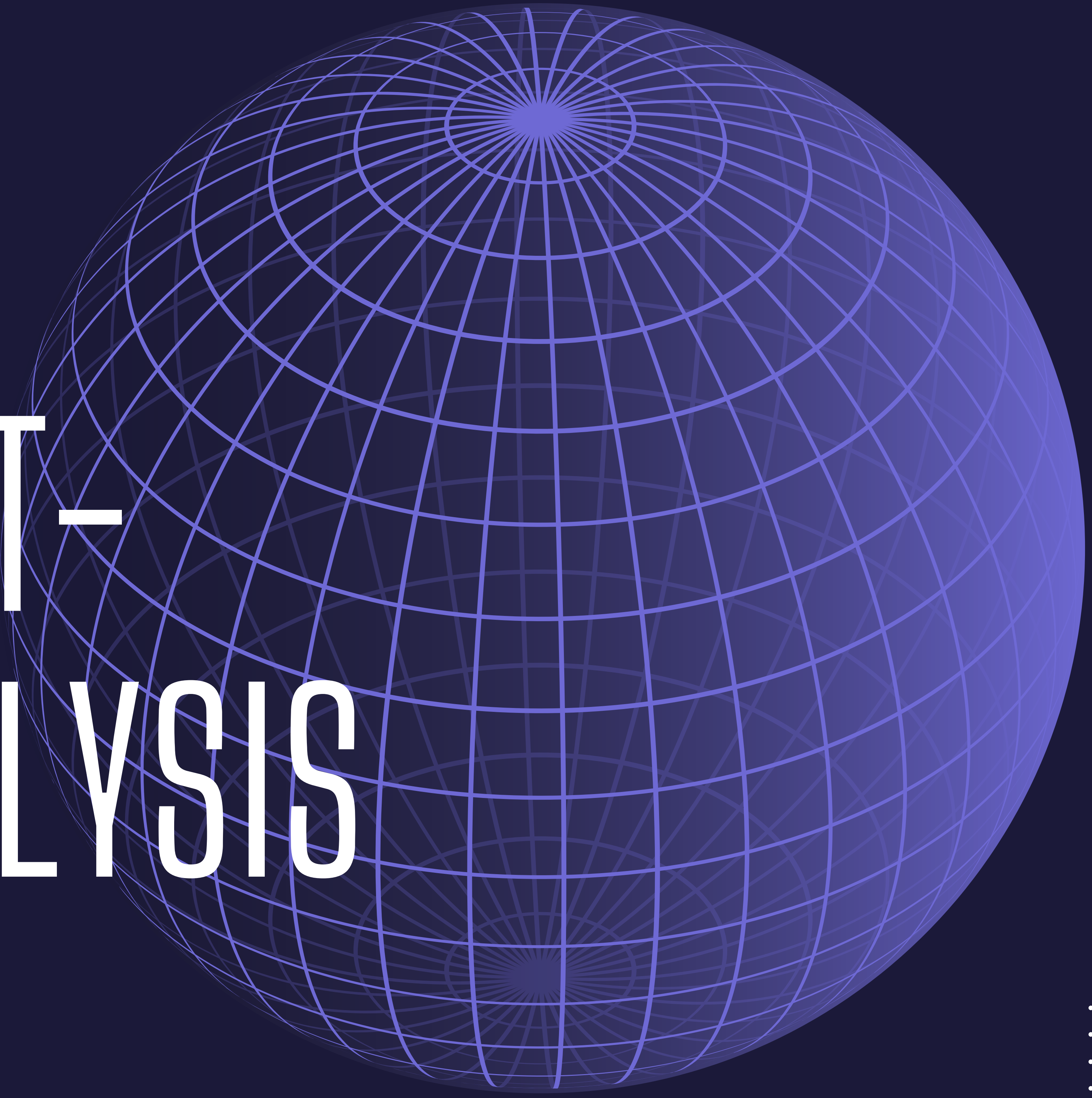
CASE STUDY: IMPROVING RT-IOT2022 ANALYSIS



