UMD Info Challenge 2022 Cybersecurity Dataset

MIDN Kade Heckel, Jennifer Jung,
Brenton Pieper, and Christian Rose

Background

Malicious hackers and automated malware attacks are one of the biggest threats facing cybersecurity experts today. To help encourage novel solutions to these problems, researchers at the Canadian Institute for Cybersecurity have assembled a number of datasets cybersecurity researchers and practitioners can use to evaluate their malware detection methodologies. The dataset for this challenge represents a subset of their 2012 Intrusion Detection Evaluation Dataset. Here, the UNB researchers employed real cyber attack and malware scenarios, along with background network traffic simulations to create an evaluation dataset.

Questions to Answer

Challenge 1: Help improve cybersecurity for networks. Create a machine learning model to predict whether network traffic is associated with normal (Tag=”Normal”) or malicious (Tag=”Attack”) activities.

Challenge 2: Predict Internet Traffic. Create a machine learning model to predict what type of traffic each row represents, using the column “appName”.

Challenge 3: Understanding a network. Do exploratory data analysis to understand activity on this network, and create informative visualizations to convey this information.

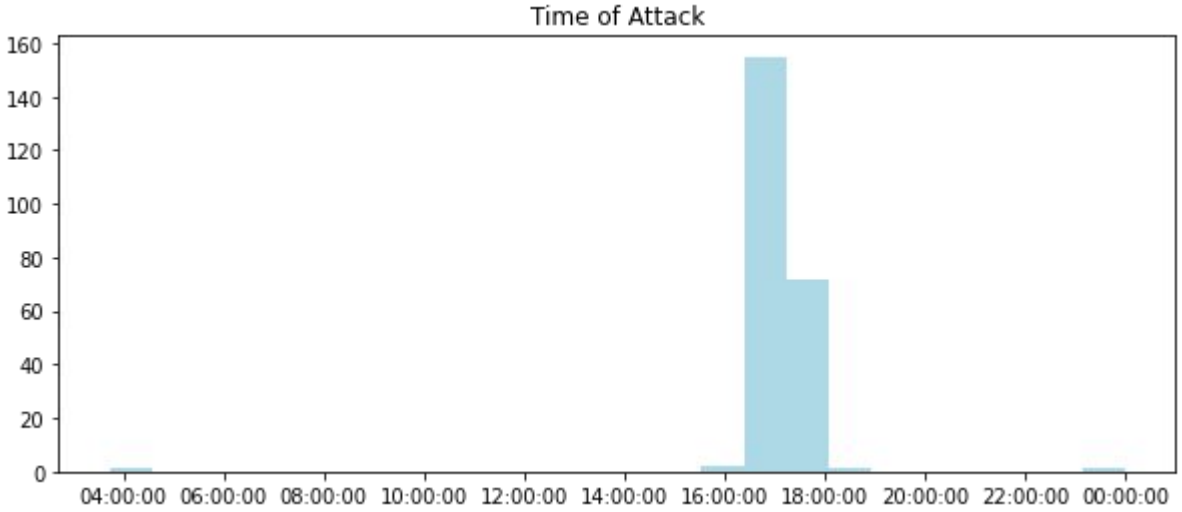
The Problem and The Data

- The dataset is network packet information for our local network
- Packets are labeled attack and normal
- An example of a specific attack is seen here

	start	Tag	appName	destination	destinationPayloadAsBase64	destinationPayloadAsUTF	destinationPort
37	2010-06-13 23:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
3614	2010-06-14 00:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
9156	2010-06-14 01:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
16533	2010-06-14 02:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
21699	2010-06-14 03:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
30672	2010-06-14 04:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
44092	2010-06-14 05:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
55669	2010-06-14 06:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
64693	2010-06-14 07:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
78499	2010-06-14 08:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
84909	2010-06-14 09:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
101732	2010-06-14 10:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
117714	2010-06-14 11:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
124935	2010-06-14 12:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
128596	2010-06-14 13:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
131710	2010-06-14 14:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0
134503	2010-06-14 15:59:17	Attack	Unknown_TCP	131.202.243.84	NaN	NaN	5555.0

Challenge 3: Data Visualization

How can we get information about these attacks that will help us defend better going forward?



Is the spike at 1700 really due to increase in cyber activity or is that when the defenders run their packet collection services?

