Hubert MĄKA, 3rd year
AGH University of Krakow
Faculty of IEiT
Telephoners Research Club

ARTIFICIAL INTELLIGENCE MODEL RECOGNIZING POTENTIAL PHISHING BASED ON HYPERLINK SYNTAX ANALYSIS

The aim of the project is to create and train an artificial intelligence model using supervised learning, the purpose of which will be to analyze a hyperlink in order to detect whether it is a potential attack vector related to an attempt to persuade the victim to trust a fake entity and to go to crafted resources (e.g., a website) created to obtain sensitive data of the attacked entity. The prepared model will solve a binary classification problem based on a given input that is a hyperlink in the form of a caption.

Publicly available labeled datasets that contain hyperlinks in text form and information about them will be used to train the model. The data will be analyzed and processed accordingly before being sent to the algorithm created earlier.

To implement the model in Python language will be used:

- TensorFlow, Scikit-learn (Machine Learning) libraries.
- Pandas, Numpy, Matplotlib libraries (Data analysis and visualization)

Various neural network architectures and machine learning algorithms will be tested to solve the problem. Using the Pandas, Matplotlib and Numpy libraries, the data will be properly prepared and cleaned for use in teaching models. The potential models will then be implemented with TensorFlow (neural network) and Scikit-learn (classical classification algorithms). In addition, the Matplotlib library will enable graphical visualization of the results obtained and the process of learning the models. As the final product, which will consist of a model (function) taking a hyperlink as input and returning as output the probability of whether a link is potentially dangerous, the model with the best result obtained during testing will be selected.*O*

Scientific supervisor of the paper:

Dr hab. inż. Marek Natkaniec