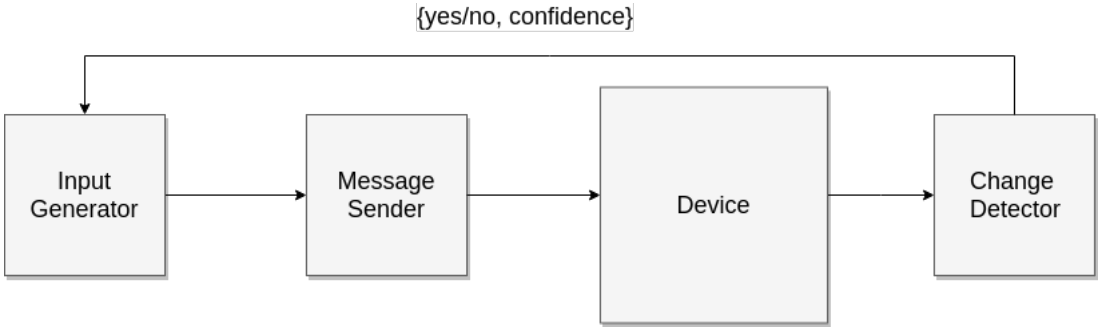
Motivation

The recent explosion of the Internet of Things (IoT) puts numerous embedded devices at the hands of governments, businesses, and consumers. Their low cost has caused manufacturers to produce and sell them without sufficient security or safety features. If action is not taken, vulnerabilities in IoT devices can lead to harm both economically and otherwise. To enforce security and safety in these devices, we will identify state transitions in order to reverse engineer the protocol specifications. This way anomalies can be identified and corrected to avoid security vulnerabilities. Traditional Hardware-in-Loop (HIL) testing methods involve significant intrusion to the system being observed. Our approach is to monitor the execution of the system to identify transitions without opening up the so called "black box", a technique known as *Side Channel Analysis*.

Problem Statement

1. **Change Detector**: Given a response from a black box system, determine if the state of the system has changed in order to learn the system's behaviour.
2. **Input Generator**: Given some inputs and knowledge of previous state changes, what should be the next query to the system?

System



Change Detector

The Change Detector determines if the device has changed behaviour based on the response from the system being observed. The response from the system is a time series signal. The steps of the Change Detector are:

1. Receive a response from the system.
2. Determine if the state has changed.
3. Return {yes or no, confidence }.

There are several ways to analyze time series signals:

1. Distance Based
2. Feature Based
3. Deep Learning

Distance Based: using a metric to determine the similarity between two or more signals. Common metrics include Euclidean distance and Dynamic Time Warping (DTW). Since our response may have slight differences in timing, DTW is the best choice.

Feature Based: using calculated features of the signal such as the mean, standard deviation, skewness, kurtosis, etc. These features are then fed into a machine learning algorithm to determine whether or not the signal has changed.

Deep Learning: the signals themselves are feed into multi-layered neural networks. Similar to feature based methods except that the features are determined by the algorithms themselves. A downside to this method is that significant data is needed for good performance.

Input Generator

What message should we send to the system in order to trigger a state change? The Input Generator should keep track of each message and the result from the Change Detector and use this information.

1. Receive answer from Change Detector.
2. Determine which message to query the system in order to try to change the state.

There are several possible methods to determine which message to send next:

1. Enumerate through all possibilities.
2. Active Learning, in particular, uncertainty sampling.
3. Genetic Algorithms to learn the best messages over time.

Additional Modules or Functionality

Protocol Specification: should be easy to switch from protocols.
Message Sender: also determined by protocol, the focus is on I2C for now.
Extract Protocol Method: given a list of messages that cause a state transition in the system, can a protocol be determined?