Module MCS 016
Machine Learning for Cyber-Security & Artififial Intelligence

Prof. Hermes Senger

Hermes Senger

email: hermes@ufscar.br
senger.hermes@gmail.com

Associate Professor
Federal University of São Carlos UFSCar Brazil

PhD Electrical Engineering, 2002

Interests:

- High Performance Computing
- Parallel and Distributed Computing
- Machine Learning Applications

Topics

- Overview: IA, Machine Learning, BigData, Data Science, Applications
- Fundamental concepts
- Decision Trees
- Bayesian networks
- Neural Networks
- Data streams – stream mining
- Data mining and machine learning for cyber-security
- Tools
- Hybrid learning

Software requirements

- For hands on and practice, students are recommended to install Weka
  - On Mac OS:

    ```
    brew install --cask weka
    ```

  - Linux and Windows:

    https://waikato.github.io/weka-wiki/downloading_weka/
- Video tutorial on how to install and explore Weka

  https://www.youtube.com/user/WekaMOOC

  Watch vídeos 1.2, 1.3, 1.4, 1.5, and 1.6

Lab Materials

- Datasets for exercises (~ 595 MB):

```
git clone https://github.com/HPCSys-Lab/ML-cybersec-students-material.git
```

Bibliography

- I. Witten, E. Frank, M.A. Hall, Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann, 2017.
- Tom M. Mitchell, Machine Learning, MacGraw-Hill, 1997.
- Technical papers published in scientific journals, conference proceedings, and technical literature.