DESCRIPCIÓN DE LA ASIGNATURA

Grado/Máster en:	Master Universitario en INGENIERÍA INFORMÁTICA por la Universidad de Málaga
Centro:	Escuela Técnica Superior de Ingeniería Informática
Asignatura:	SEGURIDAD EN SISTEMAS INDUSTRIALES Y CIBERFÍSICOS
Código:	206
Tipo:	Optativa
Materia:	ESPECIALIDAD EN CIBERSEGURIDAD
Módulo:	COMPLEMENTOS EN TECNOLOGÍAS INFORMÁTICAS
Experimentalidad:	
Idioma en el que se imparte:	Español
Curso:	2
Semestre:	1
Nº Créditos	4,5
Nº Horas de dedicación del estudiante:	112,5
Nº Horas presenciales:	33,8
Tamaño del Grupo Grande:	
Tamaño del Grupo Reducido:	
Página web de la asignatura:	

EQUIPO DOCENTE

Departamento: LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN

Área: INGENIERÍA TELEMÁTICA

Nombre y Apellidos	Mail	Teléfono Laboral	Despacho	Horario Tutorías
Coordinador/a: MARIA CRISTINA ALCARAZ TELLO	alcaraz@uma.es	95951952915	3.2.50 - E.T.S.I. INFORMÁTICA	

RECOMENDACIONES Y ORIENTACIONES

This course is closely related to the "Industrialization and Deployment of IoT Systems" and "Design and Configuration of Secure Systems in Network" courses, as students need to have a basic knowledge on i) IoT systems and ii) cybersecurity. Therefore, it is recommended that the student has successfully completed these courses. It is also recommended that the student has a basic understanding of the English language.

CONTEXTO

This course is focused on the security and privacy issues related to the deployment of Cyber-physical Systems, including their secure interactions with related technologies, such as the (Industrial) Internet of Things and Cloud Computing, and their secure integration with Smart Infrastructures, including Smart Industries, Smart Cities, Smart Homes, and Smart Healthcare. The main goal of this course is to provide students with the necessary knowledge and tools to analyze, select, develop, deploy, and evaluate security solutions in these heterogeneous and complex ecosystems.

In this course, students will understand why it is so important to integrate security and privacy solutions in the context of Cyber-physical Systems, and what are the main problems and issues related to such integration. Students will also gain knowledge regarding the threats that affect these technologies and infrastructures, and not only identify and analyze the most critical threats, but also select, integrate, and evaluate the most adequate security solutions that could be applied to protect the whole ecosystem. Moreover, students will acquire in-deep knowledge about these security solutions, including their features, advantages, and disadvantages.

COMPETENCIAS

1 Competencias generales y básicas.

Competencias básicas

1.1 CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

1.2 CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

1.3 CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

1.4 CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

1.5 CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

Competencias generales

1.1 CG1 - Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería informática.

1.2 CG2 - Capacidad para la dirección de obras e instalaciones de sistemas informáticos, cumpliendo la normativa

1 Competencias generales y básicas.

Competencias generales

vigente y asegurando la calidad del servicio.

1.4 CG4 - Capacidad para el modelado matemático, cálculo y simulación en centros tecnológicos y de ingeniería de empresa, particularmente en tareas de investigación, desarrollo e innovación en todos los ámbitos relacionados con la ingeniería en informática

1.8 CG8 - Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y mulitidisciplinares, siendo capaces de integrar estos conocimientos.

1.9 CG9 - Capacidad para comprender y aplicar la responsabilidad ética, la legislación y la deontología profesional de la actividad de la profesión de Ingeniero en Informática.

1.10 CG10 - Capacidad para aplicar los principios de la economía y de la gestión de recursos humanos y proyectos, así como la legislación, regulación y normalización de la informática.

2 Competencias específicas.

2.1 ETI1 - Capacidad para modelar, diseñar, definir la arquitectura, implantar, gestionar, operar, administrar y mantener aplicaciones, redes, sistemas, servicios y contenidos informáticos.

