SECURING THE FUTURES: CYBERSECURITY FOR DIGITAL ENTERPRISES

Grado en Computación e Inteligencia Artificial / Bachelor in Computer Science and Artificial Intelligence BCSAI SEP-2025
STF-CSAI.4.M.A

Area Computer Science
Number of sessions: 30
Academic year: 25-26
Degree course: FOURTH
Number of credits: 6.0
Semester: 1º
Category: OPTIONAL
Language: English

Professor: **LUIS ANGEL GALINDO SANCHEZ**
E-mail: lgalindo@faculty.ie.edu

Summary

- PhD Telecommunication Engineer (2012). Polytechnic University of Madrid. ANECA accredited.
- Executive MBA (2006). IESE Business School – University of Navarra
- Master, Service and Security in IP Networks (2005). Polytechnic University of Madrid
- Specialist, Network and Advanced Internet Systems (1998). Carlos III University of Madrid
- Specialist, Voice Codification (1997). Carlos III University of Madrid
- ADSS, Advanced Databases, Cybersecurity, IE Impact/Technology, Technology Scouting and Cybercrime
- Visiting Associate Professor at HEC Montreal (from 2018 till now), where I teach Enterpreneurship with my own methodology to assess the business potential of a value proposal.
- Professor in the Master of Cybercrime Master at Nebrija University (from 2018 till now). Teaching police officers how to use Big Data and Machine Learning Technologies to be more efficient working with deep and dark web.
- Researcher in GRICCI group of UDIMA, responsible of the AI area applied to the detection of cybercriminals.
- Associate Professor at Carlos III University of Madrid (from 2007 till now). Professor of Computer networks

Defined, developed and implemented a successful open innovation model, generating new relevant revenue streams results. Selective results include an increase of +200 startups working under this model with +6000 companies analyzed. Increase in revenue of +10% y-o-y leveraged on the innovative assets.

He has defined, developed and implemented a successful Digital Transformation Learning Program for more than 8 years and +2000 people trained, receiving Telefonica Excellent Teacher award along 7 consecutive years.

Principal Investigator in 7 EU funded projects (previously in 4 more) based on the technological skills that Luis has in fields like Cybersecurity, Cyber Defense, AI, Cloud Computing or IoT. He personally researches in the application of AI to the cybersecurity and cybercrime.

Teacher in several recognised universities and business schools with excellent marks from 2007.

Luis, as High Performance Senior Consultant, has implemented +20 consultancy complex projects worldwide for large enterprises in AI, economical intelligence, cybersecurity, business development, digital transformation, risk assessment, process optimization and people management issues.

Luis is an expert at understanding customers and translating their needs into actual sales by developing new markets or new products & services and Digital mindset within everyone in the organization.

He has had a leading role in complex M&A processes with digital assess acquisition like in the first world integration of a MVNO and a social network.

Frequent speaker at Innovation and Tech international conferences. He considers himself a creovator.

Office Hours

Office hours will be on request. Please contact at:

lgalindo@faculty.ie.edu

Email me in advance, if you wish to schedule a chat or a meeting.

PREREQUISITES

A basic understanding of computer systems, networks, and programming concepts is recommended but not mandatory.

A passion for learning, curiosity, and a commitment to ethical behavior in the cybersecurity domain are essential.

Critical and Lateral thinking.

Motivation to learn about Cybersecurity and how cyber attackers think.

SUBJECT DESCRIPTION

The "Securing the Futures: cybersecurity for Digital Enterprises" course is designed to provide participants with a comprehensive understanding of the principles, practices, and techniques necessary to safeguard sensitive information, protect networks, and explore the ethical aspects of hacking.

This course combines theoretical knowledge with hands-on practical exercises to equip participants with essential skills in data protection, cybersecurity, and ethical hacking.

This course explores the different aspects of the security of an organization connected to the Internet and all the threats it faces.

We will analyze the new technologies on which the Internet is based in order to glimpse the inherent technological risks.

The course explores the different types of existing attacks so that the students can have a taxonomy where to reference them.

We will review the principles of cryptography to understand that the mathematical basis of this science is in constant evolution.

