

Ransomware Anomaly Detection

Students: Ian Agrela De Freites

Mentor: Mike East, Kaseya; Carl Banzhof, RocketCyber

Instructor/Faculty: Dr. Masoud Sadjadi, Florida International University

PROBLEM

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

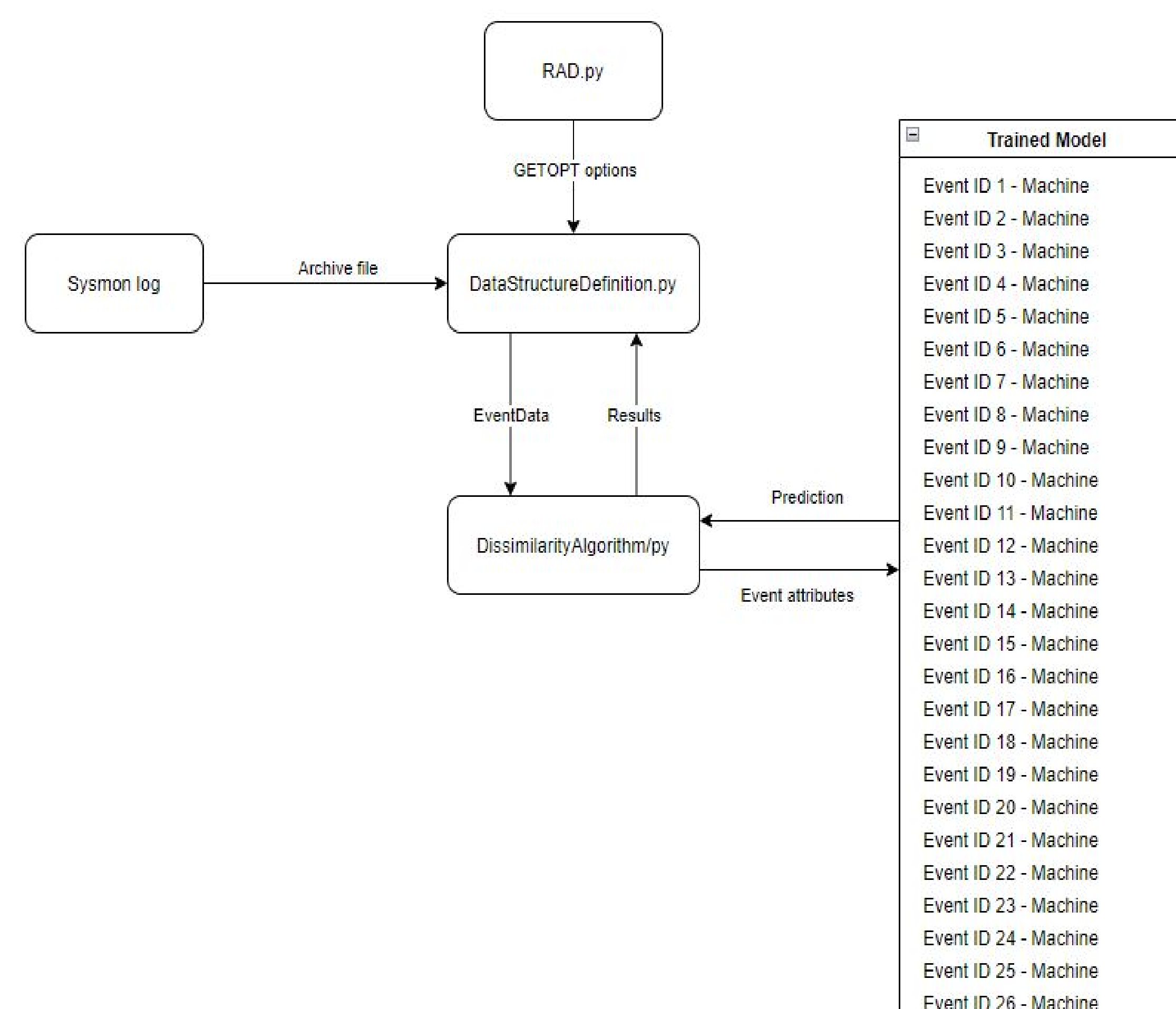
CURRENT SYSTEM

The current system works with a behavior-based detection technique of malware analysis (evaluation of new behaviors in comparison to previous ones), it achieves this by recording event log data and then calculates dissimilarity. It is compatible with machines that use Microsoft operating systems.

