Course Title	Machine Learning for Cybersecurity				
Course Code	CYS632				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	1st or 2nd Year / 2nd or 3rd Semester				
Teacher's Name	TBA				
ECTS	8	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	The course deals with the combination of machine learning and computer security. Approaches for automatically detecting and analyzing security threats are discussed. Topics include anomaly detection, automatic signature generation, classification and clustering of malicious software.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • assess the effectiveness of solutions presented and to question them in an intelligent way; • Understand and implement the most popular learning algorithms; • Perform feature selection and experimental set up on real tasks; • Evaluate multiple learning algorithms across several tasks.				
Prerequisites	None	Co-requisites	None		
Course Content	The massive increase in the rate of novel cyberattacks has made Machine-Learning (ML) techniques a critical component in detecting security threats. The course covers various applications of ML in computer and network security. Topics include: Overview of basic machine learning techniques: supervised and unsupervised learning followed by an overview of the state of information security; malware detection; network and host intrusion detection; web, email, and social network security; authentication and authorization anomaly detection; alert correlation; and potential issues such as privacy issues and adversarial machine learning.				

	• Introduction to Machine Learning: High level analysis of the different approaches to supervised and unsupervised learning. • Supervised Machine Learning: Linear Regression, Logistic Regression, Decision Trees, SVM Vectors. • Unsupervised Machine Learning: Clustering, the k-means algorithm • Density Estimation: Problem Motivation, Gausian Distribution, and the Algorithm • Building an anomaly detection system: Building and Evaluating, Anomaly detection vs Supervised learning. Choosing what features to use. • Introduction to Data Mining for Information Security • Malware Detection: Obfuscation, Polymorphism, Payloadbased detection of worms, Botnet detection/takedown • Network Intrusion Detection: Signature-based solutions (Snort, etc), Data-mining-based solutions (supervised and unsupervised), Deep packet inspection • Host Intrusion Detection: Analysis of shell command sequences, system call sequences, and audit trails, Masquerader/Impersonator/Insider threat detection • Web Security: Anomaly detection of web-based attacks using web server logs, Anomaly detection in web proxy logs • Email: Spam detection, Phishing detection • Social network security: Detecting compromised accounts, detecting social network spam • Authentication: Anomaly detection of Single SignOn (Kerberos, Active Directory), Detecting Pass-the-Hash and Pass-the-Ticket attacks • Automated correlation: Attack trees, Building attack scenarios from individual alerts • Machine learning exploited by both sides: Adversarial machine learning (use of machine learning by attackers, how to make ML algorithms robust/secure against adversaries). • Other potential topics: Fraud detection, IoT/Infrastructure security, Mobile/Wireless security
Teaching Methodology	Face – to – face
Bibliography	Applications of Data Mining in Computer Security, Daniel Barbara and Sushil Jajodia

	Machine Learning and Data Mining for Computer Security, Marcus A. Maloof Data Mining and Machine Learning in Cybersecurity by Sumeet Dua (Editor), Xian Du
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English