IoT Sensor Blinding

By: Alex Winstead (awinstead2015@my.fit.edu),
Xuchao (Steven) Jiang (xjiang2017@my.fit.edu),
Cole Clements (cclements2016@my.fit.edu),
Jeremy Gluck (jgluck2016@my.fit.edu),
Todd St. Onge (tstonge2016@my.fit.edu)

Progress Summary

Task	Completion %	To Do
Setup/Build IoT Lab	100%	Done
Collect Data	100%	Done
Parse Data	100%	All Parsers are built and implemented at scale.
Create Machine learning models	80%	RF Classifier model is working, while not perfect it demonstrates our data set as valuable to IOT researchers thus meeting the requirements of our stakeholder.

Milestone 6

Milestone 6

- Task 1: Finalize model and identifying lab devices
  - Perform any final tuning to the model.Wrap up data set.
- Task 2: finish documents required for class.
  - Ready materials.
- Task 3: Student Design Showcase
  - Prepare demo video, user manual, etc.

IoT Lab Manual

- Created document to outline lab procedures and objectives

- For handoff to other research projects

Data Collection

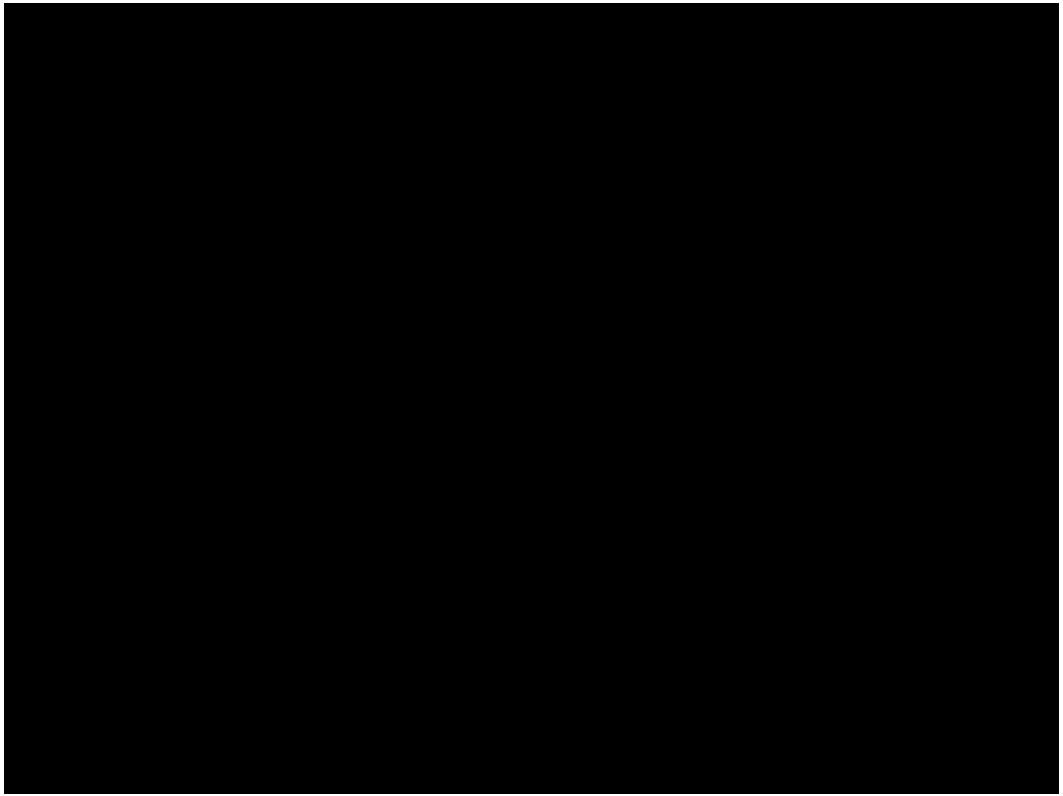
- Data collection is put to halt due to inconsistent data collected during remote access

- Data parsing code for door locks is refined and re-designed for future users

Machine Learning Model

- Server data proved to not provide meaningful insight, data will be kept in the set incase it has worth for other users and endeavors.
- Have 100% accuracy for action classifier
- Locking vs unlocking classifier is still not 100%.
- Data sets have been cleaned and packaged so that they can be presented to anyone whom would like to use them for ML.

