Aprendizagem Aplicada à Segurança

Mário Antunes

September 22, 2023

University of Aveiro

Table of Contents

Professor

Name: Mário Antunes

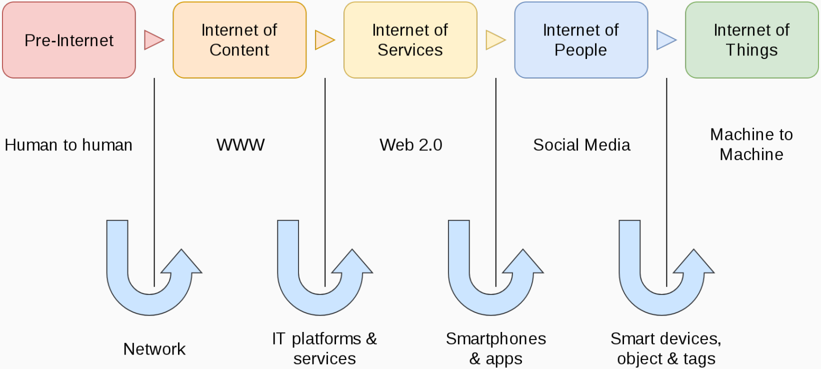
E-Mail: `mario.antunes@ua.pt`

Office: 19.2.15 (IT1)

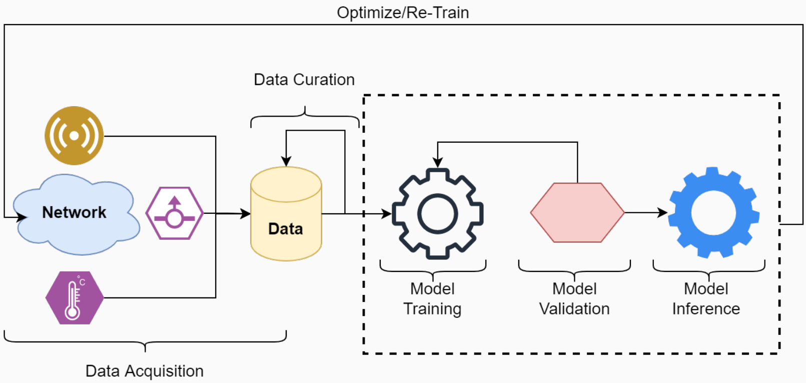
Class Introduction

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

Class Introduction



Class Introduction



Grading i

- 50% Theory + 50% Practice
- Discrete: 25% Mid-term Exam + 25% Final Exam + 20% Project Idea + 30% Project
- Final: 50% Final Exame + 50% Project

Class Schedule i

Date	Class	Topic
15/09/2023	1	Introduction
22/09/2023	2	
29/09/2023	3	SPAM Detector
06/10/2023	4	
13/10/2023	5	
20/10/2023	6	Anomaly Detection
27/10/2023	7	
03/11/2023	8	Mid-term Exam
10/11/2023	9	
17/11/2023	10	Malware Analysis
24/11/2023	11	
01/12/2023	12	Project
08/12/2023	13	
15/12/2023	14	
22/12/2023	15	

Environment i

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/

[1] S. Halder and S. Ozdemir, *Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem*. Packt Publishing Ltd, 2018.

[2] C. Chio and D. Freeman, *Machine Learning and Security*. O'Reilly, 2018.

Bibliography ii

[3] A. Parisi, *Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies*. Packt Publishing Ltd, 2019.

[4] E. Tsukerman, *Machine Learning for Cybersecurity Cookbook*. Packt Publishing Ltd, 2019.

[5] J. P. Mueller and R. Stephens, *Machine Learning Security Principles*. Packt Publishing Ltd, 2019.