Challenge 3: Data Visualization

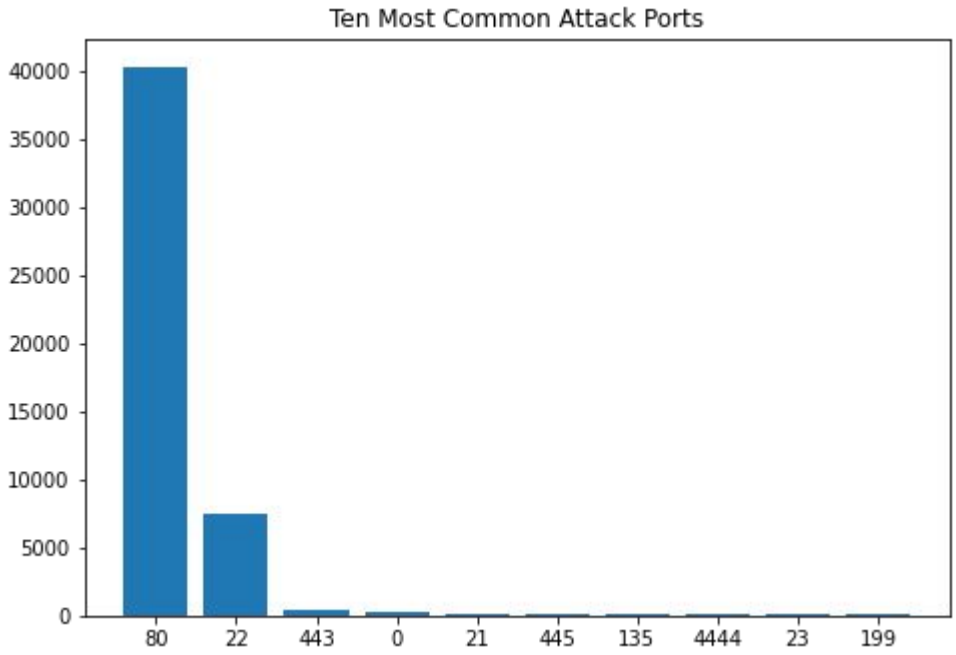
Port 80 (HTTP)

- The biggest vector of cyber attacks is still websites hosted by the victims

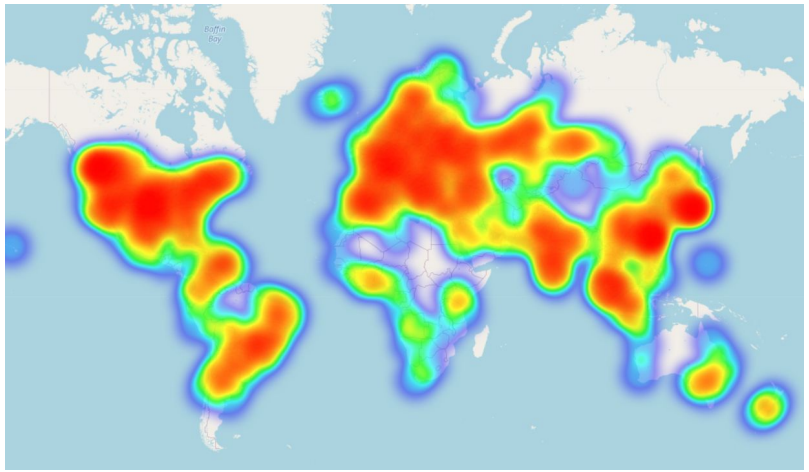
Port 22 (SSH)

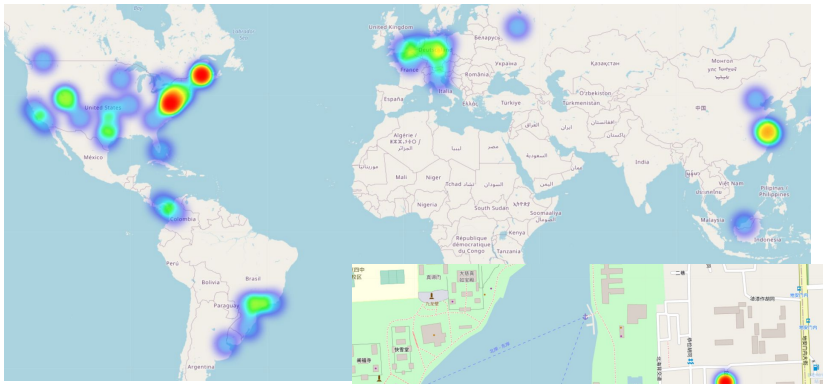
- Secure shells are used commonly to establish connections between attackers and victims

