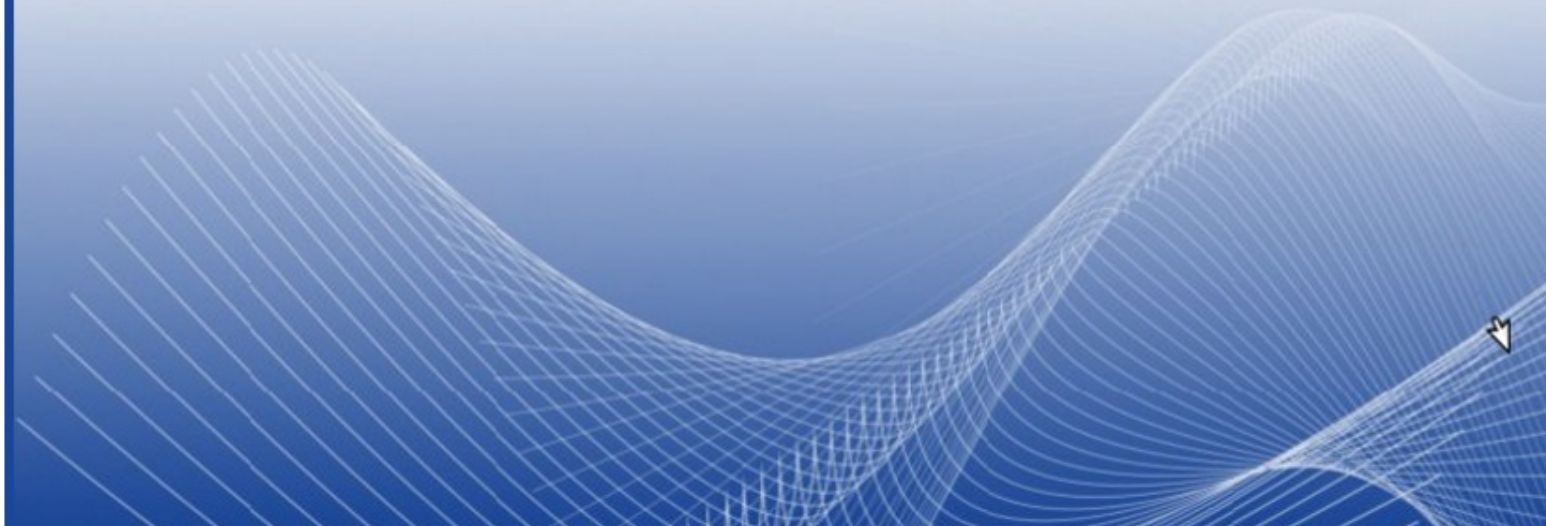
Course Contents and Rules

Aprendizagem Aplicada à Segurança

Mestrado em Cibersegurança
DETI-UA



universidade de aveiro
deti.ua.pt

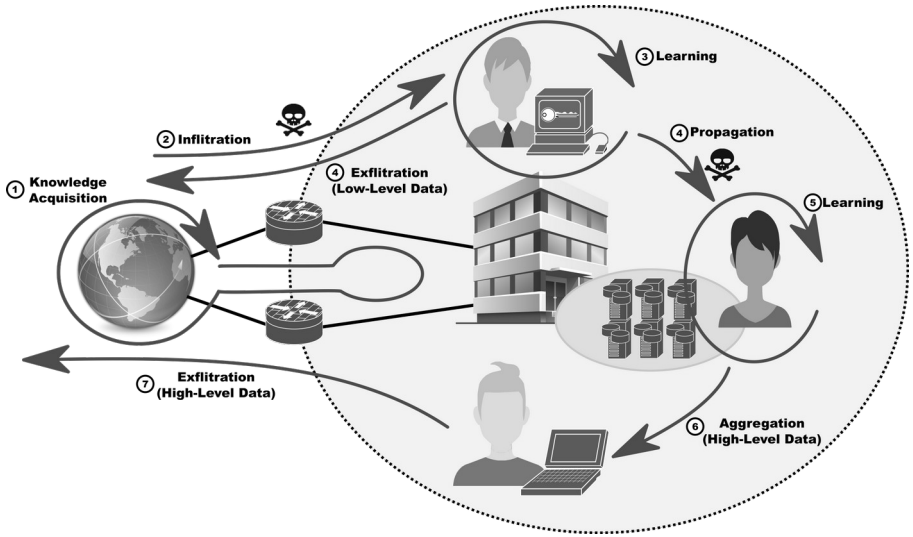
Professor

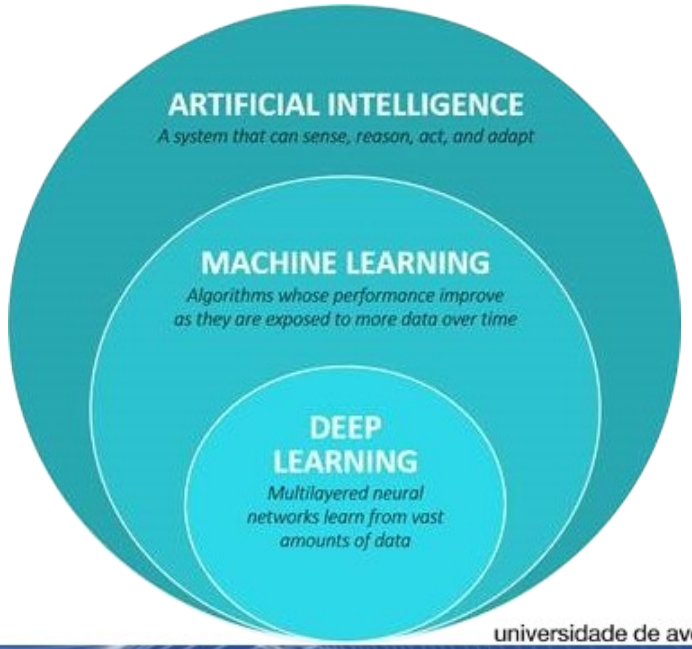
- Prof. Paulo Salvador
  - Email: salvador@ua.pt
  - Web: https://paulosalvador.net
  - Discord: https://discord.gg/bPPpKy5
    - Change your nickname to **your real name** and ask for AAS role.
  - Office: IEETA
- Prof.a Pétia Georgieva
  - Email: petia@ua.pt
  - Gabinete: IEETA

- Office hours
  - Flexible!
  - E-mail to schedule.

Course Objectives

- Learn fundamental machine learning concepts relevant for computer security.
- Learn how to apply machine learning techniques for anomaly detection in computational systems and communication networks.





Contents

- Machine Learning (ML)
  - Basic ML concepts and applications in the field of computer/informatics security,
  - Clustering and classification ML tasks.
  - Supervised and unsupervised ML.
  - Neural networks, deep learning.
- Perception of the behavior of network entities.
  - Perception as a basic technique for detecting evidence of attacks / intrusions.
  - Perception based on users, computer systems or networks.
  - Perception based on signatures or behaviors.
  - Detection of data/objects manipulation.
- Detection of behavioral anomalies using learning.
  - Classification and detection of network traffic anomalies.
  - Classification and detection of anomalous events in computer systems.

Evaluation

- Final Grade =
  - 50% * Theoretical Grade + 50% * Practice Grade
- Minimal grade: 7.0 in each component.
  - Theoretical Grade
    - Exam (100%) - Exam and/or Repeat Exam Seasons
      - Best grade is the one considered to calculate final grade.
  - Practice Grade
    - Project (100%) - in groups of 2 students (or 1 exceptionally).
      - First Presentation (40%) - December 10th
        - » Problem identification.
        - » Proposal of solution.
        - » Only presentation with slides, no report!
      - Final Presentation (60%) - last class.
        - » Presentation of results and demonstration of working solution.
