**IoT Network Traffic Dashboard Project Description**

IoT devices have become increasingly popular in recent years. With the introduction of smart home devices, everyday people now have more devices on their home network than ever before. This project aims to address some of the concerns consumers have with how their data is being handled by these devices and just how secure their home network is. A dashboard will be developed that provides users with a vast amount of network information in an easy-to-digest format. Some of the information that will be displayed includes exactly which IoT devices are connected to their network; all inbound and outbound network packets from these devices; information on the sender or receiver of these packets; statistics on how often this data is sent and received from these devices and if there are any unusual packets; as well as the security of these devices and how isolated they are from the rest of the devices on the network.

Determining some of the data that will be displayed to the users may involve a more complex process. For example, determining where the inbound and outbound packets are coming from. Preliminary findings using Wireshark for network packet capture will most likely suggest packets are being sent and received to/from either Amazon Web Services, Microsoft Azure, or Google Cloud Platform, the need for a deeper dive into the origins of the data is probable. In addition, to determine how secure the devices are, each device will be tested against popular known vulnerabilities to see if they are affected. If they are, it should be made clear what is now accessible, or may be in the future. Things such as sensitive user data, other devices, etc. may be affected which should be made known to the user. The data collected will also be used for statistical modelling, alerting the user of any anomalies in the way their IoT devices are behaving, and suggestions to increase the security of their network.

IoT Network Traffic Dashboard Schedule

| Date | Goal |
| --- | --- |
| Week of September 5th | **Preliminary Project Research** |
| Details: | This includes what tech stack I will be using and learning any required technologies. |
| Week of September 19th | **Preliminary Project Research** |
| Details: | More detailed planning, for example how the dashboard will look or which vulnerabilities I will be testing. |
| Week of October 3rd | **Analyzing Network Packet Capture** |
| Details: | Identifying IoT devices on the network and their inbound and outbound packet transfers. |
| Week of October 17th | **Analyzing Network Packet Capture – Cont’d** |
| Details: |  |
| Week of October 31st | **Developing Dashboard Interface** |
| Details: | Developing the main interface. |
| Week of November 14th | **Easy to Digest Data Visualization** |
| Details: | Presenting the data in a way users without a tech background can understand. |
| Week of November 28th | **Working on Stretch Goals / Draft Report** |
| Details: | Begin work on the final report and submit a draft. If there is time, try to implement various stretch goals outlined below. |
| Week of December 5th | **Writing Final Report** |
| Details: | Continue writing the final report and submitting the project. |

# Core Goals

|  |
| --- |
| * Network Traffic Dashboard * Information on source/destination of packets * Data on how often information is sent outside of the network from these devices * Access to logs of the data being sent (maybe estimations on what this data could be as well?) * Digestible data visualization on all important findings (packet source/destination, etc.) * Final Report |

# Stretch Goals

|  |
| --- |
| * Vulnerability testing on all devices * Identifying and alerting the user on abnormal packet transfers * A section of the Network Traffic Dashboard where users can see a more detailed look at information, for users with more of a tech background * Tips on how to potentially make the network more secure * Alerts if IoT devices on the network are acting abnormal |