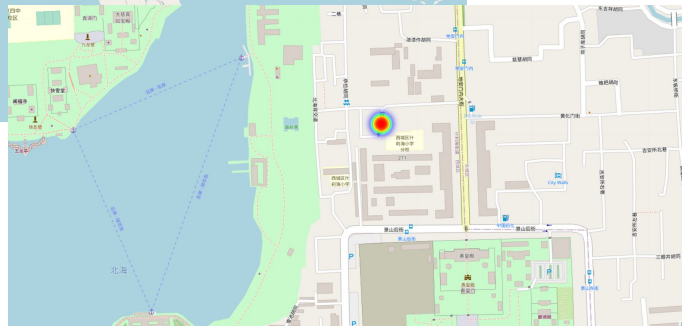
Other common ports commonly used in attacks: FTP (21), Samba (445), Microsoft RPC (135), Common attack ports used by “script kiddies” (4444 and 5555)



Data Visualization: Location Data



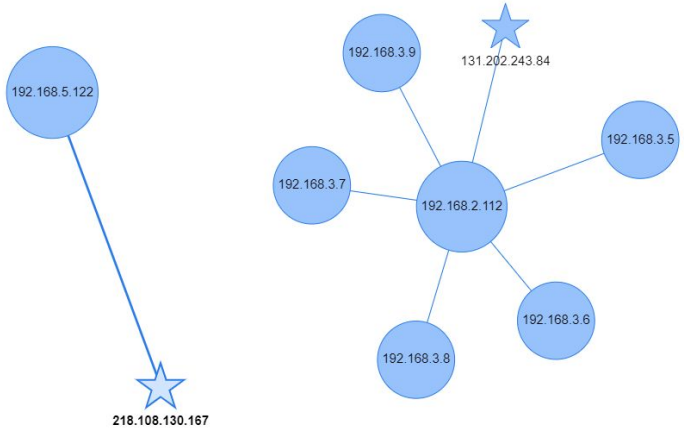


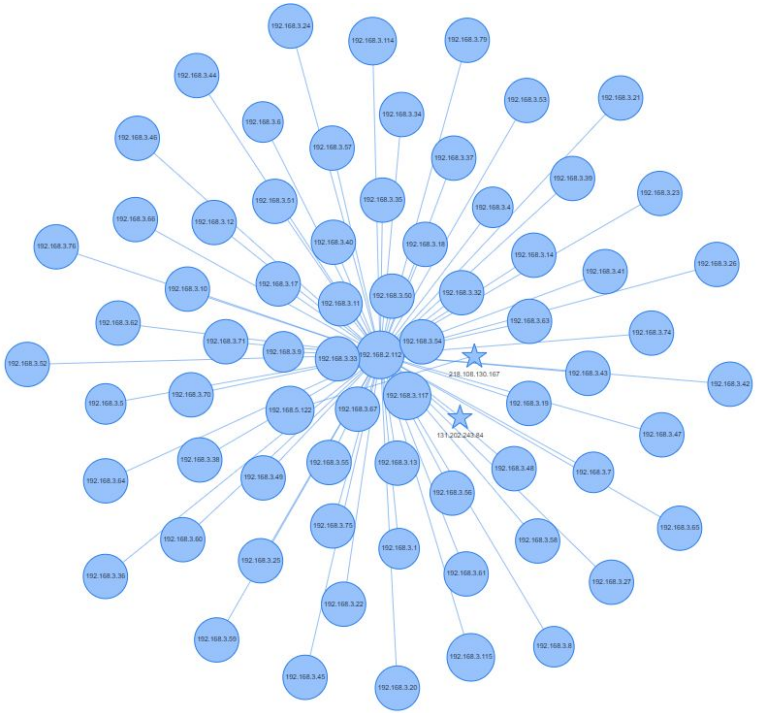


Benign Map - Packets originating from everywhere

Attack Map- Very specific IP addresses, often associated with cities

Data Visualization: Initial Attack vs. Series of Attacks



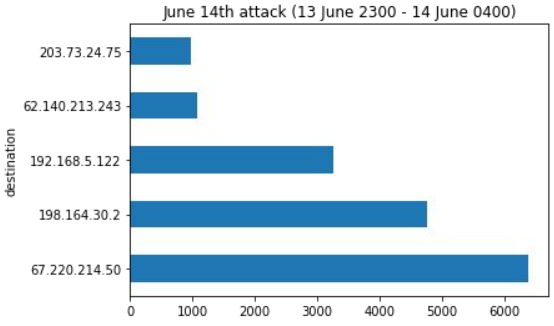


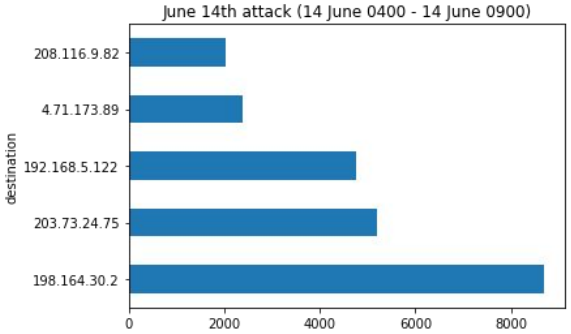
Following the Attack Chain

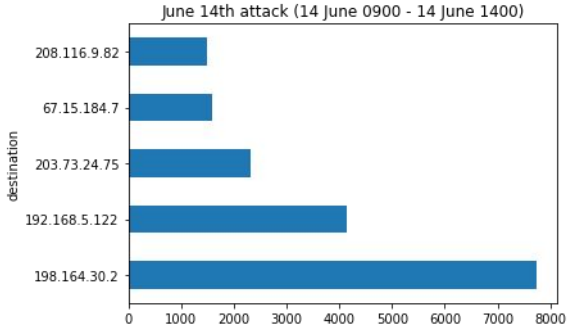
We isolated one instance of an attack between 2300 on June 13th, 2010 to 1700 on June 14th, 1700 targeting port 5555 from port 192.168.2.112. The attack port is the destination– 131.202.243.84. It sends a broadcast on the hour, every hour until 1659, sends a command shell to destination IP.

start	Tag	appName	destination	destinationPayloadAsBase64
2010-06-13 23:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 00:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 01:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 02:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 03:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 04:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 05:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 06:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 07:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 08:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 09:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 10:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 11:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 12:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 13:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 14:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 15:59:17	Attack	Unknown_TCP	131.202.243.84	nan
2010-06-14 16:59:17	Attack	SecureWeb	131.202.243.84	AGoLAE1a6AAAAABbUkVvieWBw8sRAAD/04nDV2gEAAAAUP/QaPC1olZoBQAAAFD/0wAAAAAAAAAAAAA

IP Traffic throughout an Attack



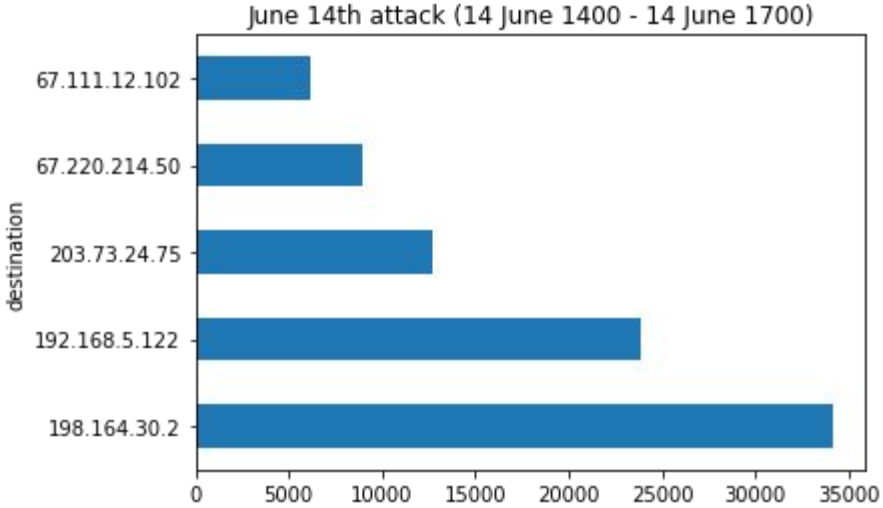




67.220.214.50 6387 (HTTPImageTransfer)	198.164.30.2 8702 (DNS/ICMP)	198.164.30.2 7750 (DNS/ICMP)
198.164.30.2 4758 (DNS/ICMP)	203.73.24.75 5186 (HTTP)	192.168.5.122 4136 (DNS, HTTP)
192.168.5.122 3261 (various: SSH, DNS, HTTP)	192.168.5.122 4768 (DNS, HTTP, ICMP)	203.73.24.75 2317
62.140.213.243 1077 (HTTP)	4.71.173.89 2389 (HTTP)	67.15.184.7 1598
203.73.24.75 969 (HTTP)	208.116.9.82 2033 (HTTP)	208.116.9.82 1503

During the Payload

- 198.164.30.2 3422
- 192.168.5.122 2384
- 203.73.24.75 1267
- 67.220.214.50 899
- 67.111.12.102 614



