GENERAL INFORMATION

Course information	
Name	Cybersecurity
Code	DIM-MIC-523
Degree	Máster Universitario en Ingeniería Industrial + Máster en Industria Conectada [2nd year]
Semester	2nd (Spring)
ECTS credits	3.0
Type	Compulsory
Department	Telematics and Computer Science
Coordinator	Javier Jarauta Sánchez

Instructor	
Name	Javier Jarauta Sánchez
Department	Telematics and Computer Science
Office	
e-mail	jarauta@comillas.edu
Phone	
Office hours	Arrange an appointment through email.

DETAILED INFORMATION

Contextualization of the course

Contribution to the professional profile of the degree

The purpose of this course is to provide students with an overview of Cybersecurity, and specifically, Cybersecurity applied to Industrial Systems, the so-called Operation Technology (OT). The main methodologies, standards, legislation, threats, and vulnerabilities will be studied. Further emphasis will be placed on technologies that help to prevent, detect, and respond to cybersecurity incidents.

Prerequisites

General knowledge of Industrial Control Systems (ICS), including PLC and SCADA, is desirable, although not strictly required.

CONTENTS

Contents
Theory
Unit 1. Introduction to cybersecurity
1.1 Definitions and basic cybersecurity concepts 1.2 History of cybersecurity in IT environments 1.3 Real industrial cases (OT) 1.4 Special considerations of industrial cybersecurity 1.5 Current trends in cyberattacks
Unit 2. Cybercrime
2.1 Cybercrime organization 2.2 Main attack vectors 2.3 Classification of cyberthreats and cybercrimes 2.4 Agencies for the fight against cybercrime 2.5 SOC/CERT/CSIRT concept and major agencies
Unit 3. Industrial cybersecurity lifecycle
3.1 Special considerations of industrial systems 3.2 End-to-end cybersecurity 3.3 Cybersecurity by design 3.4 Cybersecurity in depth (multi-layered) 3.5 The four Ps of cybersecurity: people, products, processes, and property
Unit 4. Cybersecurity framework
4.1 Good practices and standards in cybersecurity 4.2 COBIT, ISO, ISA and NIST CSF models 4.3 NIST CSF cybersecurity framework 4.4 Identification, prevention, detection, response, and recovery functions 4.5 Categories and implementation models 4.6 Industrial cybersecurity management system – Sistema de gestión de la ciberseguridad industrial (SGCI)
Unit 5. Cybersecurity architecture in industrial systems
5.1 Defense in Depth (DiD) concept 5.2 The Purdue model 5.3 Industrial security standards. ISA 62443 5.4 OT cybersecurity technologies 5.5 Implementation of the model and mitigation measures
Unit 6. Critical infrastructures and essential services
6.1 Law and regulation of critical infrastructures 6.2 Sectors concerned 6.3 Planes de Seguridad del Operador (PSO) y Planes de Protección Específicos (PPE) 6.4 The European directive on security of network and information systems (NIS) 6.5 Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)
Unit 7. Mitigation measures
7.1 Asset management and risk analysis 7.2 Physical and remote access to industrial systems 7.3 Communications and network security 7.4 Device security 7.5 Software protection

Unit 8. Fundamentals of cryptography and electronic signature

8.1 Electronic signature as a tool for digital transformation
8.2 Fundamentals of symmetric and asymmetric cryptography and hash functions
8.3 Digital certificates and electronic signature
8.4 Understanding HTTPS (SSL/TLS)
8.5 Virtual Private Networks (VPN)

Master classes

MC1. Risk analysis

Multiple existing risk analysis methodologies will be identified, specifically those most applicable to industrial systems. An example of risk analysis will be carried out on a real case.

MC2. Ethical hacking

Ethical hacking tests will be conducted following the "Cyber Kill Chain" framework. Basic knowledge of existing ethical hacking tools will be provided. Special emphasis will be put on the fundamentals for industrial and IIoT systems.

Laboratory

There will be several laboratory sessiones aimed at acquiring basic ethical hacking fundamentals:

1. Perimeter discovery and device vulnerabilities.
2. Remote access attack simulation.
3. Man-in-the-middle Wi-Fi attack simulation.

Competences and learning outcomes

Competences[1]

General competences

CG1. Have acquired advanced knowledge and demonstrated, in a research and technological or highly specialized context, a detailed and well-founded understanding of the theoretical and practical aspects, as well as of the work methodology in one or more fields of study.