IMPLEMENTATION

The learning machine model used is called Dissimilarity Algorithm-String Comparison. The algorithm runs on Windows operating systems and uses Python3, Visual Studio Code, and Windows Sysmon logs tool

SYSTEM DESIGN



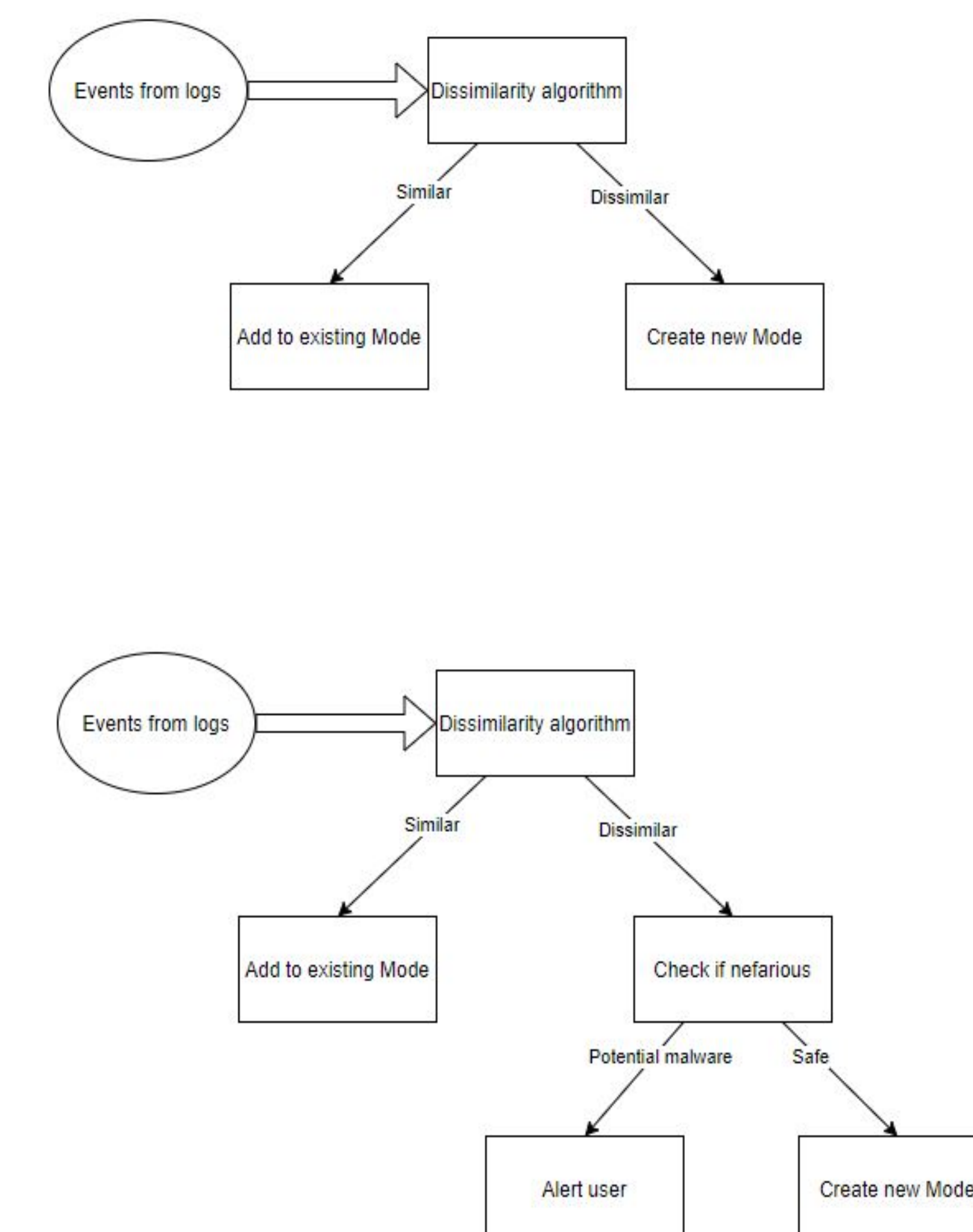
Training:

Events are fed into the application to train the model and create a baseline to be compared against. Events that are considered dissimilar are used to create new Mode to compare against

Prediction:

Happens after the model is trained. Events get compared against the trained model for dissimilarity. Dissimilar events raise flags. If found to be safe then new modes can be made to further perfect the model.

OBJECT DESIGN



VERIFICATION

Application was tested using the Sysmon Simulator application that mimics ransomware events in the Sysmon log files. The training was done with 30 days worth of computer logs. Largest recorded accuracy: 75%

REQUIREMENTS

- Microsoft Windows Sysmon v13.33
- Python3 IDE
- Sysmon Simulator

SUMMARY

Project areas I worked on:

- Machine Learning model.
- Sysmon EventIDs.
- Research on EventIDs' attributes to be tested in algorithm.

REFERENCES

- <https://github.com/ScarredMonk/SysmonSimulator>
- <https://docs.microsoft.com/en-us/sysinternals/downloads/Sysmon>

ACKNOWLEDGEMENT

The material presented in this poster is based upon the work supported by Carl Banzhoff. We/I thank Carl Banzhof and Mike East for their assistance and mentorship that we received throughout the senior design project.