

Detecting Malicious IoT Devices

Alex Korzyniowski & Jason Vettese

Department of Computer Science, University of New Hampshire



University of
New Hampshire

Summary

- Wanted to investigate the malicious behavior of common IoT devices
- Chose to test Smart Assistants like Amazon Echo since they are very common in households
- Created a methodology for analyzing IoT traffic with machine learning
- Packet captures on an isolated segregated network
- Machine learning to flag malicious traffic patterns
- Implemented Regression Decision Tree using the Gini index
- Investigated the security of popular IoT devices

Background

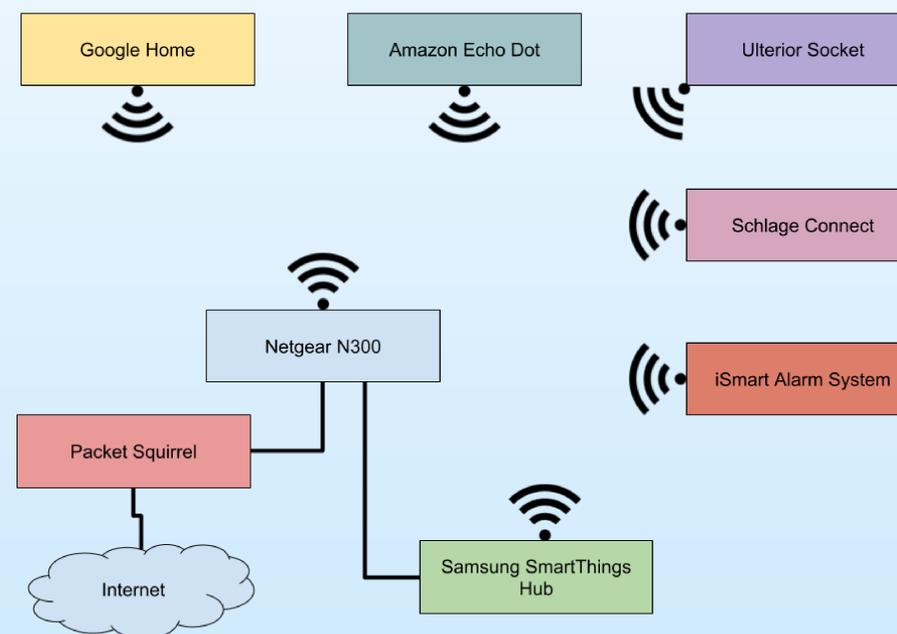
- IoT devices have grown quickly in popularity
- IoT devices have become a common attack vector
- There are few alternatives available for assessing IoT network traffic
- Compromised IoT devices put users at risk of stolen personal information and inadvertent involvement in cybercrimes are not properly secured
- The purpose of this project is to provide users with a method to flag potentially malicious traffic patterns.

Analysis

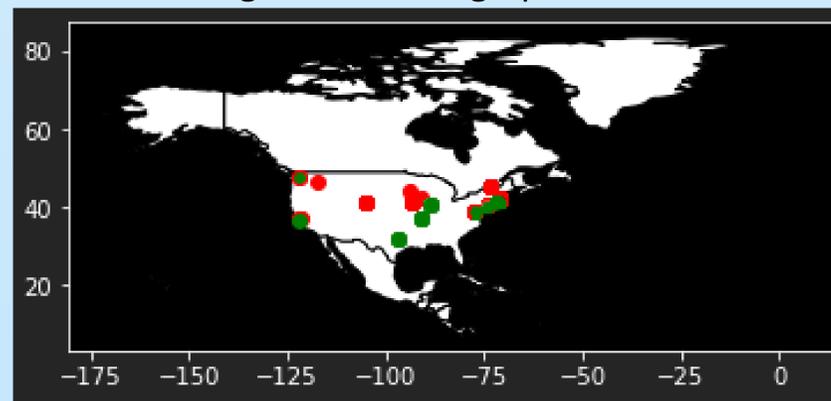
- Created Network to capture data
- Network comprised of Wireless Router and Zigbee Hub
- Captured both Wireless and Ethernet traffic
 - Wireless traffic was found to be not helpful
- Packet Squirrel was used to intercept data going inbound and outbound
- Machine Learning model was trained using a continuous dataset
- NetFlow data is primarily categorical data
 - Source IP, Destination IP, Protocol, and Packet Size
 - No deep packet inspection to reduce computational complexity
- Translation of IPs into geographic coordinates