Haber adquirido conocimientos avanzados y demostrado, en un contexto de investigación científica y tecnológica o altamente especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en uno o más campos de estudio.

CG2. Know how to apply and integrate their knowledge, understanding, scientific rationale, and problem-solving skills to new and imprecisely defined environments, including highly specialized multidisciplinary research and professional contexts.

Saber aplicar e integrar sus conocimientos, la comprensión de estos, su fundamentación científica y sus capacidades de resolución de problemas en entornos nuevos y definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar tanto investigadores como profesionales altamente especializados.

CG5. Be able to transmit in a clear and unambiguous manner, to specialist and non-specialist audiences, results from scientific and technological research or state-of-the-art innovation, as well as the most relevant foundations that support them.

Saber transmitir de un modo claro y sin ambigüedades, a un público especializado o no, resultados procedentes de la investigación científica y tecnológica o del ámbito de la innovación más avanzada, así como los fundamentos más relevantes sobre los que se sustentan.

CG6. Have developed sufficient autonomy to participate in research projects and scientific or technological collaborations within their thematic area, in interdisciplinary contexts and, where appropriate, with a high knowledge transfer component.

Haber desarrollado la autonomía suficiente para participar en proyectos de investigación y colaboraciones científicas o tecnológicas dentro de su ámbito temático, en contextos interdisciplinares y, en su caso, con una alta componente de transferencia del conocimiento.

CG7. Being able to take responsibility for their own professional development and their specialization in one or more fields of study.

Ser capaces de asumir la responsabilidad de su propio desarrollo profesional y de su especialización en uno o más campos de estudio.

Specific competences

CE9. Have an insight into the security risks associated with the digitalization of industrial processes, as well as into good practices, techniques, and technologies for the prevention of attacks and mitigation of their effects.

Tener una visión general de los riesgos de seguridad asociados a la digitalización de los procesos industriales, así como las buenas prácticas, técnicas y tecnologías para la prevención de ataques y mitigación de sus efectos.

[1] Competences in English are a free translation of the official Spanish version.

Learning outcomes
By the end of the course students will:
RA1. Understand the concepts, vocabulary, and architecture of cybersecurity, both in the general context of Information and Communication Technologies (ICT), and specifically in industrial systems.
RA2. Know the methodologies and technologies for the definition, prevention, detection, response, and recovery from cyber-attacks that apply to industrial systems.
RA3. Know the national and international regulations and legislation that applies to the protection of critical infrastructures and essential services
RA4. Be able to establish minimum safety requirements in industrial systems, demand them from manufacturers, and implement them from design to production.
RA5. Be familiar with the state-of-the-art in cybersecurity and the upcoming technology trends.

TEACHING METHODOLOGY

General methodological aspects	
Sessions will combine a theoretical presentation of the main aspects of the topic in question, with real illustrative examples of cyberattacks and cyber defense services to prevent, detect and respond to them. Active participation and the discussion of the issues presented will be encouraged.	
In-class activities	**Competences**
▪ **Lectures:** The lecturer will develop the curriculum through the projection of slides, videos, documents and the use of the blackboard. Once the theoretical concepts have been developed, practical and real examples of the instructor's day-to-day work will be presented, along with recommendations and solutions to the problems identified.	CG1, CG7, CE9
▪ **Master classes:** Industry experts will provide a deeper look into trending topics such as risk analysis and hacking.	CG2, CE9
▪ **Lab sessions:** Under the instructor's supervision, students will apply the tools and methodologies studied in the lectures. Students will later analyze and report lab results.	CG1, CG2, CG5, CG6, CG7, CE9
▪ **Tutoring** for groups or individual students will be organized upon request.	–
Out-of-class activities	**Competences**
▪ Personal study of the course material and resolution of the proposed exercises.	CG1, CG7, CE9
▪ Lab session preparation.	CG1
▪ Lab results analysis and report writing.	CG2, CG5, CE9
▪ Thematic presentation. Students will prepare and expose a summary of a cybersecurity topic that will be assigned from a list of the main cybersecurity methodologies, technologies, and services used in Cybersecurity for OT.	CG1, CG2, CG5, CG6, CG7, CE9

