Practial Project AAS 2

Mário Antunes

January 16, 2024

Introduction

This document details the necessary information for the realization of the practical project for the AAS course in the second evaluation phase. As stated at the beginning of the course, the practical project is worth 50% of the final grade. For this project it is allowed to continue the work from the first project with the same group.

The main objective of this work is to develop an application that applies the topics discussed within the course within the privacy and security environment. Each student is encouraged to propose a topic, that may be aligned with another course project, a scholarship, or the Master's Dissertation.

Five different topics are provided that serve as a baseline of what is expected (and may also be selected as the final project):

1. Malware Detection (Passive): Build an application capable of inferring if a specific file is suspicious of being malware or not. The application should only look into the file headers or bytes to extract features.
2. Malware Detection (Active): Build an application capable of inferring if a specific file is suspicious of being malware or not. The application should use a sandbox to execute/open the file and extract features from its execution.
3. Binary visualization: Veles visualizations are purely statistical representations of binary data. This visualization can then be used to "understand" the binary usage.
4. Mail (headers/content) analysis: Extract features from the headers, content, or both and produce an application capable of identifying suspicious (spam or other types of malicious) mails.
5. Real-time intrusion detection: Develop an application capable of monitoring a network and flagging certain flows as malicious.

In Section Resources you will find links to external resources that can be helpful for the realization of this project. In Section Deadline and Repository you can find more details regarding the deadline and the repository for the project.

Deadline and Repository

The project should be delivered through this link: https://classroom.github.com /a/T4AxjIjJ. All of the resources should be accessible through the repository (if there are issues with files larger than 100 Mb, please contact the professor).

The repository should contain:

1. The code for the application;
2. A README.md file with sufficient detail to use the application;
3. A report (10-page maximum of content; in PDF) with the description of the application and solution. The report should contain:
   - Project description and motivation;
   - Data gathering process;
   - ML application on the data and
   - Results and discussion.

The work can be done individually or in pairs. Please use your student number as the project/team name.

The deadline for the project is 25/01/2024 at 11:59 PM.

Resources

Several resources for the realization of the project. It is exptected that the list of resources increases as time progresses.

1. Binary visualization explained
2. Binary visualisation for malware detection
3. Malware analysis method using visualization of binary files
4. JOE Sandbox
5. Deep Malware Analysis - Joe Sandbox ML
6. JOE Sandbox - Analyses Overview
7. Malware Bazaar
8. E-Mail Header Analyzer (MHA)
9. Unveiling Network Threats: Anomaly Detection in Intrusion Detection Systems