192.168.5.122

- Previously only saw a few apps: DNS, FTP, HTTP, ICMP, POP, SMTP
- All suspicious activity is from **192.168.2.112**
- Now seeing 79 different app names:
  - **Logging on:** Authentication
  - **Remote access:** Rexec, rlogin, MSTerminal
  - **File sharing:** Oracle, Filenet, BitTorrent,. Hotline
  - **Communications:** SSL-shell, Yahoo, AOL-ICQ

Challenge 1&2: Building a Classifier

Objectives:

1. Binary classification of hostile vs benign traffic

2. Multiclass classification of application type

Approach:

- Multi-output deep neural network

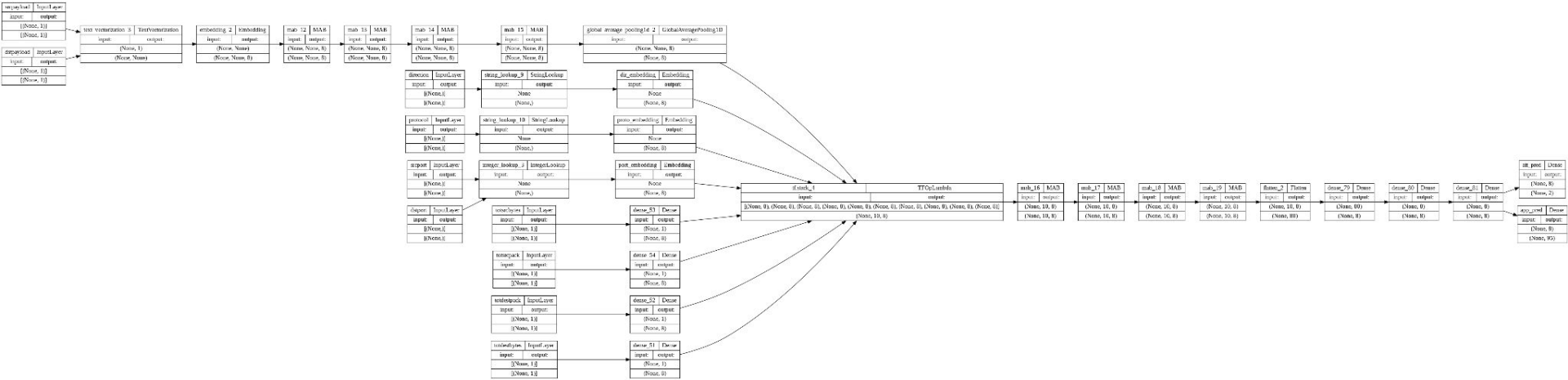
Challenge 1&2: Building a Classifier

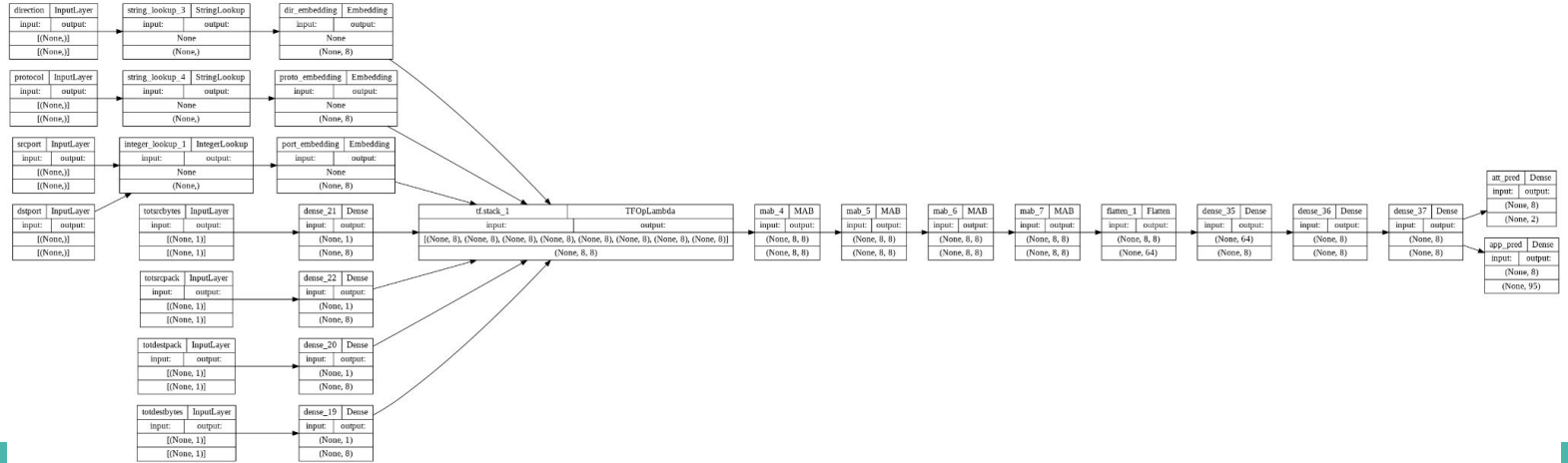
Architecture:

- A modified version of the TabTransformer architecture proposed in Huang et. al. 2020
  - Modification inspired by discussion in the SAINT paper, published by Somepalli et. al. 2021from UMD

- Model encodes and projects categorical and continuous features into a higher dimensional space and then learns new representations based on “context” of correlated values in a connection.

