ARTIFICIAL INTELLIGENCE ON CYBER SECURITY

Code: 28515

Main Scientific Area: Computer Architecture, Distributed Systems and Cybersecurity

Lecturer: Nuno Alberto Ferreira Lopes

Language of Instruction: Portuguese

Regime: S1

Contact Hours: 30h Total Workload: 138h

ECTS: 6,0

Objectives

The aim of this Curricular Unit is to provide students with the ability to identify artificial intelligence techniques for solving cybersecurity problems.

Learning Outcomes

Students will knowCybersecurity concepts: information security properties, attack, vulnerability and threat concepts, and common attack patterns.

Students will gain skills on theuse of security tools for typical security scenarios, and theapplication of AI Machine Learning techniques for preventing and detecting attacks.

Course Contents

Cybersecurity concepts:

C.I.A. information security properties

Secure (protocol) communications

Attack, vulnerability and threat concepts

Common attack patterns

Security tools:

Intrusion Detection Systems Firewalls

Detection of malware

Detection of spam email

Prevent unauthorised login access

Application of AI Machine Learning techniques for preventing and detecting attacks:

Clustering

Classification

Regression

Specific datasets for cybersecurity

Recommended Bibliography

Emmanuel Tsukerman, Machine Learning for Cybersecurity Cookbook, 2019, Packt (ISBN: 978-178-961-467-1)

Alessandro Parisi, Hands-On Artificial Intelligence for Cybersecurity, 2019, Packt (ISBN: 978-178-980-402-7)

Learning and Teaching Methods

The syllabus addresses on the one hand the theoretical concepts and some practical cases of cybersecurity, on the other hand the application of artificial intelligence techniques. These two approaches enable students to relate the interaction between them and thus fulfil the objectives of the UC.

Assessment Methods

Practical Assignment (individual), covering the complete programme (70%).

The practical assignment will have to be presented.

Written scientific paper (30%).

Evaluation outside the continuous evaluation period will have a penalty of 5 values for the practical assignment.