2.2 ETI2 - Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de redes de nueva generación, los modelos de componentes, software intermediario y servicios.

2.3 ETI3 - Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos.

2.4 ETI4 - Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

2.5 ETI5 - Capacidad para analizar las necesidades de información que se plantean en un entorno y llevar a cabo en todas sus etapas el proceso de construcción de un sistema de información.

2.8 ETI8 - Capacidad de diseñar y desarrollar sistemas, aplicaciones y servicios informáticos en sistemas empotrados y ubicuos.

3 Competencias transversales.

3.2 CT2 - Capacidad para identificar estrategias, herramientas y métodos que responden a situaciones de éxito que pueden ser abordadas con los recursos disponibles.

CONTENIDOS DE LA ASIGNATURA

Connecting Cyber-Physical Systems to Smart Environments

1.1 Fundamentals of CPS

1.2 CPS-related Technologies: IoT, IIoT, Cloud...

1.3 Smart Ecosystems: Industries, Healthcare, Cities, Homes, etc

1.4 Integration of CPS and Related Technologies in Smart Environments

1.5 Communication Protocols in an Interconnected World

Security Issues in a Smart World

2.1 Security and Privacy Problems in Smart Environments and their Technologies

2.2 Threat Taxonomy and Practical Cases

2.3 Security and Privacy Requirements for the Protection of Smart Environments

Secure Interconnection of Smart Devices

3.1 Security Primitives and Hardware Elements

3.2 Secure Communication Channels in Heterogeneous Environments

3.3 Authentication and Access Control in Constrained Devices

Advanced Cyber-Physical Systems Security in Smart Environments

4.1 Trust and Privacy in the Context of a Smart Space

4.2 Attack Prevention and Detection: The Case of a Smart Industry

4.3 Advanced Protection Services: Resilience, Blockchain in the IoT, etc

ACTIVIDADES FORMATIVAS

Actividades presenciales

Actividades presenciales

Actividades expositivas
Lección magistral

Otras actividades presenciales
Otras actividades presenciales

ACTIVIDADES DE EVALUACIÓN

Actividades de evaluación presenciales

Actividades de evaluación del estudiante
Realización de trabajos y/o proyectos
Participación en clase
Otras actividades eval.del estudiante

RESULTADOS DE APRENDIZAJE / CRITERIOS DE EVALUACIÓN

The learning outcomes of this course, plus the competencies associated with such outcomes, are as follows:

- LO1: Learn what are specific features of Cyber-physical Systems, plus its relationship with related technologies, such as IoT, IIoT, and cloud computing
Related Competencies: CG8
- LO2: Understand the concept of Smart Infrastructures, and what are the different Smart Infrastructures that exist, such as smart factories, smart cities, smart homes, and smart vehicles.
Related Competencies: CG8, ET2
- LO3: Learn about how Cyber-physical Systems and other technologies become the building blocks of Smart Infrastructures, and how Smart Infrastructures could be constructed with such building blocks.
Related Competencies: CG8, ET2
- LO4: Acquire awareness on the different security and privacy problems and issues that affect Cyber-physical Systems and related technologies; and by extension, Smart Infrastructures.
Related Competencies: CG9
- LO5: Learn how to review and identify the state of the art on the security and privacy solutions and standards for Cyber-physical Systems and related technologies.
Related Competencies: CG2, CG10
- LO6: Extract the security and privacy requirements that will be needed to deploy Cyber-physical Systems in a particular smart infrastructure.
Related Competencies: ETI1, ET5, ET8
- LO7: Learn how to identify what are the most adequate security and privacy mechanisms that will be needed in a particular smart infrastructure.
Related Competencies: CG4, CT2, ET4
- LO8: Understand how the specific features and limitations of a particular smart infrastructure (smart factory, smart industry) and Cyber-physical System technologies influence over the design, implementation and
integration of specific security mechanisms.
Related Competencies: CG1, ET1, ET8
- LO9: Learn how to integrate security and privacy mechanisms for Cyber-physical Systems in Smart Infrastructures.
Related Competencies: CG1, CG8, ET8
- LO10: Know how to test and check for the correctness of the integration of security and privacy mechanisms in Smart Infrastructures.
Related Competencies: ET3, ET4