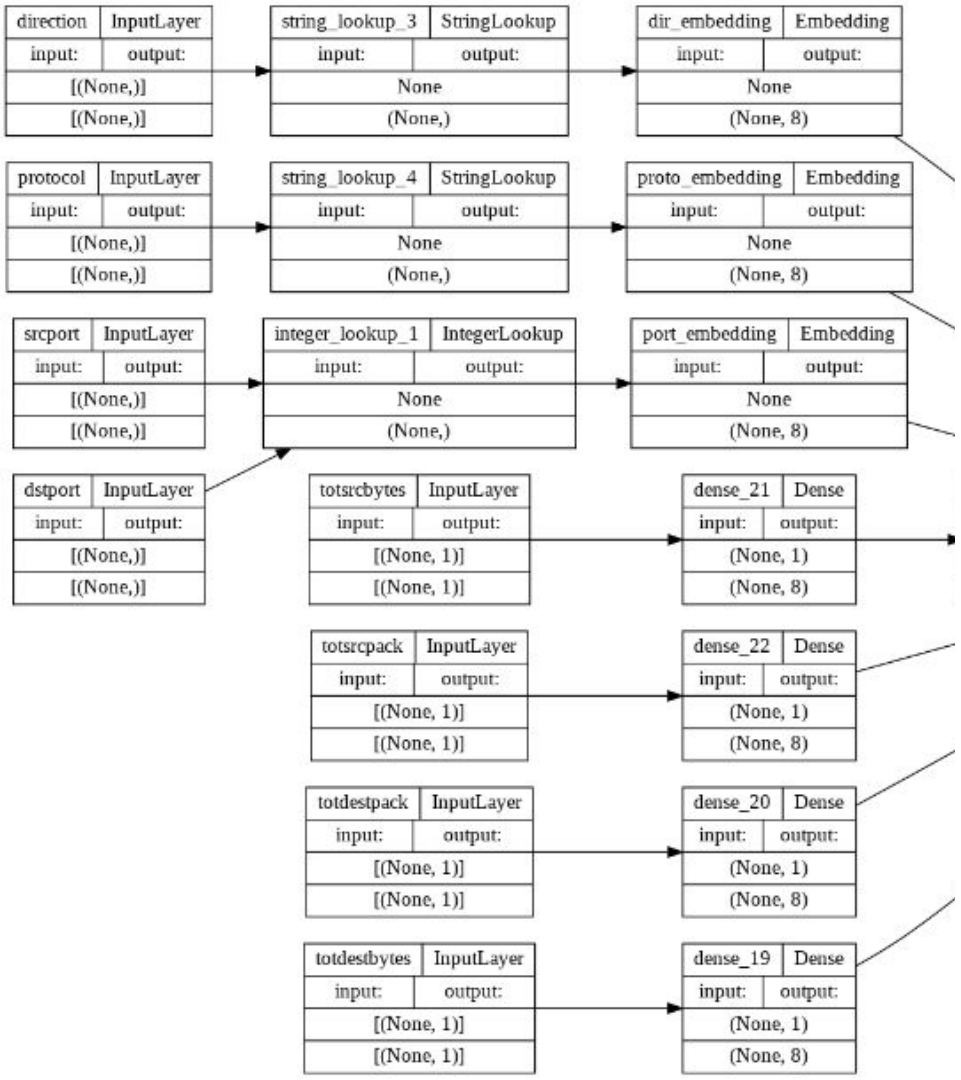
Model Architecture:





