Lateral Movement and Telco Fraud Detection

Kaiafas G., Lagraa S., State R., SnT, University of Luxembourg, Hammerschmidt C., TU Delft
georgios.kaiafas@uni.lu, c.a.hammerschmidt@tudelft.nl sofiane.lagraa@uni.lu, radu.state@uni.lu

Lateral Movement Attack

- Advanced Persistent Attack
- Use legitimate credentials
- Escalate privileges
- Traverse network stealthily

Challenges

- Difficult to obtain ‘Normal’ behavior
- Different servers different behaviors
- ‘Normal’ behavior non constant
- Reduce False Alerts
- Imbalanced data

Solution

Ensemble based Semi-supervised Machine Learning

Telco Frauds

- PBX phone calls
- Unauthorized calls to international premium numbers
- POST Luxembourg network

Challenges

- Move beyond classifying phone calls
- Limited fraud knowledge
- Develop Reliable Unsupervised Detection methods

Solution

Unsupervised Outlier Ensemble Detectors

- Isolation Forest
- Kernel Density Estimation Outlier Score
- Local Outlier Probability

Graph based approach for Investigation

Publications:
- Detecting malicious authentication events trustfully (NOMS 2018)
- Graph-based malicious login events investigation (IM 2019)

Publications:
- An Experimental Analysis of Fraud Detection Methods in Enterprise Telecommunication Data using Unsupervised Outlier Ensembles (IM 2019)

This work is supported by the project CONCORDIA that has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 830927.