Aprendizagem Aplicada à Segurança

Practical Project AAS

Mário Antunes

December 5, 2025

Introduction

This document details the necessary information for the completion of the practical project for the AAS course. As stated at the beginning of the course, the practical project is worth 50% of the final grade.

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

Proposed Topics

Below are **ten** potential topics that serve as a baseline for what is expected. You may select one of these or propose a custom topic:

1. **Malware Detection (Passive):** Build an application capable of inferring if a specific file is malicious. The application should only analyze file headers or raw bytes to extract features without executing the file.
2. **Malware Detection (Active):** Build an application capable of inferring if a specific file is malicious. The application should utilize a sandbox to execute or open the file and extract features based on its runtime behavior.
3. **Binary Visualization:** Use tools like *Veles* or similar techniques to create statistical visualizations of binary data. The goal is to use image classification or visual analysis to determine "understanding" of the binary usage or detect anomalies.
4. **Mail Analysis (Headers/Content):** Extract features from email headers, body content, or both to produce an application capable of identifying suspicious emails (Spam, Phishing, or Malware distribution).

5. **Real-time Intrusion Detection:** Develop an application capable of monitoring network traffic and flagging specific flows as malicious (NIDS).
6. **Phishing URL Detection:** Create a lightweight classifier that detects phishing attempts based solely on the lexical features of a URL (e.g., URL length, entropy, special characters) without downloading the page content.
7. **Domain Generation Algorithm (DGA) Detection:** Develop a model to detect domains generated algorithmically by botnets and command-and-control servers. The system should distinguish between legitimate domain names and random/algorithmic ones.
8. **Web Attack Detection (SQLi/XSS):** Build a classifier to analyze HTTP logs or query strings to detect common web attacks, such as SQL Injection or Cross-Site Scripting (XSS), by analyzing the payload syntax.
9. **Android Malware Analysis:** Analyze Android Application Packages (APKs). Extract features from the `AndroidManifest.xml` (permissions, intents) and bytecode to classify applications as benign or malicious.
10. **Adversarial ML Attack/Defense:** Demonstrate an adversarial attack against a security classifier (e.g., modifying a malware sample slightly so it bypasses detection) and propose a defense mechanism (e.g., adversarial training) to harden the model.

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

Requirements and Deadline

The project must be submitted via the eLearning platform in a single compressed file. All resources should be accessible within the compressed file (scripts can be used to automatically download large files, such as datasets or pre-trained models).

Each project submission must contain:

1. **Source Code:** The complete code for the application.
2. **README.md:** A file with sufficient detail to install dependencies and run/use the application.
3. **Report:** A PDF report (maximum 10 pages of content) describing the problem, the chosen solution/algorithm, and the evaluation results.

Note: Evaluation must go beyond simple accuracy; please include confusion matrices, Precision, Recall, and F1-Scores.

The work can be done individually or in pairs (groups of three are exceptional

and require professor approval).

The deadline for the project is 06/01/2026 at 23:59.

Resources

Below are several resources to assist in the realization of the project. It is expected that this list will grow as the course 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. E-Mail Header SPAM detection example
10. Unveiling Network Threats: Anomaly Detection in Intrusion Detection Systems
11. Dataset (Phishing/Benign)
12. CIC-AndMal2017 (Android Malware Dataset)