Athlone Institute of Technology
Graduate School

Applying Process Mining to Improve Microservices Cyber Security Situational Awareness

Stephen Jacob
Dr. Brian Lee, Dr. Yuansong Qiao

Motivation

Cyber Security Incident Response Teams (CSIRTs) for enterprise networks are often overwhelmed by newer, more sophisticated forms of cyber attack. Improved cyber security techniques are in high demand. At present, microservices are emerging as the dominant software design architecture for many applications [1]. The main research question for this research project is: “In what ways can business processes mining improve the detection of cyber security attacks in a microservices-based domain?”

Anomaly detection systems generate alerts for suspicious behaviour in software systems and CSIRTs require the means to prioritise these alerts and identify those that pose the greater threat to their microservices-based applications. The mining of business processes is a methodology that extracts knowledge from application log data and outputs the information in the form of process models. Previous research highlights that the discovery of process mining models is a popular topic in the field of cybersecurity, having been used to discover forms of cyber attack strategies in a log of intrusion alerts [2], and uncovering process anomalies in cyber security processes [3].

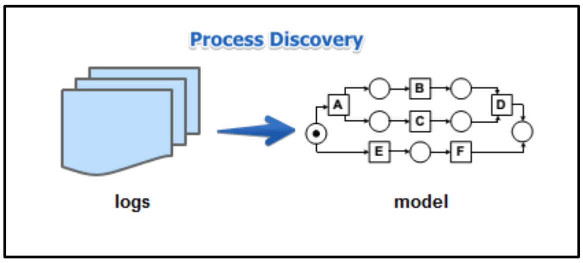

Fig 1. Process Model Discovery for Process Mining

Aims and Objectives

This project aims to provide an accurate oversight of the behaviour of microservices-based applications using process mining. This context awareness allows cyber security personnel to prioritise events and to respond appropriately. The objectives of this project are:

1) Carry out a state of the art review of process mining and deep learning, and their application for cyber security
2) Investigate the use of deep learning applications for anomaly detection in real time process execution paths
3) Carry out a case study using the open source DeathStarBench[4], a bench mark suite of microservices applications
4) Seed cyber attacks against a microservice application and generate the resulting process calls or traces
5) Apply a deep learning model to learn the behaviour of the behaviour and detect anomalous traces
6) Evaluate the anomaly detection model

Process Mining

Conventional process mining extracts knowledge from log data and outputs the information in the form of process models as shown in Fig 1. The logged data consists of **cases** which are sequences of **events**. Another approach to process mining is to train a neural network to learn the typical form of cases and to use this network to make predictions about future events.

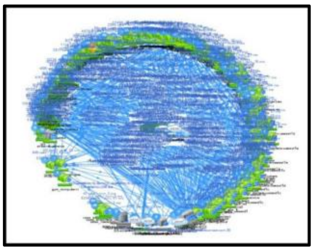

Fig 2. Microservices architecture of Netflix in [5]

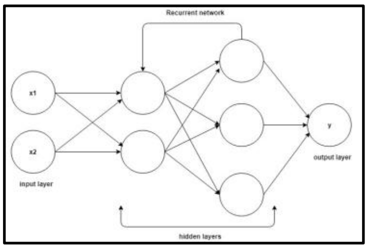

Fig 3. Recurrent Neural Network Layout

Recurrent Neural Networks

A Recurrent Neural Network (RNN) is a Neural Network where the output of layers in the network is fed back into the network on subsequent iterations as shown in Fig 3. This makes RNNs ideally suited for modelling sequences of events. Long Short Term Memory (LSTM) networks are a specific type of RNN designed to carry information over long sequences.

BPIC 2014 Case Study

The application used was a Service Management tool that logged customer calls for software support. The log files for the application were published by Rabobank Group ICT as part of the Business Process Intelligence Challenge in 2014 [6]. The aim was to use the log files to train an RNN to learn the business processes. The neural network model can then be used to predict subsequent events given an initial sequence of events.

The LSTM model created has a single hidden layer with 100 nodes. It was trained with a dataset of 20,000 cases, where a case is a single sequence of events. There were 90 different event types and the longest case contained 178 events. The model application was run on an NVIDIA GPU server with a four card Tesla V100 SXM2, and took 35 minutes to train.

Results

The model was tested with 5000 cases and initial tuning of hyper-parameters for the model has resulted in an accuracy of 49% for predicting future events. This is not low for a multi-classification task with 90 different event classes. A random guess would result in an accuracy of approximately 1%.

References

[1]: Gan, Yu, and Christina Delimitrou. "The Architectural Implications of Cloud Microservices." *IEEE Computer Architecture Letters* 17, no. 2 (2018): 155-158.
[2]: de Alvarenga, Sean Carlisto, Bruno Bogaz Zarpelão, S. Barbon Jr, Rodrigo Sanches Miani, and Michel Cukier. "Discovering attack strategies using process mining." (2015): 119-125.
[3]: Van der Aalst, Wil MP, and Ana Karla A. de Medeiros. "Process mining and security: Detecting anomalous process executions and checking process conformance." *Electronic Notes in Theoretical Computer Science* 121 (2005): 3-21.
[4]: http://microservices.ece.cornell.edu/
[5]: Gan, Yu, et al. "Seer: Leveraging Big Data to Navigate the Complexity of Performance Debugging in Cloud Microservices." In *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems*, pp. 19-33. ACM, 2019.
[6]: https://www.win.tue.nl/bpi/doku.php?id=2014:challenge