DON ELEAZAR T. FERNANDEZ

PRINCE WALLY G. ESTEBAN

RT-IOT DATASET

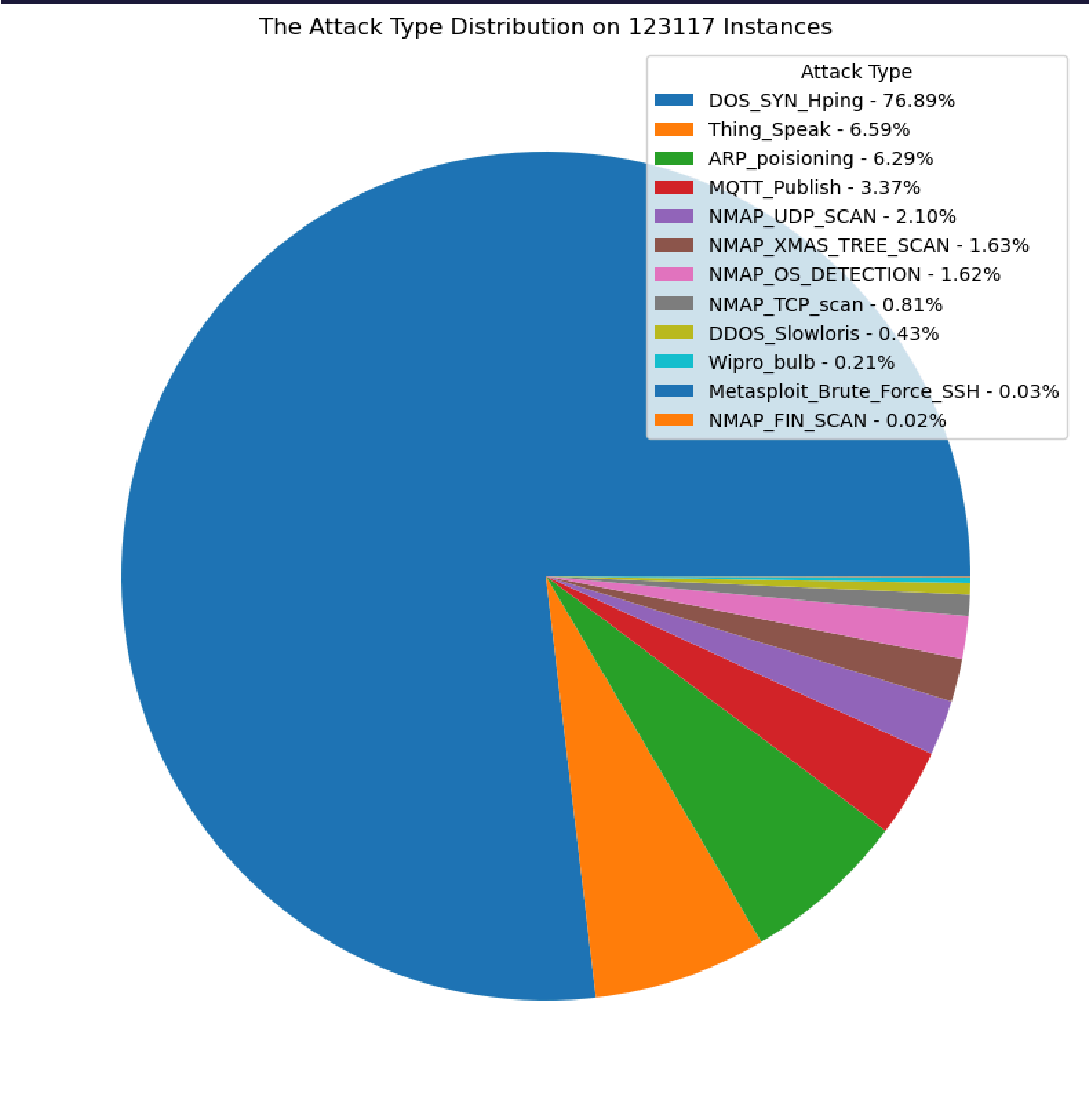
The “RT-IoT2022" is a dataset created from IoT networks. It includes data from IoT devices, as well as cyberattacks, such as Brute-Force SSH, and DDoS attacks. It shows how both normal and harmful network traffic look.

