Abstract

The BoT-IoT dataset was created by designing a realistic network environment in the Cyber Range Lab of the centre of UNSW Canberra Cyber, as shown in Figure 1. The environment incorporates a combination of normal and botnet traffic. The dataset's source files are provided in different formats, including the original pcap files, the generated argus files and csv files. The files were separated, based on attack category and subcategory, to better assist in labelling process.

The captured pcap files are 69.3 GB in size, with more than 72.000.000 records. The extracted flow traffic, in csv format is 16.7 GB in size. The dataset includes DDoS, DoS, OS and Service Scan, Keylogging and Data exfiltration attacks, with the DDoS and DoS attacks further organized, based on the protocol used.

To ease the handling of the dataset, we extracted 5% of the original dataset via the use of select MySQL queries. The extracted 5%, is comprised of 4 files of approximately 1.07 GB total size, and about 3 million records.

Location

The BoT-IoT dataset can be downloaded from Here:

Link