Students will experiment with the hidden Internet, because additionally to the 'visible Internet', there is a Deep and a Dark web where very lucrative businesses move and where cybercrime moves like fish in water.

We will also see how companies and governments are using cyber-intelligence and counter-intelligence units to safeguard secrets, protect critical infrastructure or carry out attacks on national security.

LEARNING OBJECTIVES

Upon completing this course, students will be able to:

- Understand Data Protection Principles: Learn the fundamental concepts of data protection, including data classification, privacy laws, and regulations. Gain insights into data governance, risk assessment, and mitigation strategies to ensure compliance and protect personal and organizational data.
- Explore Cybersecurity Fundamentals: Delve into the world of cybersecurity and explore various threats, attack vectors, and vulnerabilities that organizations face. Understand the importance of defense-in-depth strategies, security frameworks, and risk management practices to safeguard networks, systems, and data.
- Understand the functioning of encryption techniques without being a mathematician.
- Ethical Hacking Foundations: Gain an ethical hacker's perspective and develop a deep understanding of hacking techniques, methodologies, and tools. Learn how to identify vulnerabilities, perform penetration testing, and assess the security posture of networks and applications.
- Network Security: Acquire knowledge about network security principles, protocols, and defense mechanisms. Explore topics such as firewalls, intrusion detection systems (IDS), virtual private networks (VPNs), and secure network design principles to protect network infrastructure from unauthorized access.
- Web Application Security: Dive into the world of web application security and understand common vulnerabilities, such as SQL injection, etc. Learn how to identify and mitigate these vulnerabilities to ensure secure web application development and usage.
- Have a strategic vision of the steps to be taken to protect an organization.
- Understand that organized crime is based on cybercrime, changing the way many criminal clans operate, where results can be optimized in the face of risk. Learn how criminals act to make business in critical sectors like health care and connected industry

TEACHING METHODOLOGY

IE University teaching method is defined by its collaborative, active, and applied nature. Students actively participate in the whole process to build their knowledge and sharpen their skills. Professor's main role is to lead and guide students to achieve the learning objectives of the course. This is done by engaging in a diverse range of teaching techniques and different types of learning activities such as the following:

Learning Activity	Weighting	Estimated time a student should dedicate to prepare for and participate in
Lectures	26.7 %	40.0 hours
Discussions	13.3 %	20.0 hours
Exercises in class, Asynchronous sessions, Field Work	20.0 %	30.0 hours
Group work	20.0 %	30.0 hours
Individual studying	20.0 %	30.0 hours
TOTAL	100.0 %	150.0 hours

AI POLICY

Generative artificial intelligence (GenAI) tools may be used in this course for research, ideation, generating an outline, proofreading, grammar check, coding, image generation with appropriate acknowledgement. GenAI may not be used for exams. If a student is found to have used AI-generated content inappropriately, it will be considered academic misconduct, and the student might fail the respective assignment or the course.

If you are in doubt as to whether you are using GenAI tools appropriately in this course, I encourage you to discuss your situation with me.

In case you use GenAI for assignments, what is expected is to provide critical thinking and creativity on top of the results of the tool.

Below, a suggested format to acknowledge the use of generative AI tools. Please note that acknowledging AI will not impact your grade.

I acknowledge the use of [AI systems link] to [specify how you used generative AI]. The prompts used include [list of prompts]. The output of these prompts was used to [explain how you used the outputs in your work]

If AI was permitted to use in your assignment, but you have chosen not to include any AI generated content, the following disclosure is recommended:

No content generated by AI technologies has been used in this assignment.

PROGRAM

SESSION 1 (LIVE IN-PERSON)

WELCOME AND INTRODUCTION TO CYBERSECURITY

Introduction to the course: logistics, evaluation system, and content at-a-glance.

With the Internet era, organizations are attacked daily from any point of the world. Cybersecurity is a huge concern for companies. Data breaches cost businesses an average of $4.35 million in 2022.

SESSION 2 (LIVE IN-PERSON)

CYBERSECURITY CONCEPTS

We will review the cybersecurity concepts to have a common dictionary which allows us a right interaction. We will establish the basis for a common understanding during the course.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 3 (LIVE IN-PERSON)

DATA PROTECTION

In this session, we will provide an overview of data protection principles, the importance of protecting personal data, and the legal and regulatory frameworks governing data protection (e.g., GDPR, CCPA), covering topics such as data subject rights, lawful bases for processing, data breach notification requirements, and international data transfers.

