Analyzing Ring Doorbell Network Traffic

Group members: Amelia Pasco

Project Topic: Network Traffic Data Collection and Analysis of a Ring Doorbell

Introduction

The goal of this project is to analyze the network traffic of a Ring doorbell device using Wireshark. The traffic capture was taken by capturing the doorbell's network traffic over WiFi, and by generating traffic by moving in front of the doorbell. The packet capture was then analyzed using a Python script that analyzed the total packet count, the different protocol counts, and the source and destination IP addresses.

Methods

The network traffic was captured using Wireshark on a computer connected to the same WiFi network as the Ring Doorbell. To generate network traffic from the doorbell, I moved in front of the doorbell for 10 seconds to trigger the motion detection. I wrote a script using python to analyze the packet capture, using specifically the pyshark library. The script got info about the total packet count, various protocol counts, and stored the source and destination IP addresses in a dictionary. It still needs fine tuning, so I conducted a manual analysis of the packet capture.

Results

The preliminary results show that there are three different source IPs associated with the Ring doorbell (this could be from all our other Ring cameras), which are broadcasting under the ARP protocol. The ARP protocol is used by devices to map a network address to a physical address, like a MAC address. In this case, the Ring doorbell could be using the ARP protocol to discover other devices on the network and create a mapping of IP addresses to MAC addresses. Further investigation into the source and destination IP addresses in the packet capture is needed, as well as more info on the network protocols used by the Ring doorbell. I also believe another packet capture with more generated traffic could also provide more detailed results.

Link to pcap
https://github.com/ameliap123/cpe400/tree/main