Guía docente
240273 - 240AU130 - Telemática

Última modificación: 16/05/2023

Unidad responsable: Escuela Técnica Superior de Ingeniería Industrial de Barcelona
Unidad que imparte: 744 - ENTEL - Departamento de Ingeniería Telemática.

Titulación: MÁSTER UNIVERSITARIO EN INGENIERÍA INDUSTRIAL (Plan 2014). (Asignatura optativa).
MÁSTER UNIVERSITARIO EN INGENIERÍA DE AUTOMOCIÓN (Plan 2019). (Asignatura optativa).

Curso: 2023 **Créditos ECTS:** 6.0 **Idiomas:** Castellano

PROFESORADO

Profesorado responsable: Francisco José Rico Novella

Otros: Josep Paradells Aspas

REQUISITOS

La asignatura parte de unos conocimientos de sistemas comunicación ya vistos en asignaturas anteriores y se profundiza en sistemas específicos para la automoción.

METODOLOGÍAS DOCENTES

Clases expositivas
Clases de aplicación
Trabajo individual (no presencial)
Trabajo en grupo (no presencial)
Pruebas de respuesta corta (control)
Pruebas de respuesta corta (test)
Pruebas de respuesta larga (Examen final)

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

La asignatura se divide en dos partes que se imparten en paralelo, pero de forma coordinada, ya que los conocimientos ofrecidos en cada parte se reutilizan en la otra.

Una parte tiene como objetivo describir las comunicaciones usadas en los vehículos, incluyendo las internas (buses de comunicación) y las externas con el usuario, otros vehículos o plataformas de servicios. Estas últimas pueden ser bidireccionales como las relativas al acceso a información o unidireccionales como las de localización usadas por los sistemas GNSS (Global Navigation Satellite System).
Estas comunicaciones tienen diferentes requisitos como de retardo o velocidad, pero principalmente de seguridad. Se debe evitar que las comunicaciones puedan ser inspeccionadas (violación de privacidad) o alteradas, de forma que se pueda poner en riesgo la seguridad física de los pasajeros o del propio vehículo. Dada la importancia de la seguridad se dedica la otra parte de la asignatura a este tema. Se proporcionan los conocimientos de los mecanismos y técnicas de seguridad en las comunicaciones.
La asignatura combina una parte teórica con otra practica, tanto en la parte dedicada a ver los sistemas de comunicaciones como la seguridad. La asignatura parte de unos conocimientos de sistemas comunicación ya vistos en asignaturas anteriores y se profundiza en sistemas específicos para la automoción. De la misma forma se introducen conceptos de seguridad y se ejemplarizan en las comunicaciones en la automoción. Las clases son de dos tipos: teóricas y de aplicación. En las primeras se presentan los principios básicos y en las segundas se particularizan los conocimientos en casos reales de uso en automoción y con la oportunidad de visualizar estos conocimientos en clases de demostración o con ejercicios hechos en clase.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas grupo pequeño	54,0	36.00
Horas aprendizaje autónomo	96,0	64.00

Dedicación total: 150 h

CONTENIDOS

Parte seguridad (Teoría: 19 h, Aplicación: 6, Aprendizaje autónomo: 48h)

Descripción:
1. Introducción a la criptografía (Teoría: 2h. Aprendizaje Autónomo: 4h)
Servicios de seguridad
Criptografía clásica vs moderna
2. Criptografía de clave simétrica (Teoría: 5h + 1h Aplicación. Aprendizaje Autónomo: 8h)
Cifradores en flujo
Cifradores en bloque
Modos de cifrado
Aplicaciones
3. Criptografía de clave pública (Teoría: 8h + 3h Aplicación. Aprendizaje Autónomo: 21h)
Definiciones
Teoría de la complejidad
Diffie-Hellman
RSA
Otros métodos de cifrado
Firma digital
Criptografía de curva elíptica
Implicaciones de la computación cuántica
4. Sistemas tamperproof (Teoría: 2h. Aprendizaje Autónomo: 4h)
Aplicación al "security element"
5. Ejemplos en automoción (Teoría: 4h + 2h Aplicación. Aprendizaje Autónomo: 11h)
Jamming y spoofing
Algoritmos de seguridad en RFID: Crypto1
Rooling Codes
Relay attack
Uso de certificados en comunicaciones vehiculares

Dedicación: 25h
Grupo grande/Teoría: 25h

Parte de comunicaciones en el vehículo (Teoría: 20h, Aplicación: 5h, Aprendizaje autónomo: 48)

Descripción:

1. Servicios que requieren conexión en un vehículo (Teoría: 2h. Aprendizaje Autónomo: 4h)
Mantenimiento
Localización
Acceso
Ahorro de cable
Conducción segura
Información y entretenimiento
Conducción remota
2. Servicios de localización basados en satélite (Teoría: 2h. Aprendizaje Autónomo: 4h)
Sistemas GNSS
Asistencia
3. Conexión teléfono móvil con el vehículo (Teoría: 4h + Aplicación 2h. Aprendizaje Autónomo: 10h)
Bluetooth
Perfiles
Plataformas (Android Auto de Google, CarPlay de Apple y MirrorLink)
4. Acceso al vehículo (Teoría: 4h + Aplicación 2h. Aprendizaje Autónomo:8h)
Llaves digitales
Inmovilizador
RFID
Llaves inalámbricas
Control de acceso
Sistemas de despertado
Sistema de localización
5. Ahorro de cable (Teoría: 1h. Aprendizaje Autónomo: 2h)
Monitorización presión de los neumáticos
6. Sistemas celulares (Teoría: 3h + Aplicación 1h. Aprendizaje Autónomo: 8h)
4G y 5G
eCall
7. Comunicaciones vehículo a vehículo (Teoría: 4h Aprendizaje Autónomo: 12h)
IEEE802.11p
C-V2X
Arquitecturas de protocolos

Dedicación: 25h
Grupo grande/Teoría: 25h

SISTEMA DE CALIFICACIÓN

Ambas partes se evaluarán mediante dos controles cada una. También se podrá aprobar mediante el examen final de cada parte.
Para aprobar la signatura, el promedio de ambas partes debe ser igual o superior a 5 puntos no pudiendo ser la nota de alguna de las partes inferior a 3.5 puntos

BIBLIOGRAFÍA

Básica:

- Held, Gilbert. Inter- and Intra-Vehicle communications [en línea]. Boca Raton: CRC Press, 2008 [Consulta: 21/10/2022]. Disponible a : https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=321835. ISBN 9780367388317.
- Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan. "Cybersecurity challenges in vehicular communications". Vehicular Communications [en línea]. Volume 23, 2020, ISSN 2214-2096 [Consulta: 17/07/2020]. Disponible a: https://www-sciencedirect-com.recursos.biblioteca.upc.edu/journal/vehicular-communications.- Lucena López, Manuel. Criptografía y seguridad en computadores [en línea]. 5a ed. s.l.: s.n., 2022 [Consulta: 21/04/2023]. Disponible a: https://ccia.esei.uvigo.es/docencia/SSI/cripto.pdf.

Complementaria:

- Menezes, A. J. ; Scott A. Vanstone ; Paul C. Van Oorschot. Handbook of applied cryptography. Boca Ratón [etc.]: CRC Press, cop. 1997. ISBN 0849385237.
- Verdult, R.; Garcia, Flavio D.; Balasch, J. "Gone in 360 Seconds: Hijacking with Hitag2". 21st USENIX Security Symposium (USENIX Security 2012) [en línea]. [Consulta: 26/04/2023]. Disponible a: https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final95.pdf.