Demo Video



Showcase Preparation

NORTHROP GRUMMAN
ENGINEERING & SCIENCE
STUDENT DESIGN SHOWCASE
FLORIDA TECH

IOT Sensor Blinding: A ML Approach to Network Traffic Classification

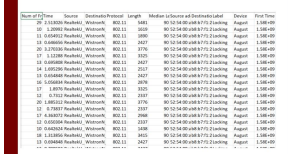
By: Jeremy Gluck, Todd St. Onge, Xuchao 'Steven' Jiang, Alex Winstead, Matthew Craven

Faculty Advisor: Dr. Terrance O'Connor, Dept of Computer Engineering and Sciences, Florida Institute of Technology

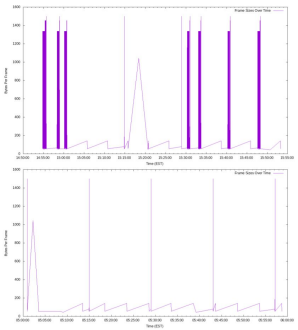
IoT devices exhibit patterns in their wireless transmissions that facilitate the creation of models to study their behaviour. In this study, we have constructed a labeled dataset of over 7000 samples of IoT device wireless communications from a variety of vendors. The dataset is hosted publicly online for use in further research. To showcase a usage of the dataset, we have constructed a machine learning based model to classify what signals are coming from which devices with 70% accuracy, verified using 30% of the dataset as the holdout set.

Capturing Methodology

In a lab setting we procedurally triggered IoT devices while recording their traffic, allowing us to generate labels during the creation of the datapoints. The pcap files output from airodump were then parsed, using our own script, into csv format.

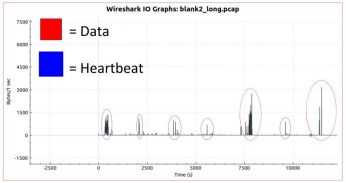


Example capture of network traffic from IoT locks



Top Image: Ring Doorbell Use activity
Bottom Image: Ring Doorbell Heartbeat activity

Example Model



Results

The model we trained to differentiate which device is currently communicating on the network works currently with 70% accuracy using a 30% holdout set. We also tried to train a model to determine if a door lock was locking or unlocking and it achieved 50% accuracy, again with a 30% holdout set for verification. Both models tested used SciKitLearn's RandomForestClassifier. The dataset currently contained 7392 labeled samples, and we have created a guide for future researchers to continue to populate the dataset.

Conclusions

Further research can be done to improve the model for classifying IoT device behaviour from an unprivileged perspective. In addition, further data should be added from both devices already in the database and new devices.

Works Cited

T. OConnor, R. Mohamed, M. Miettinen, W. Enck, B. Reaves, and A.-R. Sadeghi, "Homesnitch: Behavior transparency and control for smarthome iot devices," in ACM Conference on Security and Privacy inWireless and Mobile Networks (WiSec). Miami,FL: ACM, 2019.

T. OConnor, W. Enck, and B. Reaves, "Blinded and confused: Uncov-ering systemic flaws in device telemetry for smart-home internet ofthings," in ACM Conference on Security and Privacy in Wireless andMobile Networks (WiSec).Miami,FL: ACM, 2019.

Task Matrix for Milestone 6

	Alex	Cole	Jeremy	Steven	Todd	Complete
Data Collection				100%		100%
Machine Learning	100%					100%
Use Case Testing						
Conference Paper						
E-Book and Poster			50%		50%	100%
User Manual		25%	20%	25%	30%	100%
Demo Video	100%					100%

Questions?