WHAT WE DID

- Cleaned The Dataset
- Performed Transformations
- Determined The Statistics (Mean and Standard Deviation)
- Analyzed The Results

INSIGHTS

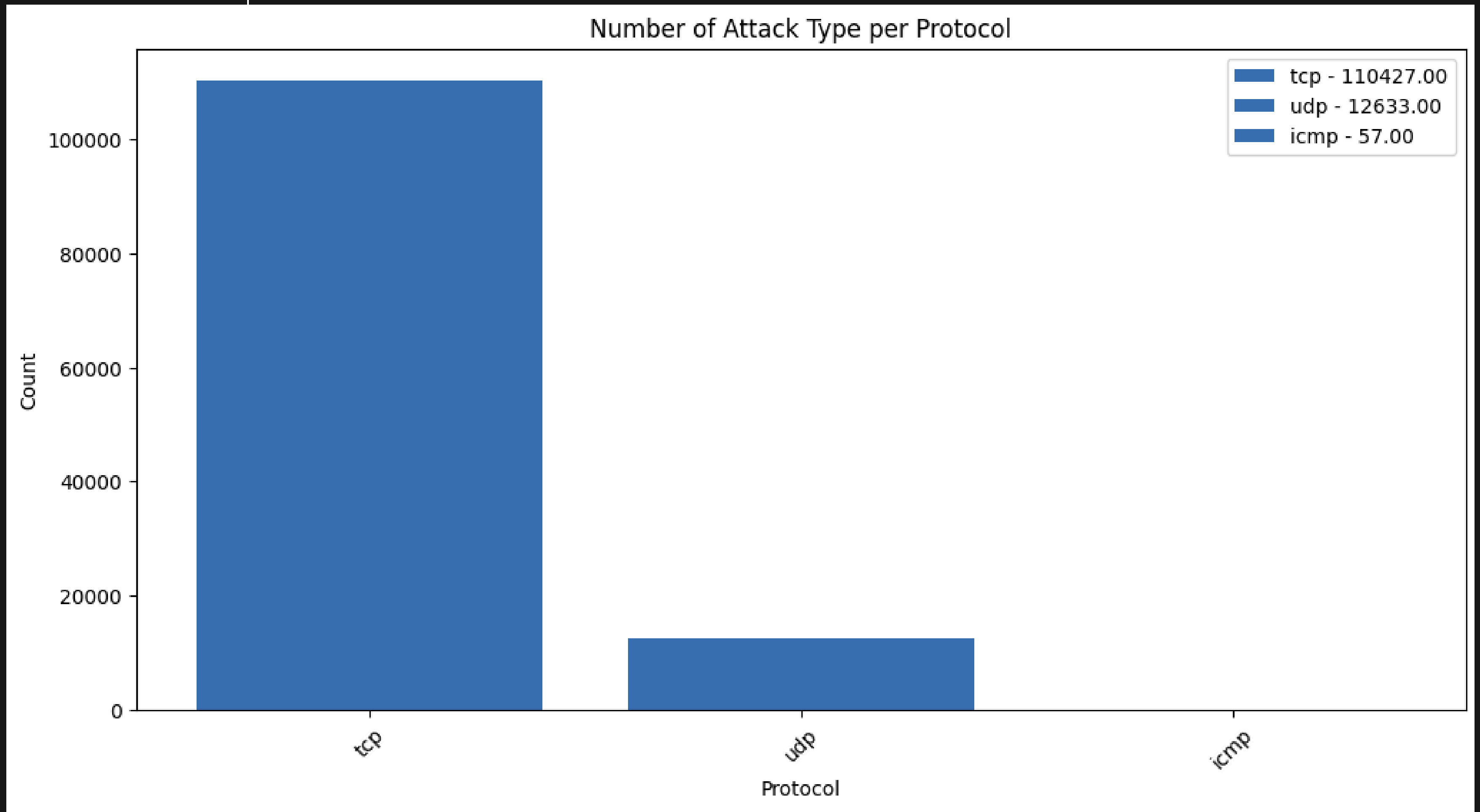
- The most dominant attack types are:
    - DOS_SYN_Hping: 76.89%
    - Thing_Speak: 6.59%
    - ARP_poisoning: 6.29%

