Deep Neural Networks for Sequence based Anomaly Detection in Cyber Security

Ashima Chawla, Dr. Paul Jacob, Dr. Brian Lee, Dr. Sheila Fallon
Department of Electronics & Informatics, Faculty of Engineering & Informatics, Athlone Institute of Technology

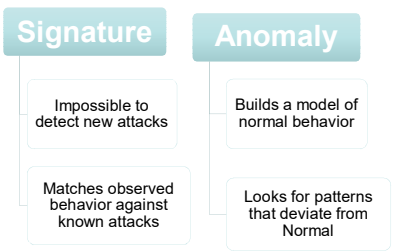
Abstract

Cyber security has become one of the most challenging aspects of modern world digital technology and it has become imperative to minimize and possibly avoid the impact of cybercrimes. Host based intrusion detection systems help to protect systems from various kinds of malicious cyber attacks. One approach is to determine normal behaviour of a system based on sequences of system calls made by processes in the system. The proposed model describes a computationally efficient anomaly based intrusion detection system based on Recurrent Neural Networks. Using Gated Recurrent Units rather than the normal LSTM networks it is possible to obtain a set of comparable results with reduced training times. The incorporation of stacked CNNs with GRUs leads to improved anomaly IDS. Intrusion Detection is based on determining the probability of a particular call sequence occurring from a language model trained on normal call sequences from the ADFA Data set of system call traces. Sequences with a low probability of occurring are classified as an anomaly

Introduction

Intrusion Detection Systems (IDS) are a crucial requirement to safeguard an organization's electronic assets. There are two types of intrusion detection systems commonly known as Host based Intrusion Detection systems (HIDS) and Network based Intrusion Detection systems (NIDS).

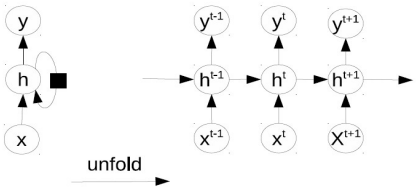
Network based intrusion detection systems are used to monitor and analyse network traffic to protect a system from network-based threats. Host based intrusion detection systems are a network security technology originally built for detecting vulnerability exploits against a target application or computer system.



In this context, Australian Defence Force Academy Linux Dataset(ADFA-LD), a system call dataset consists of 833 normal training sequences,746 attack, 4372 validation sequences and has been used for evaluating a system call based HIDS.

Methodology

A feed-forward neural network has an input layer, a number of hidden layers and an output layer. The output for a node in the network is obtained by applying a weight matrix to the node's inputs and applying an activation function to the result. The network is trained using an algorithm such as backpropagation.

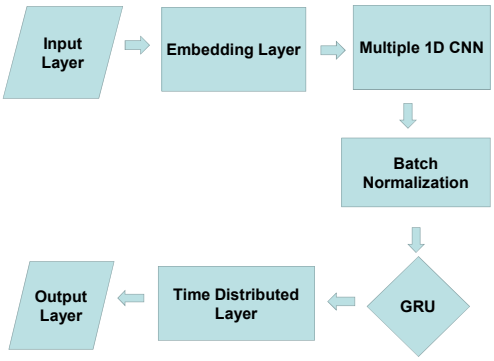


For the purposes of evaluation, Detection Rate (DR) and False Alarm Rates (FAR) were defined as:

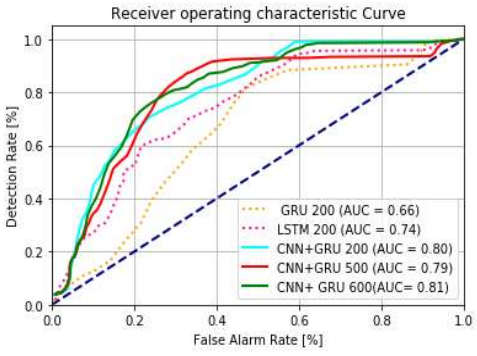
$$DR = TP / (TP + FN)$$

$$FAR = FP / (FP+TN)$$

Model Architecture



Results



Conclusion

The model with CNN+GRU 600 units gave the best value (0.81) for the Area Under the ROC curve (AUC). CNN+GRU 200 and 500 units were only marginally behind resulting in an AUC value of 0.80. The model produces 90% True Detection Rate with a False Alarm Rate of 30%.

The CNN-GRU language model implementation has substantially reduced the training time when compared to an LSTM model. The model was able to achieve better accuracy by stacking multiple CNN layers before the GRU layer. The time taken for stacked CNN/GRU is approximately 10 times faster than LSTM due to faster convergence in training. While the CNN-GRU model converged after 10 training epochs, giving an AUC of 0.80, the LSTM model needed 100 epoch to converge resulting in an AUC of 0.74 with 100 epochs.

Model	RNN Units	Training Time (sec)	Testing Time (sec)	AUC
GRU	200	376	444	0.66
LSTM	200	4444	541	0.74
CNN+GRU	200	390	441	0.80
CNN+GRU	500	402	493	0.79
CNN+GRU	600	423	533	0.81

References

[1] Sepp Hochreiter, Jrgen Schmidhuber: Long short-term memory. Neural Computation 9(8): 1735{1780 (1997)

[2] Gyuwan Kim, Hayoon Yi, Jangho Lee, Yunheung Paek, Sungroh Yoon, LSTM-Based System-Call Language Modelingand Robust Ensemble Method for Designing Host-Based Intrusion Detection Systems, eprint arXiv:1611.01726 (2016)

[3] Miao Xie, Jiankun Hu, Evaluating Host-Based Anomaly Detection Systems: A Preliminary Analysis of ADFA-LD, In: 6th International Congress on Image and Signal Processing (CISP), Hangzhou, China, (2013)

[4] Junyoung Chung, Caglar Gulcehre, KyungHyun Cho, Yoshua Bengio: Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling,arXiv:1412.3555, Presented at the Deep Learning workshop at NIPS (2014)

Acknowledgment

This research has received funding from the European Union Horizon 2020 research and innovation programme under grant agreement No. 700071 for the PROTECTIVE project.