DATA CLASSIFICATION

In this session, we will cover how to classify data based on its sensitivity and value to the organization. Discuss the importance of maintaining a data inventory to track the types of data being processed, the purposes of processing, and data retention periods. Emphasize the principle of collecting and processing only the minimum amount of personal data necessary for a specific purpose. Discuss the importance of clearly defining and documenting the purposes of processing.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 4 (LIVE IN-PERSON)

CRYPTOGRAPHY I

In this session, we will introduce the concept of cryptography, the basic concepts related to this science and we will explain who symmetric encryption works.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 5 (LIVE IN-PERSON)

CRYPTOGRAPHY II

In this session, we will introduce Asymmetric Encryption techniques covering PKI, Message Autentication and Hash Functions.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 6 (LIVE IN-PERSON)

A VIEW TO THE HISTORY OF CODING. INDIVIDUAL ASSIGNMENT

Each student will analyze individually one of the chapters of "The code book" assigned by the professor, and in this session, individual works will be presented.

20% of your grade

Book Chapters: The code book : the science of secrecy from ancient Egypt to quantum cryptography (See Bibliography)

SESSION 7 (LIVE IN-PERSON)

CLASS EXERCISE. DECRYPTING INFORMATION

This class exercise will consist of decrypting a piece of information coded by using Crypto tool

SESSION 8 (LIVE IN-PERSON)

THREATS I

Many of the techniques for attacking systems share common characteristics. We will explore a categorization to define patterns which could suggest where protections needed to be tightened.

In these two sessions, we will explore APTs, social engineering, Malware, DoS...

SESSION 9 (LIVE IN-PERSON)

THREATS II

Many of the techniques for attacking systems share common characteristics. We will explore a categorization to define patterns which could suggest where protections needed to be tightened.

In these two sessions, we will explore APTs, social engineering, Malware, DoS...

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the Threat sessions.

SESSION 10 (LIVE IN-PERSON)

TEAM PRESENTATION 1

In this session, groups will present the work done in the definition of a realistic scenario combining several technologies with the goal of training under a realistic situation

10% of your grade

SESSION 11 (LIVE IN-PERSON)

TRANSVERSAL CHALLENGES I

Cybersecurity is a highly multifaceted and often subjective discipline, and the absence of universally accepted definitions of used terms along with the lack of a shared vision on what are the scourges of the current landscape makes the need of a technically focused approach for the identification, analysis and categorisation of the most pressing current and emerging challenges. We will explore transversal challenges applicable to the different technologies used in our society and in our extended society.

SESSION 12 (LIVE IN-PERSON)

TRANSVERSAL CHALLENGES II

Cybersecurity is a highly multifaceted and often subjective discipline, and the absence of universally accepted definitions of used terms along with the lack of a shared vision on what are the scourges of the current landscape makes the need of a technically focused approach for the identification, analysis and categorisation of the most pressing current and emerging challenges. We will explore transversal challenges applicable to the different technologies used in our society and in our extended society.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the Transversal Challeges sessions.

SESSION 13 (LIVE IN-PERSON)

THREATS AND WEAKNESSES IN CRITICAL SECTORS. INDUSTRY 4.0

Connected Industry 4.0 is a coinned term to explain how new technologies like 5G, IoT, AI... can increase the productivity of the industrial sector. This connected industry open doors to be attacked by cybercriminals sitting in any part of the world connected to Internet.

We will explore threats and weaknesses in the CI 4.0 domain.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 14 (LIVE IN-PERSON)

THREATS AND WEAKNESSES IN CRITICAL SECTORS. HEALTH CARE

Healthcare has evolved dramatically in the last few years due to the introduction of new technologies connected to Internet. IoT implanted devices provides a good opportunity to make easier the patients' life while create opportunities for cyberterrorists to kill someone without any risk.

