IT352: Information Assurance and Security

Project Summary

N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders

Group Number 12:
Bhagyashri Bhamare (181IT111)
Utkarsh (181IT250)
Chinmayi C. Ramakrishna (181IT113)

Date: 23rd January, 2021

Abstract:

The growing adoption of Internet-of-Things devices brings with it the increased participation of said devices in botnet attacks, and as such novel methods for IoT botnet attack detection are needed. The paper proposes a network-based anomaly detection method for the IoT called N-BaIoT. This extracts behavior snapshots of the network and uses deep autoencoders to detect anomalous network traffic from compromised IoT devices. The autoencoders have more than one hidden layer. To evaluate their method, the paper has infected nine commercial IoT devices with two widely known IoT-based botnets, Mirai and BASHLITE. The results proved their accuracy of the model.

Methodology:

1. First extract statistical features that capture behavioral snapshots of benign IoT traffic.
2. Train a deep autoencoder (one for each device) to learn the IoT device's normal behaviors.
3. The autoencoders attempt to compress snapshots.
4. When an autoencoder fails to reconstruct a snapshot, it is a strong indication that the observed behavior is anomalous (the IoT device has been compromised and is exhibiting an unknown behavior).

Novelty of the paper:

- This paper as is known so far is the first to apply autoencoders to IoT network traffic for anomaly detection as a complete means of detecting botnet attacks.
- In the paper, evaluation has been done with real traffic data, gathered from nine commercial IoT devices infected by authentic botnets from two families.
- Experimental results have been found on two IoT based botnets, Mirai and BASHLITE.

Benefits:

1. An advantage of using deep autoencoders is their ability to learn complex patterns. This results in an anomaly detector with hardly any false alarms.
2. The model provides heterogeneity tolerance by profiling each device with a separate autoencoder. This addresses the growing heterogeneity of IoT devices.
3. The proposed autoencoders are trained to detect when a behavior is abnormal. Thus, their method can detect previously “unseen” botnet behaviors.
4. The model is Efficient as it uses incremental statistics to perform the feature extraction, and the training of the autoencoders can be performed in a semi online manner (train on a batch of observations and then discard). The training is therefore practical, and there is no storage concern. Additionally, it's a network-based model so it does not consume any computation, memory, or energy resources from the (typically constrained) IoT devices.

Related Work:

Previous IoT-related botnet detection studies focused mainly on the early steps of propagation and communication with the C&C server. [2][4]

Botnet detection approaches are either host-based[4] or network-based[2][3]. We consider host-based techniques less realistic because not all IoT manufacturers can be relied on to install designated host-based anomaly detectors on their products

A hierarchical taxonomy of network-based botnet detection approaches, not limited to the IoT domain, was proposed by Sebastián García, Alejandro Zunino, and Marcelo Campo[5]. One of the detection sources they surveyed was honeypots, which have commonly been used for collecting, understanding, characterizing, and tracking botnets14 but are not necessarily useful for detecting compromised endpoints or the attacks emanating from them. Moreover, honeypots normally require a substantial investment in procurement or emulation of real devices, data inspection, signature extraction, and keeping up with mutations.

Results:

1. Our method succeeded in detecting every single attack launched by every compromised IoT device (True Positive Rate of 100 percent).
2. Our method also raised the fewest false alarms. It demonstrated a mean FPR (False Positive Rate) of 0.007 ± 0.01, lower and more consistent than for SVM (0.026 ± 0.029), IsolationForest (0.027 ± 0.041), and LOF (0.086 ± 0.081).
3. Our method required only 174 ± 212 ms to detect the attacks, and frequently much less t time.

Novelty of our project

1. The paper trains and deploys different models for each IoT device. This can be burdensome in real world scenarios where networks are large. The first step would be to combine datasets for different devices as one dataset. The autoencoder algorithm can be applied on this dataset.
2. Our project will employ a feature selection mechanism. This will allow for assessment of autoencoder method accuracy on smaller feature subsets.
3. Since the project doesn't contain the source code, the complete technical implementation will be done based on the paper with some required fixes.

References:

[1] https://ieeexplore.ieee.org/document/8490192

[2] M. Özçelik, N. Chalabianloo, and G. Gür, “Software-Defined Edge Defense against IoTBased DDoS,” Proc. 2017 IEEE Int’Conf. Computer and Information Technology (CIT 17), 2017; doi.org/10.1109/CIT.2017.61.

[3] H. Bostani and M. Sheikhan, “Hybrid of Anomaly-Based and Specification-Based IDS for Internet of Things Using Unsupervised OPF Based on MapReduce Approach,” Computer Comm., vol. 98, 2017, pp. 52–71.

[4] D.H. Summerville, K.M. Zach, and Y. Chen, “Ultra-Lightweight Deep Packet Anomaly Detection for Internet of Things Devices,” Proc. 2015 IEEE 34th Int’l Performance Computing and Comm. Conf. (IPCCC 15), 2015; doi.org/10.1109/PCCC.2015.7410342.

[5] S. García, A. Zunino, and M. Campo, “Survey on Network-Based Botnet Detection Methods,” Security and Communication Networks, vol. 7, no. 5, 2014, pp. 878–903.