Analyzing Ring Doorbell Network Traffic

Group Members: Amelia Pasco

Goal of the project: I want to ensure that the Ring Doorbell data is encrypted and cannot be viewed without a key or credentials. I also want to determine if the doorbell has sent the data to the cloud and not to any unauthorized actors.

Details of Code:

- **How to run:** You should have your pcapnp file in the same folder as the script and it must be named “ring.pcapng”. To run the script, use the command “python3 ringAnalyzer.py”
- **Environment:** You need the libraries “scapy” and “prettytable”
- **Input/Output:** The script will prompt for the IP address of Ring device you wish to analyze. It will then output a destination address table with the different addresses and the associated packet count. It will output a destination port table with the different ports and their associated packet count. And lastly, it will output a protocol table with the protocols used and their associated packet count.
- **Extra comments:** My code focuses more on traffic sent from the given IP, not traffic sent to it. It didn’t seem relevant as the goal of this project was to see if the doorbell data was being sent securely.

Details of data: it should be a pointer to data

- **Pointer to data:** Below is the github link to the data I collected and project code https://github.com/ameliap123/cpe400/tree/main
- **Cleaning and processing:** Please describe how you cleaned the data, or if it needed any additional processing. The pcapng file didn’t need additional processing as the script would only be looking at the data from the given IP address anyways.
- **Any extra comments:** If I were to clean the data, I would add a capture filter on WIreshark so that it only captures traffic associated with the given IP. But it is easier for the script to do it as you can change the IP you are analyzing.

Methodology: For this project, I first collected network traffic using Wireshark and saved it as a .pcapng. For the packet capture, I set off my family's Ring Doorbell with movement as well as rang the doorbell. Additionally, I had a live feed on my phone of the doorbell’s activity. For the analysis, I believe the categories for destination IP, destination port, and protocol, would sufficiently allow me to determine if the Ring Doorbell data was secure. I chose this project because I was curious how Ring Doorbell data was transported and what steps were taken to provide security. I looked at this video provided below for reference, as it showed how Wireshark captured image files from a security camera.
https://www.youtube.com/watch?v=va1wUSPGgSU

Evaluation results:

- **Destination Address Analysis:**

  With this analysis, we see the destination IPs the user provided Ring Doorbell address was talking to. We are trying to determine where the ring data is being sent and if there are any destination IPs that are unexpected. The results show that 192.145.118.152 was the most frequent, which is the IP address of my phone. The 239.255.255.250 is a reserved multicast address used for the Simple Service Discovery Protocol (SSDP). This is normal traffic as it is just devices on the network advertising their services. In conclusion, the Ring Doorbell was only sending data to the live feed running on my phone.

```
Enter the source IP address to filter by: 192.168.1.164
+-----------------------+--------------+
| Destination Addresses | Packet Count |
+-----------------------+--------------+
|    192.145.118.152    |     316      |
|    239.255.255.250    |      22      |
+-----------------------+--------------+
```

- **Destination Port Analysis:**

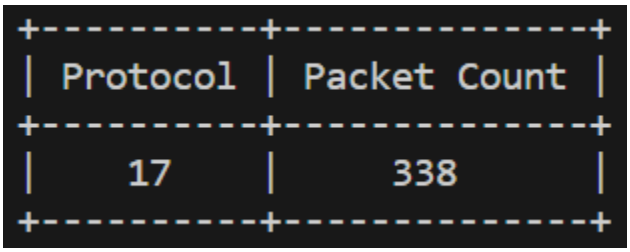
  With this analysis, we see the destination ports used by the Ring Doorbell during the experimentation. With this data, we are able to determine what services are being used to transport data to the Ring's cloud storage. The results showed small amounts of traffic on port 1900, which is used for SSDP. This is normal and expected traffic. The results also showed that the doorbell mainly used the port 51820, which is associated with UDP protocol Wireguard VPN service. It is not uncommon for IoT devices to use VPNs to establish secure connections, so we can conclude that the Ring Doorbell is using the WIreguard VPN to tunnel traffic to my phone during the live feed.

```
+-------------------+--------------+
| Destination Ports | Packet Count |
+-------------------+--------------+
|       51820       |     316      |
|        1900       |      22      |
+-------------------+--------------+
```

- **Protocol Analysis:**

  With this analysis, we see the protocols used by the Ring Doorbell and how often they are used throughout the packet capture. We are trying to determine what transport protocols are being used to transfer the Ring Doorbell data. The results showed that the Ring Doorbell used the protocol 17, which is UDP. Ring uses UDP mainly for realtime

audio and video streaming. This makes sense as I was running a live feed of the Ring Doorbell on my phone, and streaming services utilize protocols like UDP.



Protocol	Packet Count
17	338

Workload: I am the only member in my team.

Tools that you used: For data collection, I used Wireshark to capture the network traffic of the Ring Doorbell. To analyze the data I used the python programming libraries ring_doorbell and scapy.

Challenges: In the beginning, I struggled with getting the proper packet capture but found that moving in front of the Ring Doorbell for longer periods of time would be easier to analyze in the capture. I also struggled with finding the IP address for the Ring Doorbell, but the Ring App showed the MAC address for the device. So I used the MAC address in Wireshark and looked at ARP requests to find the IP.

Future directions: I think that, if I had more time for this project, I would like to see if I could decrypt the Ring Doorbell data so I could view it. In the video I watched as a reference for the project, he reset the connection of users on the network and intercept the passwords or credentials as they reconnect using Wireshark to decrypt or deauthorize the security camera's data. I think security would be a good topic for a class project, we like hacking things.