In this session, we will also explore threats and weaknesses in the Healthcare domain.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 15 (LIVE IN-PERSON)

TEAM PRESENTATION 2

In this session, groups will present the work done creating a storytelling of attack one of the realistic scenario defined in Presentation 1 by one of the groups.

Professor will define which group will act as attacker to define the strorytelling.

10% of your grade

SESSION 16 (LIVE IN-PERSON)

PROTECTING THE ORGANIZATION. FIREWALLS

In this session we will explore what a Firewall is and the functionalities provided to protect an organization.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 17 (LIVE IN-PERSON)

PROTECTING THE ORGANIZATION. IDS AND SIEM

In this session we will explore advance elements like IDS, IPS and SIEM usually deployed in organizations to protect them.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 18 (LIVE IN-PERSON)

CLASS EXERCISE ON COUNTERMEASURES.

This class exercise will consist on assigning countermeasures in a corporate network of a Industry 4.0.

SESSION 19 (LIVE IN-PERSON)

SECURITY OF DATA TRANSMISSION (TLS/SSL)

From the beginning of human history to date, the communication of sensitive messages between a sender and a receiver has been an object of study in the attempt to protect the message

information during its transit. In this session we will explore the main features of TLS and SSL.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 20 (LIVE IN-PERSON)

CLASS EXERCISE. TLS TRACES

This class exercise in groups will be focused in understanding how we can get some traces in the initial steps of using TLS.

SESSION 21 (LIVE IN-PERSON)

SECURITY OF DATA TRANSMISSION (IPSec)

From the beginning of human history to date, the communication of sensitive messages between a sender and a receiver has been an object of study in the attempt to protect the message

information during its transit. In this session we will explore the main features of IPSec.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 22 (LIVE IN-PERSON)

TEAM PRESENTATION 3

In this session, groups responsible of each scenario created in Team Presentation 1 will present the work done in the identification and deployment of countermeasures to mitigate the storytelling defined by other group in Team Presentation 2.

10% of your grade

SESSION 23 (LIVE IN-PERSON)

CLASS EXERCISE. NMAP

This class exercise in groups will be focused in understanding how NMAP works.

SESSION 24 (LIVE IN-PERSON)

CYBER THREAT INTELLIGENCE

Cyber Threat Intelligence (CTI) is information about threats and attackers to mitigate harmful events. In this session, we will explore OSINT sources, Forensic Audit, Indicators of Compromise, Pyramid of Fear, etc to show the complexity to provide resiliance to an organization against cyber security attacks.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 25 (LIVE IN-PERSON)

BROWSING THE DEEP/DARK WEB

We will browse the Deep/Dark web to show how it is and what it can be found.

SESSION 26 (LIVE IN-PERSON)

ETHICAL HACKING AND COUNTERINTELLIGENCE

Ethical hacking involves various methodologies and techniques, including network scanning, vulnerability assessment, penetration testing, social engineering, and more.

In the last few years, we are seeing foreign intelligence services, non-state actors and criminals using intelligence collection techniques against companies to steal valuable trade secrets and assets. Companies have to protect in advance against these vulnerabilities that could cause a terrible situation for them.

In this session, we will explore ethical hacking and counterintelligence.

IN-CLASS QUIZ

In the last 5 minutes of the class, we will run a quiz related to the concepts explained during the session.

SESSION 27 (LIVE IN-PERSON)

CLASS EXERCISES. ZAPPING

This class exercise in groups will be focused in understanding how OWASP ZAP works.

SESSION 28 (LIVE IN-PERSON)

MANAGEMENT AND ADMINISTRATION OF CYBERSECURITY

In this session, we will talk about Risk Analysis and Information Systems Security Management and the rules applicable to manage cybersecurity: ISO/IEC 27000 family

IN-CLASS EXERCISE

In the second part of the session, groups will start working in a Risk Management exercise identifying risks in a situation provided

SESSION 29 (LIVE IN-PERSON)

RECAP SESSION

Groups will present the recap of the sessions covered in the course

Presentations will be graded in the Participation issue

SESSION 30 (LIVE IN-PERSON)

FINAL EXAM

15% of your grade

EVALUATION CRITERIA

Class Participation (20%)

This includes class exercises, voluntary participation on the whiteboard, discussion board (forum) activity, class attendance, and active participation in in-class discussions, with the goal of ensuring a continued learning process, good teamworking, and ability to apply class concepts in real-world problems. Participation is based on the quality, rather on the quantity, of your contributions.