ASSESSMENT AND GRADING CRITERIA

Assessment activities	Grading criteria	Weight
Final exam	▪ Understanding of industrial cybersecurity concepts. ▪ Basic references about Spanish legislation for critical infrastructure protection.	40%
Thematic presentation	▪ Problem analysis. ▪ Attitude, effort, initiative, and proactivity. ▪ Teamwork. ▪ Oral and written communication skills.	50%
Participation and lab reports	▪ Proactivity. ▪ Oral and written communication skills. ▪ Application of theoretical concepts to real problem-solving. ▪ Ability to use and develop cybersecurity software.	10%

GRADING AND COURSE RULES

Grading

Regular assessment

- Final exam: 40%
- Thematic presentation: 50%
- Participation and lab reports: 10%

In order to pass the course, both the mark of the final exam and the weighted average mark must be greater or equal to 5 out of 10 points.

Retake

All marks except of that of the final exam will be preserved. Students will write a retake exam worth 40%.
As in the regular assessment period, in order to pass the course, both the mark of the retake exam and the weighted average mark must be greater or equal to 5 out of 10 points.

Course rules

- Class attendance is mandatory according to Article 93 of the General Regulations (Reglamento General) of Comillas Pontifical University and Article 6 of the Academic Rules (Normas Académicas) of the ICAI School of Engineering. Not complying with this requirement may have the following consequences:
  - Students who fail to attend more than 15% of the lectures may be denied the right to take the final exam during the regular assessment period.
  - Regarding laboratory, absence to more than 15% of the sessions can result in losing the right to take the final exam of the regular assessment period and the retake. Missed sessions must be made up for credit.
- Students who commit an irregularity in any graded activity will receive a mark of zero in the activity and disciplinary procedure will follow (cf. Article 168 of the General Regulations (Reglamento General) of Comillas Pontifical University).

WORK PLAN AND SCHEDULE

In and out-of-class activities	Date/Periodicity	Deadline
Final exam	After the lecture period	–
Lab sessions	Towards the end of the course	–
Review and self-study of the concepts covered in the lectures	After each lesson	–
Lab preparation	Before every lab session	–
Lab report writing	–	One week after the end of each session
Thematic presentations	–	Last week

<table>
<tr><th colspan="6">STUDENT WORK-TIME SUMMARY</th></tr>
<tr><th colspan="6">IN-CLASS HOURS</th></tr>
<tr><th colspan="2">Lectures</th><th colspan="2">Master classes</th><th colspan="2">Lab sessions</th></tr>
<tr><td colspan="2">20</td><td colspan="2">4</td><td colspan="2">6</td></tr>
<tr><th colspan="6">OUT-OF-CLASS HOURS</th></tr>
<tr><th colspan="3">Self-study</th><th colspan="3">Lab preparation and report writing</th></tr>
<tr><td colspan="3">40</td><td colspan="3">20</td></tr>
<tr><th colspan="5">ECTS credits:</th><th>3 (90 hours)</th></tr>
</table>

BIBLIOGRAPHY

Basic bibliography

- Slides prepared by the lecturer (available in Moodlerooms).
- P. Ackerman, *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*, 1st Ed., Packt Publishing, 2017. ISBN-13: 978-1-788-39515-1
- Fundación Borredá, *Guía de Protección de Infraestructuras Críticas*, 2018 [In Spanish].

Complementary bibliography

- Boletín Oficial del Estado, Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas [In Spanish]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630
- Boletín Oficial del Estado, Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas [In Spanish]. Available: https://www.boe.es/buscar/doc.php?id=BOE-A-2011-8849
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148
- Boletín Oficial del Estado, Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [In Spanish]. Available: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257
- Consejo de Seguridad Nacional (Gobierno de España), *National Cybersecurity Strategy*, Jun. 2019 [Online]. Available: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
- Ministerio de Política Territorial y Función Pública (Gobierno de España), *Spanish National Security Framework (NSF)*, Jul. 2019 [Online]. Available: https://administracionelectronica.gob.es/ctt/ens/descargas

In compliance with current legislation on the **protection of personal data**, we inform and remind you that you can check the privacy and data protection terms you accepted at registration by entering this website and clicking "download".

https://servicios.upcomillas.es/sedeelectronica/inicio.aspx?csv=02E4557CAA66F4A81663AD10CED66792