Google Home	Amazon Alexa	Schlage Smart Lock
192.168.1.2 192.168.1.3 TCP 183	192.168.4.240 224.0.0.251 IGMPv2 60	3.93.142.211 192.168.1.2 TCP 60
192.168.1.3 192.168.1.2 TCP 183	192.168.4.254 239.255.255.250 IGMPv2 60	192.168.1.2 239.255.255.250 SSDP 214
192.168.1.2 192.168.1.3 TCP 183	192.168.4.254 224.0.0.252 IGMPv2 60	192.168.1.2 239.255.255.250 SSDP 214
192.168.1.3 192.168.1.2 TCP 183	0.0.0.0 255.255.255.255 DHCP 590	192.168.1.2 239.255.255.250 SSDP 214
192.168.1.2 192.168.1.3 TCP 66	192.168.4.1 255.255.255.255 DHCP 342	192.168.1.2 192.168.1.1 DNS 87
169.54.204.231 192.168.1.2 TLSv1.2 97	0.0.0.0 255.255.255.255 DHCP 590	192.168.1.1 192.168.1.2 DNS 103
192.168.1.2 169.54.204.231 TLSv1.2 101	192.168.4.1 255.255.255.255 DHCP 342	192.168.1.2 172.217.12.202 GQUIC 1392
169.54.204.231 192.168.1.2 TCP 66	192.168.4.253 192.168.5.5 DNS 78	192.168.1.2 172.217.12.202 GQUIC 794
192.168.1.2 192.168.1.3 AJP13 183	192.168.5.5 192.168.4.253 DNS 94	172.217.12.202 192.168.1.2 GQUIC 1392
192.168.1.3 192.168.1.2 AJP13 183	192.168.4.253 192.168.5.5 DNS 79	172.217.12.202 192.168.1.2 GQUIC 73
192.168.1.2 192.168.1.3 TCP 66	192.168.4.253 192.168.5.6 DNS 79	192.168.1.2 172.217.12.202 GQUIC 83
192.168.1.2 192.168.1.1 DNS 87	192.168.5.5 192.168.4.253 DNS 95	192.168.1.2 172.217.12.202 GQUIC 70
192.168.1.1 192.168.1.2 DNS 103	192.168.5.6 192.168.4.253 DNS 95	172.217.12.202 192.168.1.2 GQUIC 62
192.168.1.2 172.217.12.202 GQUIC 1392	192.168.4.253 54.239.27.116 TCP 74	172.217.12.202 192.168.1.2 GQUIC 341
192.168.1.2 172.217.12.202 GQUIC 791	54.239.27.116 192.168.4.253 TCP 66	172.217.12.202 192.168.1.2 GQUIC 170
172.217.12.202 192.168.1.2 GQUIC 1392	192.168.4.253 54.239.27.116 TCP 60	192.168.1.2 172.217.12.202 GQUIC 70
172.217.12.202 192.168.1.2 GQUIC 73	192.168.4.253 54.239.27.116 TLSv1.2 240	192.168.1.2 173.194.68.188 TCP 66
192.168.1.2 172.217.12.202 GQUIC 83	54.239.27.116 192.168.4.253 TCP 60	173.194.68.188 192.168.1.2 TCP 66
192.168.1.2 172.217.12.202 GQUIC 70	54.239.27.116 192.168.4.253 TCP 60	192.168.1.2 172.217.12.202 GQUIC 65
172.217.12.202 192.168.1.2 GQUIC 62	54.239.27.116 192.168.4.253 TLSv1.2 1514	172.217.12.202 192.168.1.2 GQUIC 62
172.217.12.202 192.168.1.2 GQUIC 341	54.239.27.116 192.168.4.253 TCP 1514	192.168.1.2 52.53.178.201 NTP 90
172.217.12.202 192.168.1.2 GQUIC 189	54.239.27.116 192.168.4.253 TLSv1.2 1514	52.53.178.201 192.168.1.2 NTP 90
192.168.1.2 172.217.12.202 GQUIC 70	54.239.27.116 192.168.4.253 TLSv1.2 141	192.168.1.2 187.170.29.136 NTP 90
192.168.1.2 192.168.1.3 TCP 183	192.168.4.253 54.239.27.116 TCP 60	187.170.29.136 192.168.1.2 NTP 90
192.168.1.3 192.168.1.2 TCP 183	192.168.4.253 54.239.27.116 TCP 60	192.168.1.2 208.75.88.4 NTP 90
192.168.1.2 192.168.1.3 TCP 66	192.168.4.253 54.239.27.116 TCP 60	208.75.88.4 192.168.1.2 NTP 90
169.54.204.231 192.168.1.2 TLSv1.2 97	192.168.4.253 54.239.27.116 TCP 60	192.168.1.2 173.194.68.188 TCP 66
192.168.1.2 169.54.204.231 TLSv1.2 101	192.168.4.253 54.239.27.116 TLSv1.2 180	173.194.68.188 192.168.1.2 TCP 66
169.54.204.231 192.168.1.2 TCP 66	192.168.4.253 54.239.27.116 TCP 1514	192.168.1.2 173.194.68.188 TCP 66

Network Capture Model

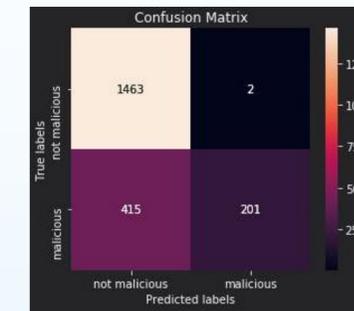


Google Home Geographic Data



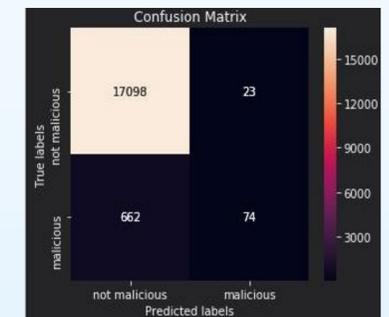
Results

Google Home:



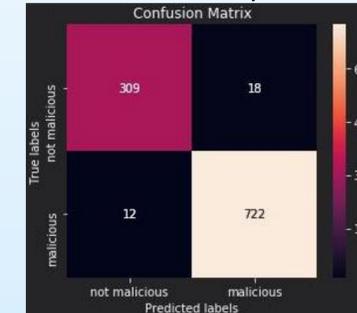
Google Home Model Accuracy: **74.75%**

Amazon Echo:



Amazon Echo Model Accuracy: **96.16%**

iSmart Alarm System:



iSmart Alarm Model Accuracy: **97.17%**

Discussion

The results that were attained from the model seem to make sense. It is interesting that the model was not able to predict the Google Home as accurately as the Echo or iSmart Alarm. This result is most likely due to the way the model is developed. The model gets more accurate with the more data that is given to it. In the case of the Echo, it had good accuracy since it had a large dataset.

Future Work

- “Your results are only as good as your data”
- Expanding malicious dataset to detect additional forms of traffic
- More Effective Man in the Middle detection
- Refine model parameters
- Live processing model