Workgroups/Group presentations (30%)

Throughout the course, 3 group assignments will be given that are to be completed in groups.

Individual presentations (20%)

Throughout the course, 1 individual assignment will be given to be completed individually.

In-class quizzes (15%)

Students will have to individually solve the scheduled in-class quizzes after most of the sessions. Simple questions based on what was explained during the session.

Final Exam (15%)

The final exam will include all the material explained in the course, and will be held during the last session.

Minimal Marks:

The overall passing course grade is 5.0.

All the presentations/videos/exams/codes will be submitted via Campus Online. No other option will be accepted.

criteria	percentage	Learning Objectives	Comments
Intermediate Tests	15 %		
Individual Presentation	20 %		
Group Presentation	30 %		
Class Participation	20 %		
Final Exam	15 %		

RE-SIT / RE-TAKE POLICY

Each student has four chances to pass any given course distributed over two consecutive academic years: ordinary call exams and extraordinary call exams (re-sits) in June/July.

Students who do not comply with the 80% attendance rule during the semester will fail both calls for this Academic Year (ordinary and extraordinary) and have to re-take the course (i.e., re-enroll) in the next Academic Year.

Evaluation criteria:

- Students failing the course in the ordinary call (during the semester) will have to re-sit the exam in June / July (except those not complying with the attendance rule, who will not have that opportunity and must directly re-enroll in the course on the next Academic Year).
- The extraordinary call exams in June / July (re-sits) require your physical presence at the campus you are enrolled in (Segovia or Madrid). There is no possibility to change the date, location or format of any exam, under any circumstances. Dates and location of the June / July re-sit exams will be posted in advance. Please take this into consideration when planning your summer.
- The June / July re-sit exam will consist of a comprehensive exam. Your final grade for the course will depend on the performance in this exam only; continuous evaluation over the semester will not be taken into consideration. Students will have to achieve the minimum passing grade of 5 and can obtain a maximum grade of 8.0 (out of 10.0) – i.e., “notable” in the in the re-sit exam.
- Retakers: Students who failed the subject on a previous Academic Year and are now re-enrolled as re-takers in a course will be needed to check the syllabus of the assigned professor, as well as contact the professor individually, regarding the specific evaluation criteria for them as retakers in the course during that semester (ordinary call of that Academic Year). The maximum grade that may be obtained in the retake exam (3rd call) is 10.0.

After ordinary and extraordinary call exams are graded by the professor, you will have a possibility to attend a review session for that exam and course grade. Please be available to attend the session in order to clarify any concerns you might have regarding your exam. Your professor will inform you about the time and place of the review session. Any grade appeals require that the student attended the review session prior to appealing.

Students failing more than 18 ECTS credits after the June-July re-sits will be asked to leave the Program. Please, make sure to prepare yourself well for the exams in order to pass your failed subjects.

In case you decide to skip the opportunity to re-sit for an exam during the June / July extraordinary call, you will need to enroll in that course again for the next Academic Year as a re-taker and pay the corresponding extra cost. As you know, students have a total of four allowed calls to pass a given subject or course, in order to remain in the program.

BIBLIOGRAPHY

Compulsory

- Simon Singh. *The code book : the science of secrecy from ancient Egypt to quantum cryptography.* Anchor books. ISBN 9780307787842 (Digital)

Recommended

- William Stallings. *Cryptography and Network Security. Principles and Practices.* ISBN 1280736298 (Digital)

- William R Cheswick, Steven M Bellovin, Aviel D Rubin. *Firewalls and Internet security : repelling the wily hacker.* Addison-Wesley. ISBN 020163466XB01 (Digital)

BEHAVIOR RULES

Please, check the University's Code of Conduct here. The Program Director may provide further indications.

ATTENDANCE POLICY

Please, check the University's Attendance Policy here. The Program Director may provide further indications.

ETHICAL POLICY

Please, check the University's Ethics Code here. The Program Director may provide further indications.