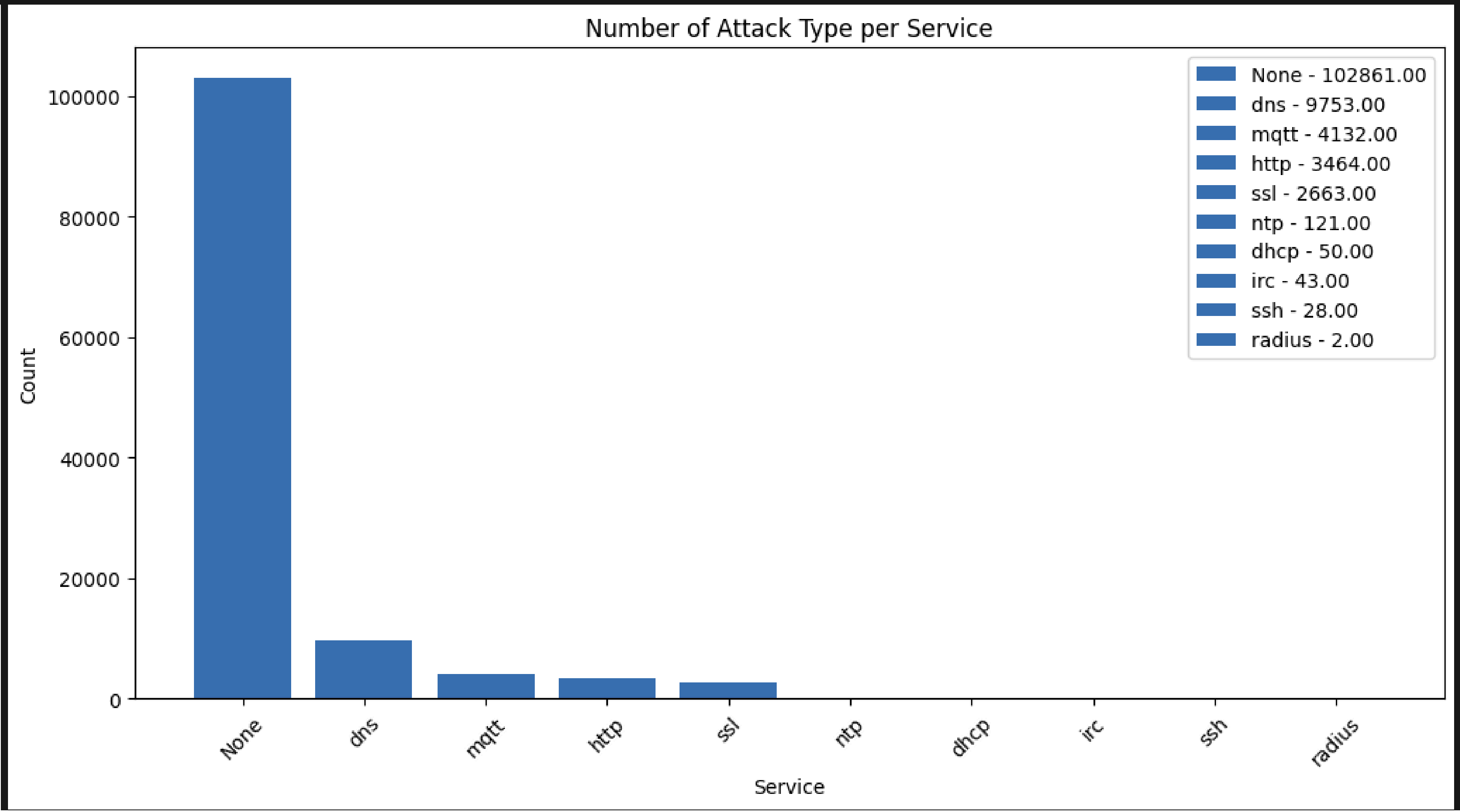


ESTEBAN | FERNANDEZ

INSIGHTS

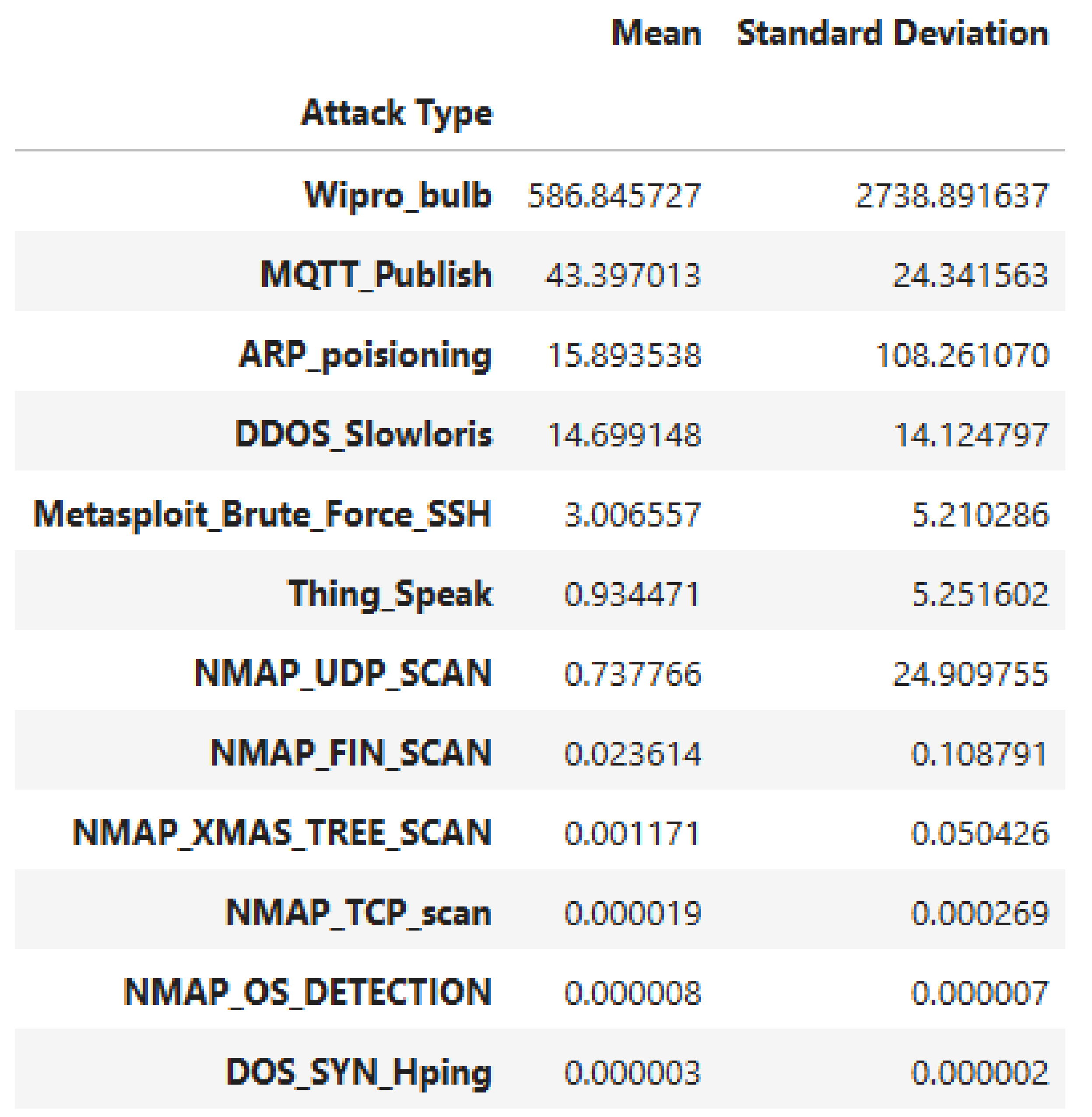
- Protocol and Service vary across different attack types. The most common are:
  - TCP in protocol - 110427
  - None in service - 102861



