DDoS Attack Detection

Eric Blander
@EricB10

DDoS Attack

Distributed Denial of Service (overwhelm server with bots)

$9.3 Billion

Spent in 2019 on prevention & mitigation

10 Million

Est. DDoS attacks in 2020

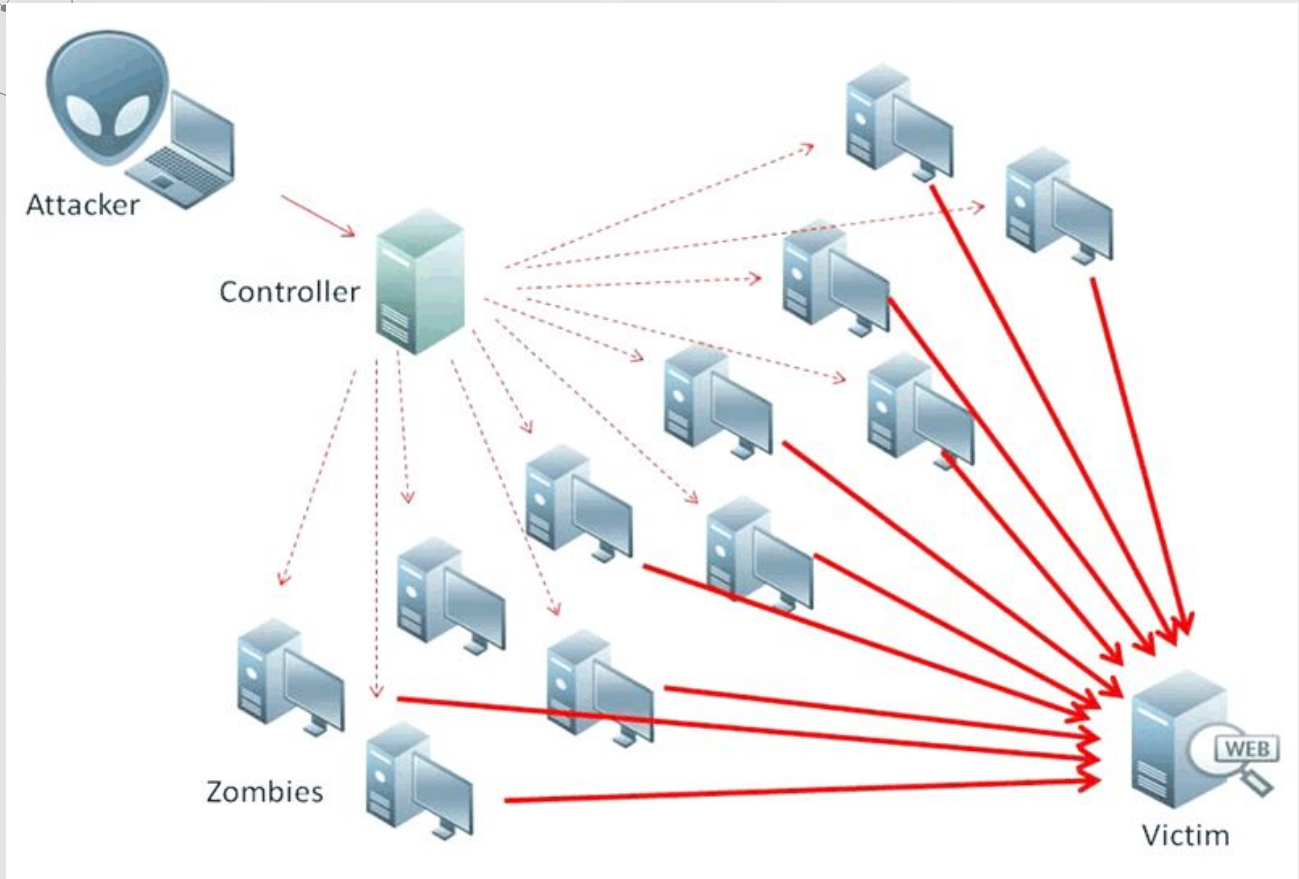
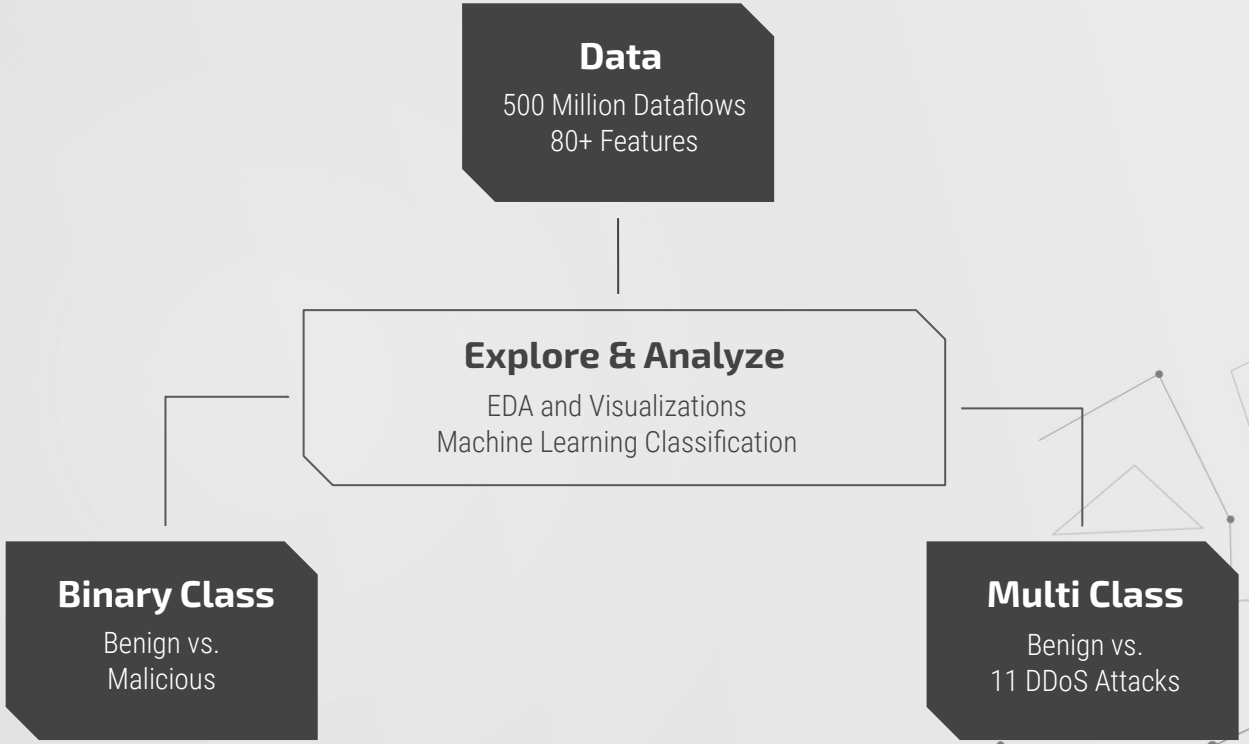
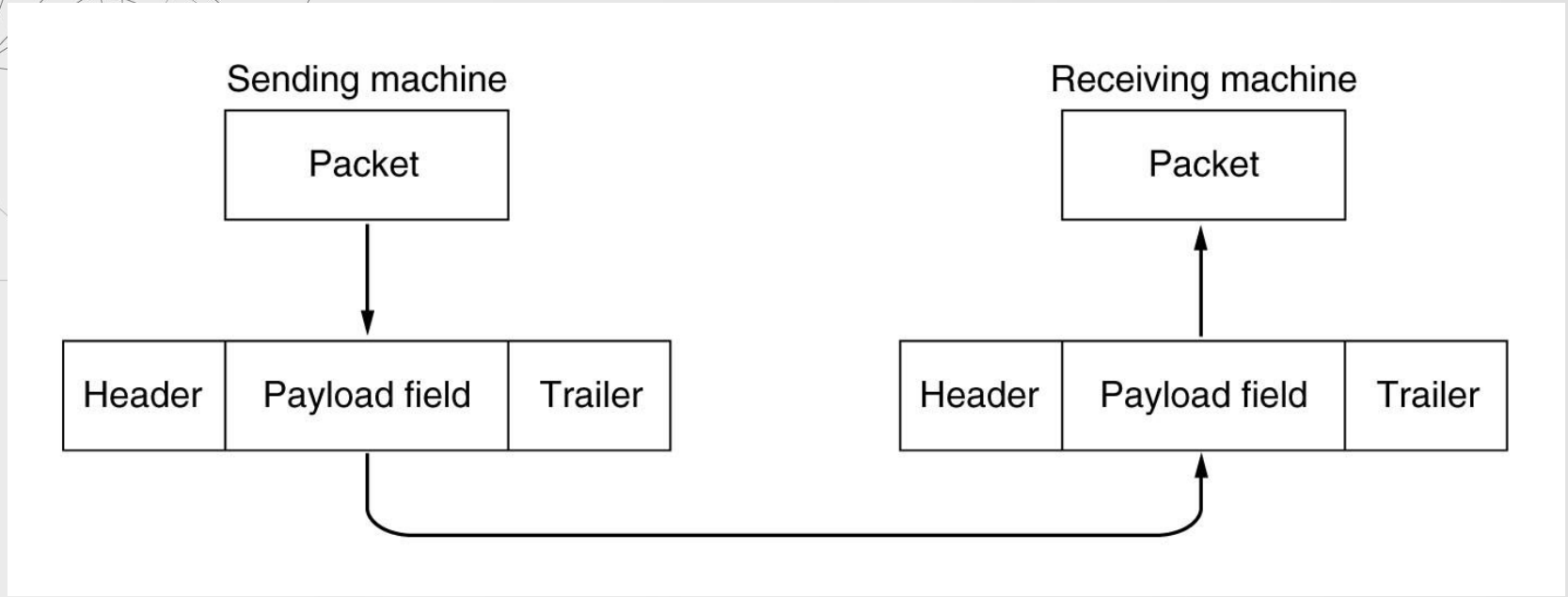