      - During presentations/demo students must answer to specific questions. Grades may be different within a group.
    - Repeat Exam Season
      - The project can be improved (or fully redone).
      - Best grade is the one considered to calculate final grade.

Classes Planning (tentative)

	Class	Friday		Professor	Obs.
1	15-Oct	Introduction. Network and systems attack vectors. IDS/IPS. Forensics.		PS/PG	
2	22-Oct	Network and systems monitoring, data acquisition and data pre-processing.	TP: Data Acquisition	PS	
3	29-Oct		TP: Data Acquisition	PS	
4	05-Nov	Features Extraction	TP: Data Processing and Features Extraction	PS	
5	12-Nov		TP: Data Processing and Features Extraction	PS	
6	19-Nov		TP: Data Processing and Features Extraction	PS	
7	26-Nov	Univariate/Multivariate Gaussian Distribution	TP: Anomaly detection	PG	
8	03-Dec	Univariate/Multivariate Linear regression. Overfitting, regularization.	TP: Regression	PG	
9	10-Dec	Artificial Neural Networks (ANN) Support Vector Machines (SVM)	TP: Classification	PG	Proj.: Problem idea and Planning
10	17-Dec	K-means clustering - Data dimensionality reduction - PCA (Principal components analysis)	TP:Clustering	PG	
	24-Dec	Férias Natal			
	31-Dec	Férias Natal			
11	07-Jan	Introduction to DL. Convolutional Neural Networks (CNN)	TP: Deep Learning	PG	
12	14-Jan	Project		PS	
13	21-Jan	Project		PS/PG	Proj.: Results and Demo

Bibliography

- Course slides.
- Chio, C., & Freeman, D. (2018). Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly Media, Inc.. ISBN 978-1491979907
- Maloof, M. A. (Ed.). (2006). Machine learning and data mining for computer security: methods and applications. Springer Science & Business Media. ISBN 978-1846280290
- Santos, O. (2015). Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security. Cisco Press. ISBN 978-1587144387
- Collins, M., & Collins, M. S. (2014). Network security through data analysis: building situational awareness. O'Reilly Media, Inc.. ISBN 978-1587144387
- Gardner, B., & Thomas, V. (2014). Building an information security awareness program: Defending against social engineering and technical threats. Elsevier. ISBN 978-0124199675
- Bhaiji, Y. (2008). Network security technologies and solutions (CCIE professional development series). Pearson Education. ISBN 978-1587052460