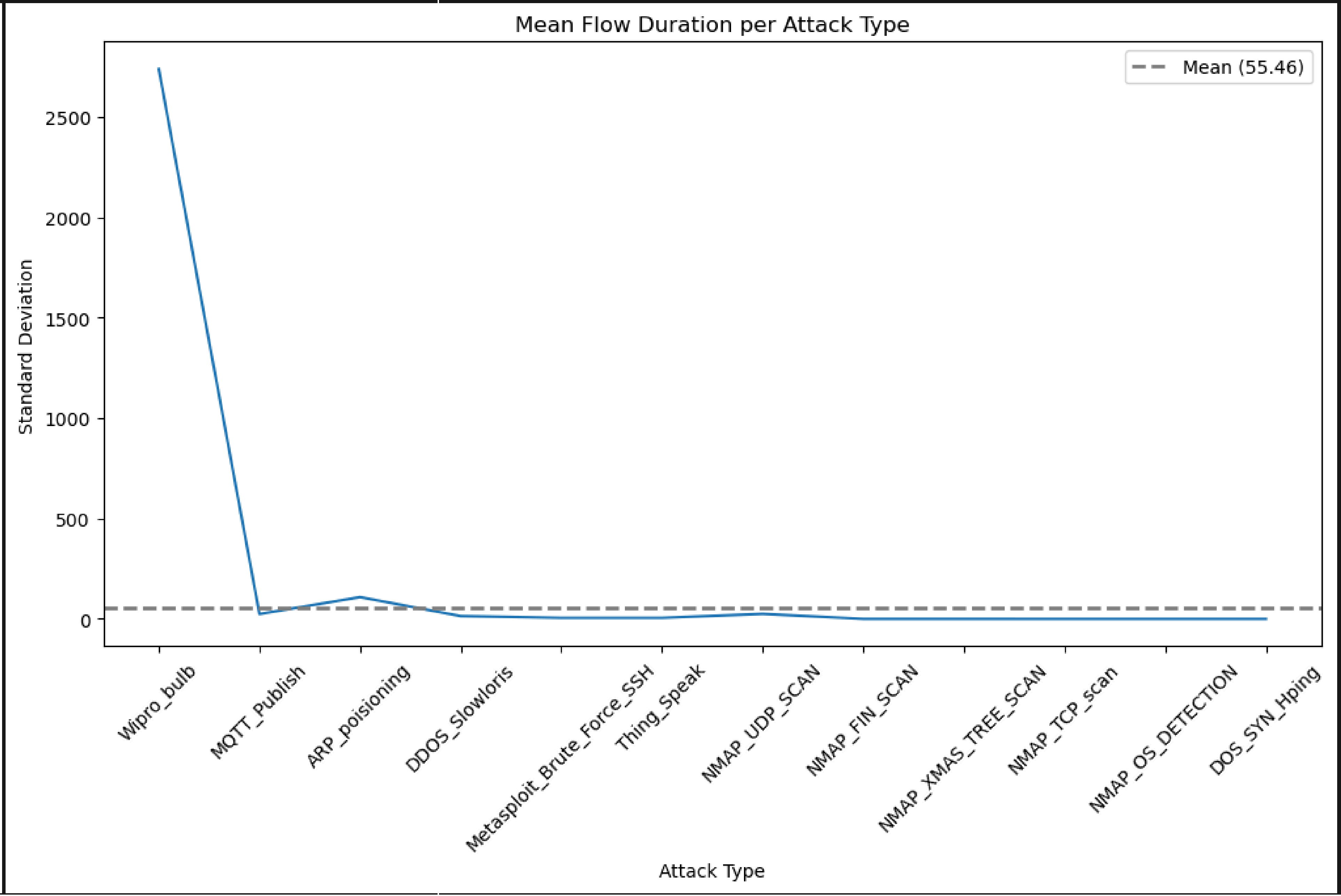


INSIGHTS

- Flow durations vary per attack type: The Highest Flow Duration: Wipro_bulb - 586.85



Attack Type	Mean	Standard Deviation
Wipro_bulb	586.845727	2738.891637
MQTT_Publish	43.397013	24.341563
ARP_poisioning	15.893538	108.261070
DDOS_Slowloris	14.699148	14.124797
Metasploit_Brute_Force_SSH	3.006557	5.210286
Thing_Speak	0.934471	5.251602
NMAP_UDP_SCAN	0.737766	24.909755
NMAP_FIN_SCAN	0.023614	0.108791
NMAP_XMAS_TREE_SCAN	0.001171	0.050426
NMAP_TCP_scan	0.000019	0.000269
NMAP_OS_DETECTION	0.000008	0.000007
DOS_SYN_Hping	0.000003	0.000002



CONCLUSION

To conclude, the analysis reveals that DOS_SYN_Hping is the most common attack, highlighting vulnerabilities in SYN flood attacks, with TCP being the most targeted protocol. Attacks are also more frequent when no specific service is listed. The Wipro_bulb attack shows high variability in duration, while attacks like MQTT_Publish and ARP_poisoning are more consistent. These findings emphasize the need for better protection of the TCP protocol, unspecified services, and more effective detection of attacks with varying durations.

RECOMMENDATIONS

- Strengthen security for the TCP protocol
- Secure unspecified services ("None")
- Improve detection and monitoring of attacks with varying durations