Image Source: WPDIY

Process


Data
500 Million Dataflows
80+ Features
Explore & Analyze
EDA and Visualizations
Machine Learning Classification
Binary Class
Benign vs.
Malicious
Multi Class
Benign vs.
11 DDoS Attacks



Each dataflow consists of many packets

Important Features

Protocol

TCP, UDP, etc

Packets & Headers

Total Forward & Backward
Min, Max & Mean Size

Initial Window

Duration & Size

Flow Time

Duration
Down & Uptime

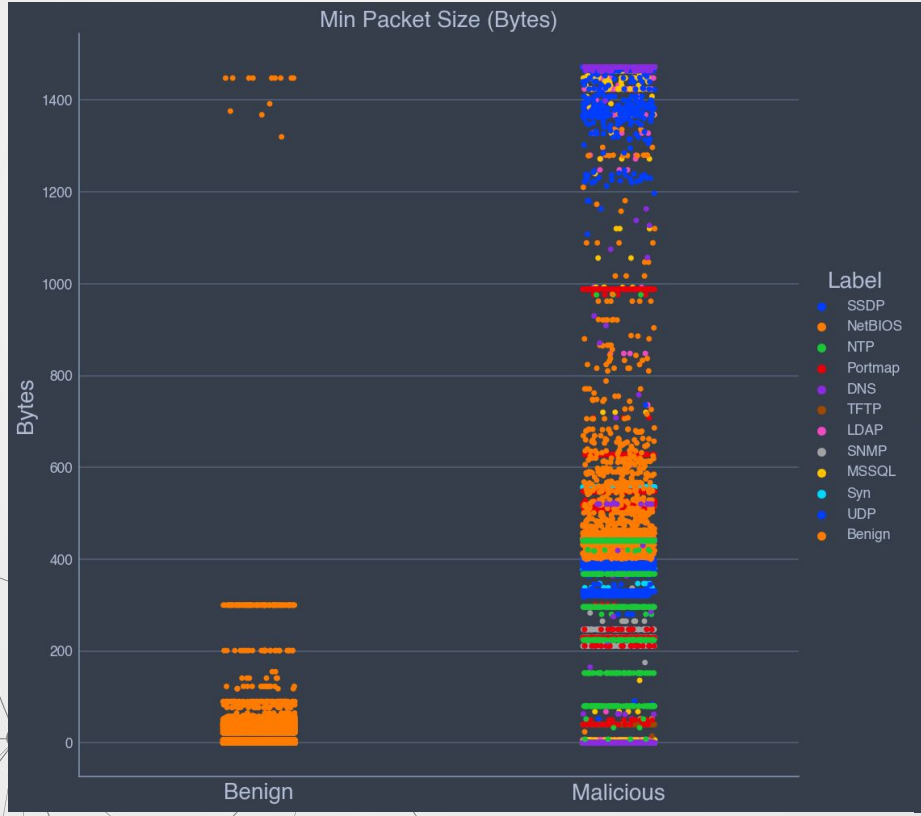
Transfer Rates

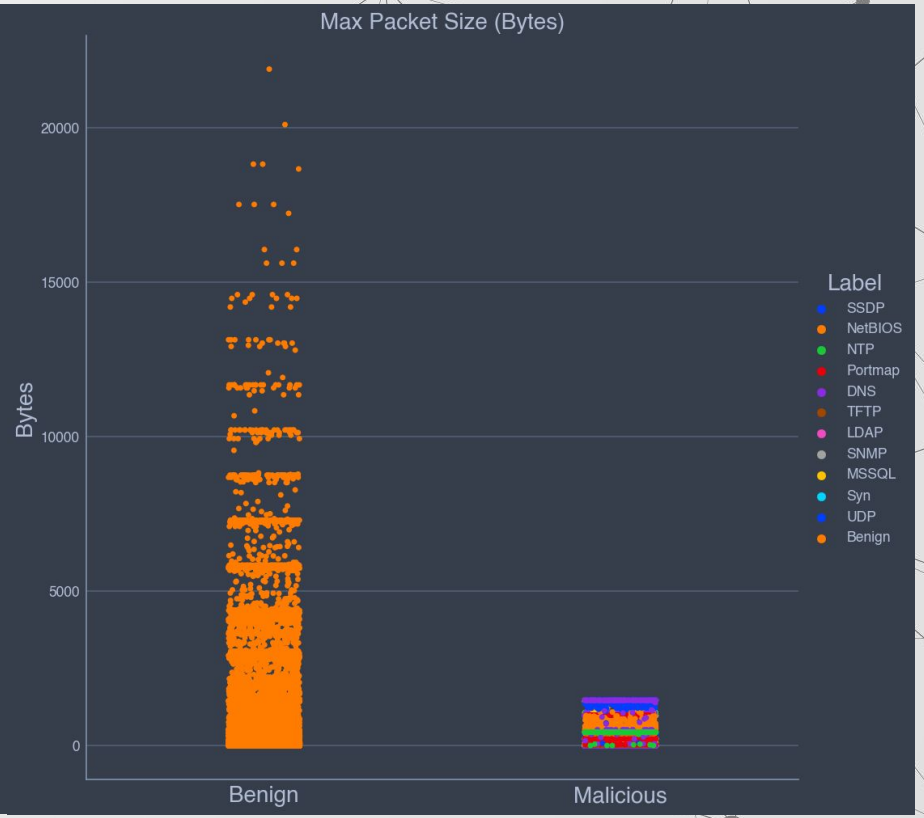
Bytes/Sec
Packets/Sec

Flags

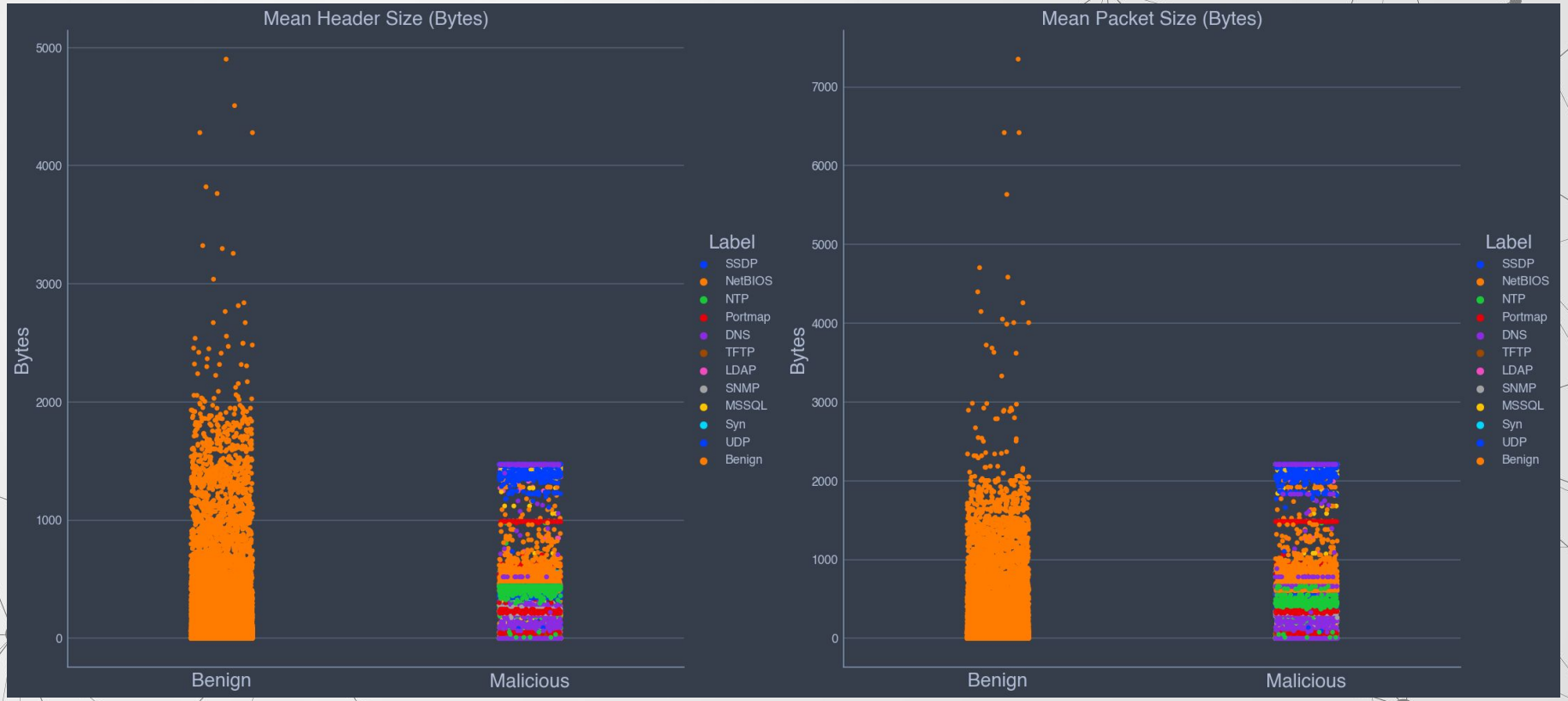
ACK, URG, etc

Min & Max Packet Size





Mean Header & Packet Size



Balanced Dataset
(50% Benign, 50% Malicious)

	Binary Cl Acc	Binary Cl F1	Multi Cl* Acc	Multi Cl* F1
Decision Tree	99.8%	99.8%	84.6%	84.7%
Random Forest	99.9%	99.9%	85.2%	85.1%
XGBoost	99.9%	99.9%	86.5%	86.4%