The basic competences are reflected in the learning outcomes in the following way:

- Students will learn to understand that certain areas have their specific security needs. The knowledge acquired by students will enable them to integrate / adapt / develop specific security solutions for particular contexts (CB6).
- Students will be able to provide protection mechanisms to cutting-edge technologies applied in novel infrastructures (CB7).
- Students will understand that in this field they will have to handle such decisions involving the balance between potential threats and attack probabilities (CB8).
- The development of technical reports associated with lab works will allow students to communicate their results in a clear and unambiguous way (CB9).
- Students will have to be autonomous and able to learn by their own in order to solve the lab projects. (CB10).

PROCEDIMIENTO DE EVALUACIÓN

Evaluation of the contents of the course will be mainly based on lab projects developed by the student along the semester.

More precisely, up to 70% of the final grade will be based on two incremental lab projects (with an assignation of 35% each) and corresponding practical assignments, that student will individually perform, for which will provide activity reports.

Given the specificity of the practical activities of this course, it will not be possible to consider a different evaluation system for part-time students or high-level university athletes, including other types of special students such as those doing internships or stays abroad. All of them will have to deliver

all the activities or works proposed for the overcoming the course and that they will be able to develop outside the Center. In this case, it is essential to consider the following conditions: the quality of the description of the projects, the fulfillment of the objectives set and the delivery of the proposed activities within the established period.

For the evaluation process, the application of specific learning methodologies will also be taken into account, such as: project-based learning and based on serious games (Gamification). This means that the student could obtain extra points (up to 0,5 points) to his final grade.

The remaining 30% will correspond to a specific evaluation: 5% for participation and interest, and 25% for tests and quizzes carried out throughout the different modules.

For september (but not for december), the student can save the grade (corresponding to 70%) obtained in the practical part if desired. If he/she does not want to keep that grade, then he/she will have to complete the (theoretical-practical) questions included in the exam related to the practical part with the following assignation: theoretical part - 70%; practical part - 30% of the grade.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Alasdair Gilchrist, Industry 4.0: The Industrial Internet of Things, Apress, 2016.

Al-Sakib Khan Pathan, Securing Cyber-Physical Systems, CRC Press, 2015.

Brian Russell; Drew Van Duren, Practical Internet of Things Security, Packt Publishing, 2016.

Houbing Song; Glenn A. Fink; Sabina Jeschke, Security and Privacy in Cyber-Physical Systems, Wiley-IEEE Press, 2017.

Mohammad S Obaidat; Petros Nicopolitidis, Smart Cities and Homes, Morgan Kaufmann, 2016.

Tim Mather; Subra Kumaraswamy; Shahed Latif, Cloud Security and Privacy, O'Reilly Media, Inc., 2009.

Complementaria

John R. Vacca, Computer and Information Security Handbook, 3rd Edition Morgan Kaufmann, 2017.

Luis Ayala, Cyber-Physical Attack Recovery Procedures: A Step-by-Step Preparation and Response Guide, Apress, 2016.

DISTRIBUCIÓN DEL TRABAJO DEL ESTUDIANTE

ACTIVIDAD FORMATIVA PRESENCIAL

Descripción	Horas	Grupo grande	Grupos reducidos
Lección magistral	11,8	☑	☐
Otras actividades presenciales	22	☑	☐
TOTAL HORAS ACTIVIDAD FORMATIVA PRESENCIAL	**33,8**		
TOTAL HORAS ACTIVIDAD FORMATIVA NO PRESENCIAL	**67,45**		
TOTAL HORAS ACTIVIDAD EVALUACIÓN	**11,25**		
TOTAL HORAS DE TRABAJO DEL ESTUDIANTE	**112,5**		