Aprendizagem Aplicada à Segurança

Mário Antunes

September 19, 2025

Universidade de Aveiro

Table of Contents i

Class Introduction

Grading

Class Schedule

Environment

Bibliography

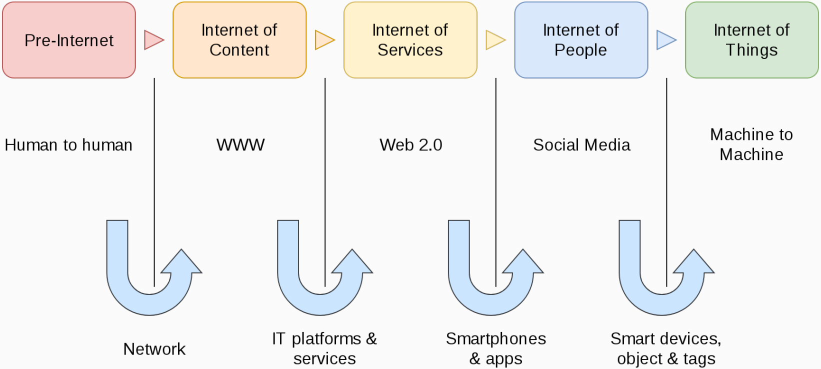
Professor

- **Name:** Mário Antunes
- **E-Mail:** mario.antunes@ua.pt
- **Office:** 19.2.15 (IT1)

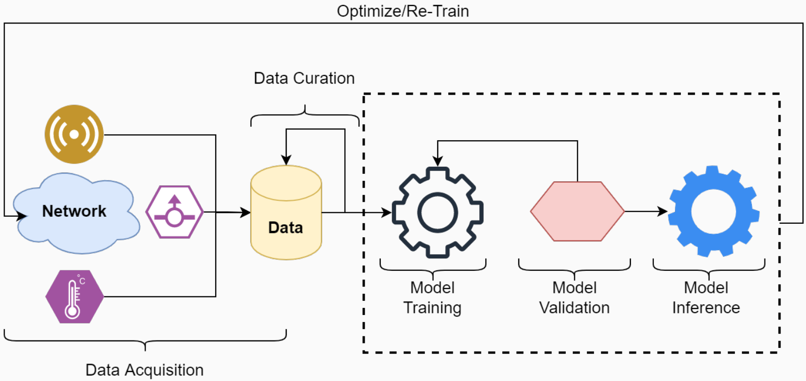
Class Introduction i

- Given the evolution of the threats
- And the complexity of the systems
- AI/ML are gaining traction as a usefull tool

Class Introduction ii



Class Introduction iii



Grading

- 50% Theory + 50% Practice
- Discrete: 25% Mid-term Exam + 25% Final Exam + 50% Project
- Final: 50% Final Exame + 50% Project

Class Schedule

Date	Class	Topic
19-09-2025	1	Class Presentation
26-09-2025	2	SPAM Detector
03-10-2025	3	
10-10-2025	4	
17-10-2025	5	Anomaly Detection
24-10-2025	6	
31-10-2025	7	
07-11-2025	8	Mid-term Exam
15-11-2025	9	Malware Analysis
21-11-2025	10	
28-11-2025	11	
05-12-2025	12	Project
12-12-2025	13	
19-12-2025	14	

Environment

pandas
scikit
learn
matplotlib
seaborn
NumPy
TensorFlow
PyTorch
pymoo
GENSIM
topic modelling for humans
spaCy

Bibliography i

All of the books are available here: https://learning.oreilly.com/

Chio, Clarence, and David Freeman. 2018. *Machine Learning and Security*. O'Reilly.

Halder, Soma, and Sinan Ozdemir. 2018. *Hands-on Machine Learning for Cybersecurity: Safeguard Your System by Making Your Machines Intelligent Using the Python Ecosystem*. Packt Publishing Ltd.

Mueller, John Paul, and Rod Stephens. 2019. *Machine Learning Security Principles*. Packt Publishing Ltd.

Bibliography ii

Parisi, Alessandro. 2019. *Hands-on Artificial Intelligence for Cybersecurity: Implement Smart AI Systems for Preventing Cyber Attacks and Detecting Threats and Network Anomalies*. Packt Publishing Ltd.

Tsukerman, Emmanuel. 2019. *Machine Learning for Cybersecurity Cookbook*. Packt Publishing Ltd.