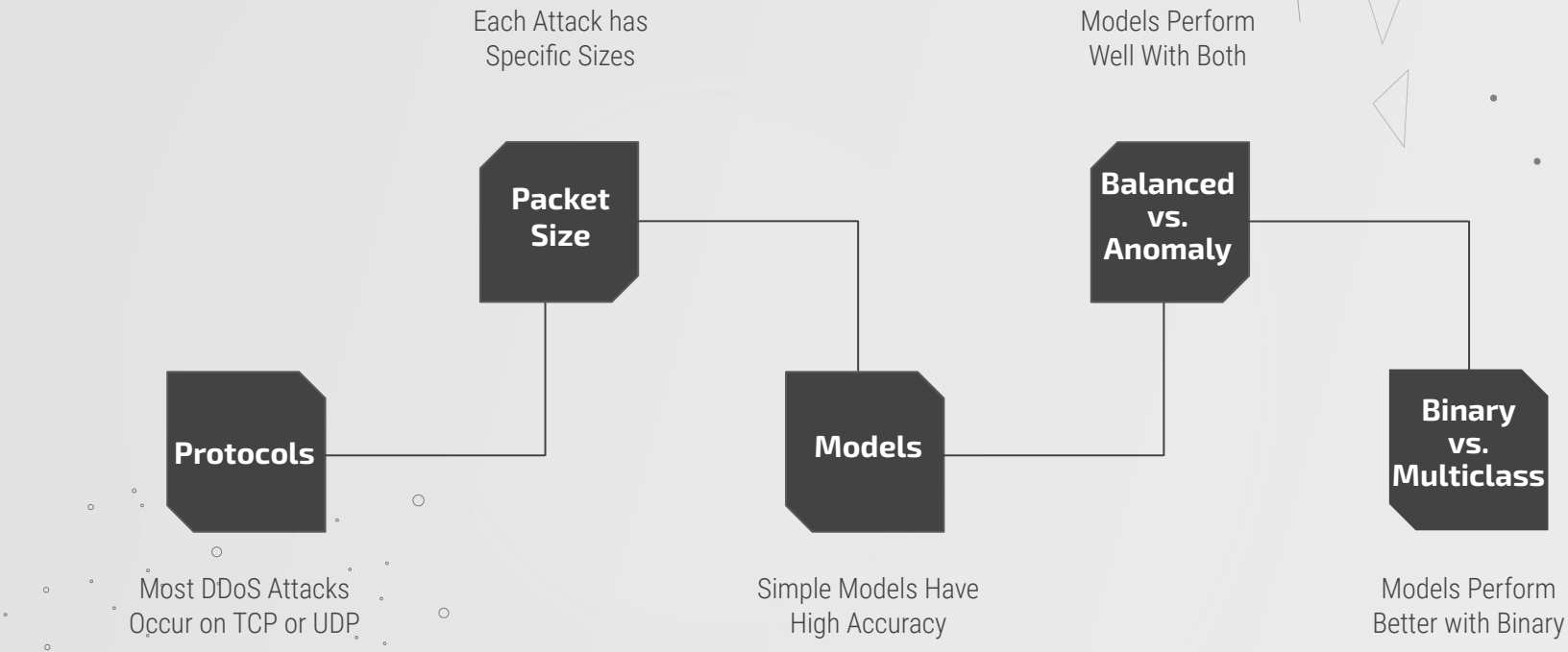
***Multi Class:** Benign + 11 Distinct DDoS Attacks

Anomaly Detection Dataset (99% Benign, 1% Malicious)

	Binary Cl Acc	Binary Cl F1	Multi Cl* Acc	Multi Cl* F1
Decision Tree	99.7%	99.6%	82.1%	82.8%
Random Forest	99.9%	99.8%	83.0%	83.1%
XGBoost	99.9%	99.9%	83.9%	83.8%

***Multi Class: Benign + 11 Distinct DDoS Attacks**

Conclusions



Future Plans

Larger Data

Train models on dataset
.01% malicious dataflows

Real Time

Deploy trained model
on real-time data

Front End

Implement into
Application with GUI

Thanks

Eric Blander
@EricB10

Special thanks to the
Canadian Institute for Cybersecurity