Ben-Gurion University of the Negev
Faculty of Engineering
Department of Software and Information Systems Engineering
Methods for Detecting Cyber Attack, No. 372-2-5203, spring semester 2017
Instructor: Dr. Asaf Shabtai, CISSP shabtaia@bgu.ac.il

Course Objectives

The usage of machine learning techniques in the security domain is increasing in recent years. The aim of the course is to understand how machine learning can be applied in the security domain and be used for detecting cyber-attacks.

The course introduces different machine learning methods and their application in security problems such as intrusion and malware detection, data leakage and data misuse detection, authentication, protecting privacy in social networks, alert correlation, forensics, and fraud detection.

The course covers various challenges in applying machine learning methods in the security domain including: measuring, collecting and processing data, big data problem (applying complex analysis on massive amounts of data or data coming at high rates), concept drift, defining the evaluation process, imbalanced datasets, multiclass problems, vulnerability of machine learning to attacks and more.

The course presents various techniques for approaching these challenges such as ensemble algorithms, active learning and co-training, feature selection, over/under sampling, incremental learning, clustering, anomaly detection and more.

These topics will be examined through readings, discussions, and through a mini-project assignment. The course consists of 3 hours lectures per week that cover the above mentioned issues.

Course Assignments

- A presentation on selected topic (10%)
- Practical / theoretical exercise (10%)
- Mini project (practical) assignment (35%)
- Final exam (Moed A only) – must pass the exam (45%)

All assignments are mandatory.

Tentative Lectures Program

Lecture No.	Topic(s)
1	Introduction – using machine learning in cyber security
2	Introduction to machine learning
3-4	Intrusion detection using misuse detection and anomaly detection
5	Malware detection using machine learning
6-7	Data leakage detection using machine learning
8	Applying machine learning for forensics
9	Privacy in social networks
10	Data processing – data collection, data representation, feature selection
11-12	Challenges in applying machine learning in cyber security (concept drift, multi-class, imbalance, data dimensionality)
13	The security of machine learning (adversarial learning)

Bibliography

1. Dua S. and Du X. *Data Mining and Machine Learning in Cyber Security*, CRC Press, 2011
2. Maloof M.A. *Machine Learning and Data Mining for Computer Security*, Springer, 2006
3. Thomas Mitchell (1997), Machine Learning, McGraw-Hill.

Selected papers for reading will be provided during class