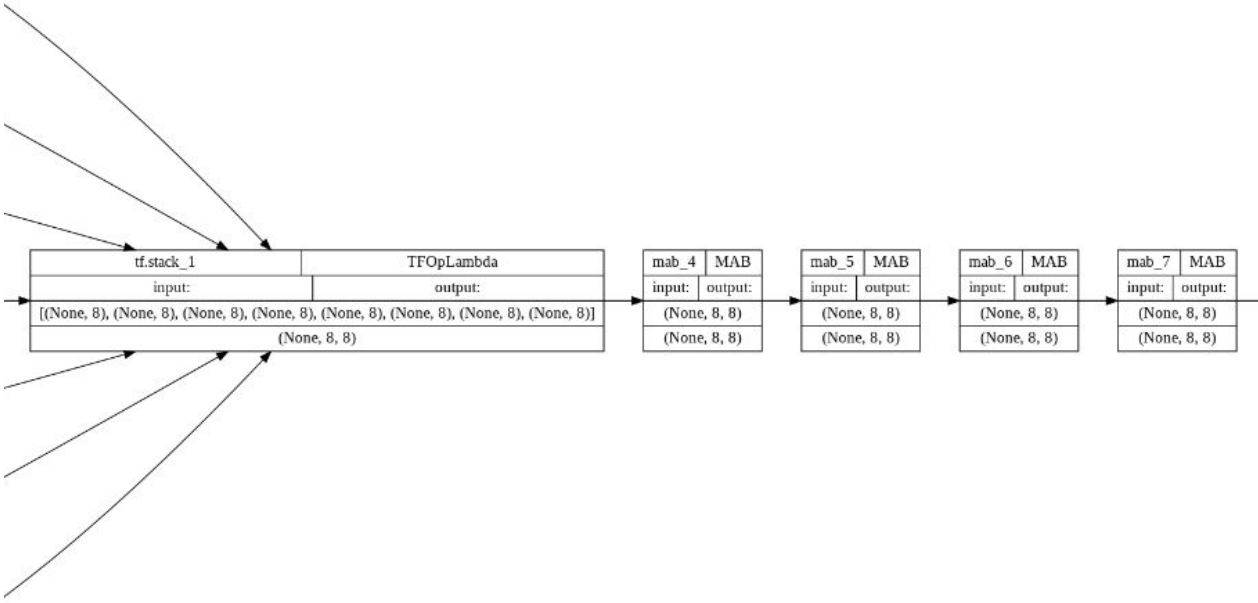
Embedding Layers

- Receive input data
- Project categorical features such as port numbers and continuous features such as total bytes sent into a higher dimensional latent space



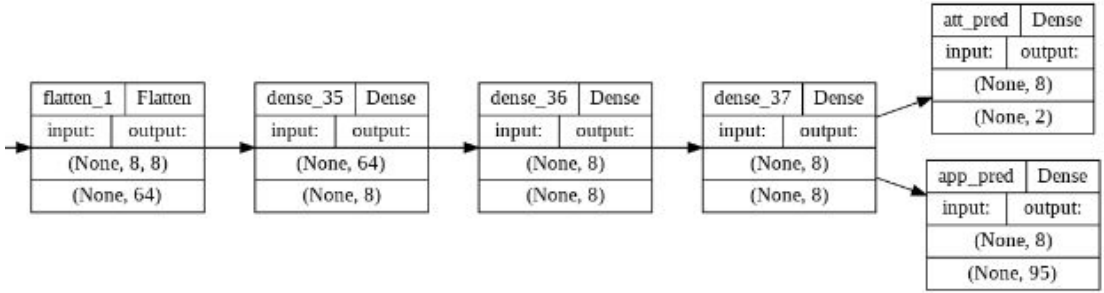
Attention Layers

- Stack projections of each feature together
- Learn linear combinations of these feature vectors to produce meaningful representations



Classification Heads

- Flatten the transformed representations into a single vector
- Pass this vector through a series of dense layers before adding a prediction head for each of the assigned tasks

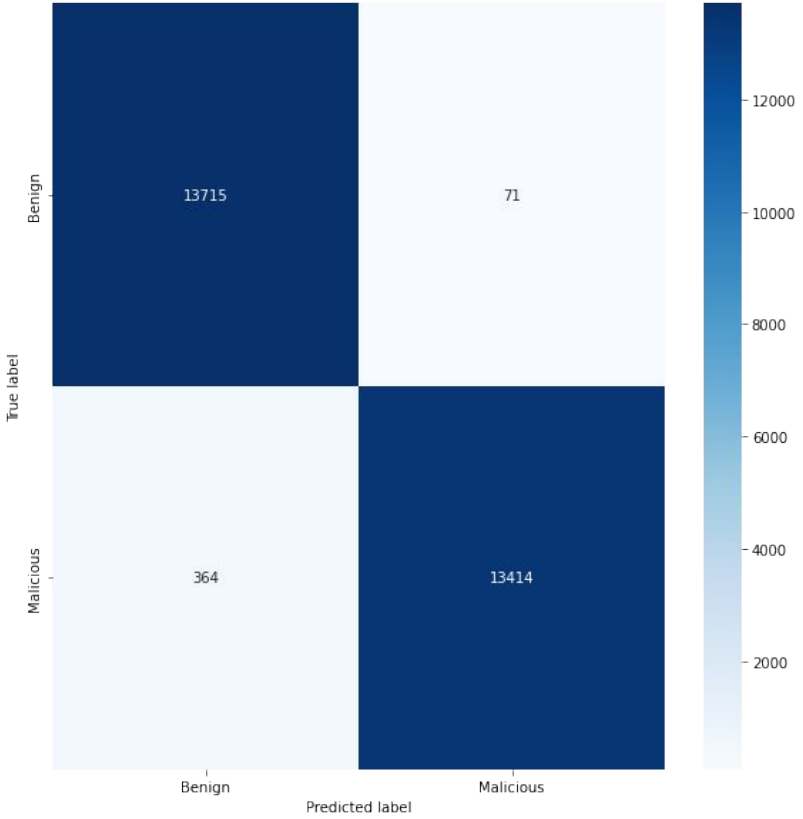


Is the packet payload needed?

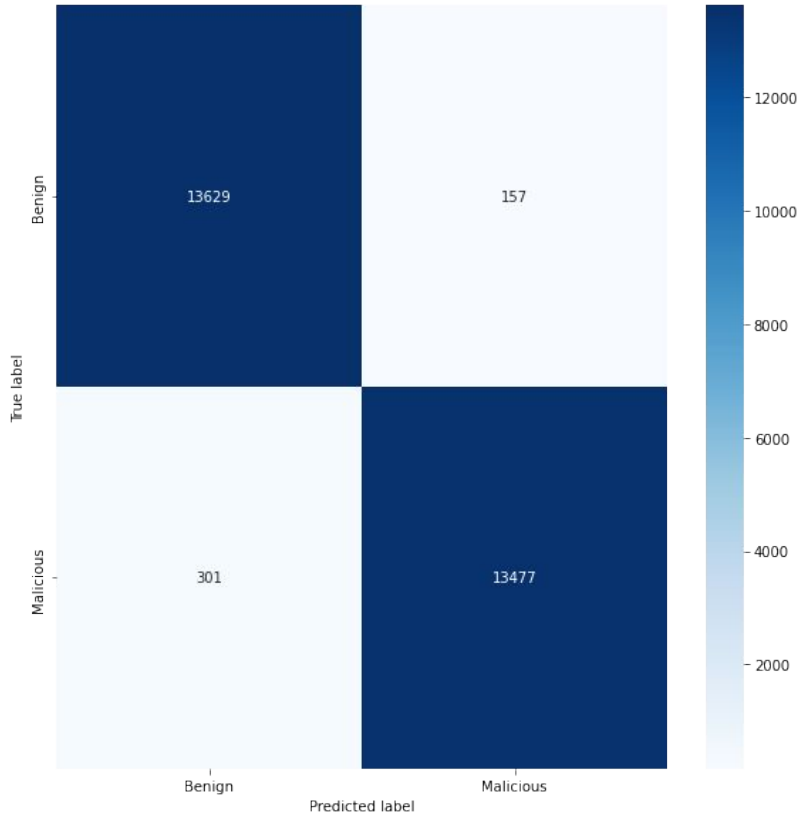
5 epochs each	Train	Validation	Test
With Payload BinAcc (Threat): Top3 (App):	 .9920 .9992	 .9833 .9972	 .9844 .9974
Without Payload (6x faster) BinAcc (Threat): Top3 (App):	 .9895 .9993	 .9830 .9978	 .9833 .9982

Binary Classification Accuracy

With Payload



Without Payload



Data Visualization: Interactive Links

- HeatMaps
  - Benign:https://blackgazzelle.github.io/UMD_INFOCHAL_IC22024/data_visualization_html/benignHeatMap.html
  - Attack:https://blackgazzelle.github.io/UMD_INFOCHAL_IC22024/data_visualization_html/attackHeatMap.html
- Network Traffic Directions
  - Benign: https://blackgazzelle.github.io/UMD_INFOCHAL_IC22024/data_visualization_html/networkTrafficDirections.html
  - Attack:https://blackgazzelle.github.io/UMD_INFOCHAL_IC22024/data_visualization_html/attackDirections.html
- Network Attack Traffic Graphs:
  - Initial Attack: https://blackgazzelle.github.io/UMD_INFOCHAL_IC22024/data_visualization_html/initialAttackNetwork.html
  - Series of Attacks:https://blackgazzelle.github.io/UMD_INFOCHAL_IC22024/data_visualization_html/attackTrafficNetwork.html