Universidad Zaragoza

Curso Académico: 2023/24

60962 - Seguridad avanzada

Información del Plan Docente

Año académico: 2023/24
Asignatura: 60962 - Seguridad avanzada
Centro académico: 110 - Escuela de Ingeniería y Arquitectura
Titulación: 623 - Máster Universitario en Ingeniería de Telecomunicación
Créditos: 6.0
Curso: 1
Periodo de impartición: Segundo semestre
Clase de asignatura: Obligatoria
Materia:

1. Información básica de la asignatura

El objetivo principal de la asignatura es ofrecer al alumno un panorama de las diversas metodologías y modelos existentes para la generación de servicios de comunicaciones seguros. Además de conocer las herramientas básicas de seguridad (confidencialidad, integridad y autenticidad), ahora necesitamos adquirir la capacidad de poder diseñar y evaluar las posibilidades de servicios más complejos (pruebas de conocimiento cero, identificación anónima, juego de azar en línea, etc.) para tener la base de planificar aquellos que en un futuro profesional se le pueda plantear. Y todo esto, sin perder de vista los servicios y las redes que actualmente las sustentan, para seguir ofreciendo un nivel de eficacia y eficiencia óptimo, y un equilibrio adecuado con los niveles de seguridad requeridos en cada servicio propuesto.

Estos planteamientos y objetivos están alineados con algunos de los Objetivos de Desarrollo Sostenible, ODS, de la Agenda 2030 (https://www.un.org/sustainabledevelopment/es/), de tal manera que la adquisición de los resultados de aprendizaje de la asignatura contribuirá en cierta medida al logro de la metas 16.5, 16.6 y 16.7 del objetivo 16.

2. Resultados de aprendizaje

El estudiante, al superar esta asignatura, obtendrá los siguientes resultados:

Conoce una amplia gama de operadores criptográficos y sus características de eficiencia y costos computacionales.

Sabe valorar adecuadamente los diferentes operadores criptográficos que se deben aplicar para las exigencias que un escenario de comunicaciones puede ofrecer.

Sabe distinguir entre la seguridad de un operador y la seguridad de un protocolo.

Extrae, a partir de las finalidades de un servicio, cuáles van a ser las necesidades de seguridad en su implementación.

A partir de diferentes requisitos de los servicios, es capaz de identificar los diferentes roles de seguridad que aparecerán en su modelado.

Reconoce la corrección en el diseño de servicios seguros.

Conoce diferentes herramientas de modelado que le servirán para establecer una métrica de seguridad.

Sabe analizar el nivel de seguridad de un servicio.

Conoce los protocolos criptográficos que se aplican a la mayor parte de los servicios de seguridad y es capaz de adaptarlos a las necesidades de una implementación particular.

Es capaz de analizar un problema de seguridad en las comunicaciones, para después poder ofrecer alternativas de diseño con los operadores correspondientes y obtener una solución óptima al problema planteado.

3. Programa de la asignatura

Introducción a los servicios seguros de comunicaciones: motivación y definición.

Principios de diseño de servicios seguros.

Operadores criptográficos: Criptografía simétrica y asimétrica.

Funciones pseudoaleatorias.

Cifrado en bloque.

Funciones Hash.

Cifrado autenticado.

Criptografía de clave pública.

Herramientas de análisis y gestión de servicios seguros.

Servicios seguros: Confidencialidad, autenticidad, integridad, distribución de claves, compartición de secretos, blockchains, etc.

4. Actividades académicas

Clase magistral (30 horas). Estará complementada con el estudio individual previo del alumno de material bibliográfico y combinada con su participación activa.

Resolución de problemas y casos (10 horas). Resolución de problemas propuestos por el profesor, con posibilidad de exposición de los mismos por parte de los alumnos de forma individual o en grupos autorizada por el profesor.

Prácticas de laboratorio (20 horas). Los alumnos realizarán sesiones de prácticas de 2 horas de duración cada semana.

Evaluación (3 horas). Conjunto de pruebas escritas teórico-prácticas y presentación de informes o trabajos utilizados en la evaluación del progreso del estudiante.

5. Sistema de evaluación

El estudiante deberá demostrar que ha alcanzado los resultados de aprendizaje previstos mediante las siguientes actividades de evaluación.

El alumno dispondrá de una prueba global en cada una de las convocatorias establecidas a lo largo del curso. Las fechas y horarios de las pruebas vendrán determinadas por la Escuela. La calificación de dicha prueba se obtendrá de la siguiente forma:

E1A: Examen de contenidos teórico/prácticos (50%). Puntuación de 0 a 10 puntos. Se trata de un examen escrito. Mediante esta prueba se evalúan los resultados de aprendizaje. En consecuencia, el examen incluye tanto preguntas teóricas como preguntas que implican la resolución de problemas, con resultados numéricos concretos. Para superar la asignatura es necesaria una puntuación mínima de 4 puntos sobre 10.

E1B: Evaluación de prácticas de laboratorio y trabajo práctico (50%). Puntuación de 0 a 10 puntos. Se realizará una práctica cuya entrega y posterior defensa frente al profesor supondrán la nota de la misma. Para superar la asignatura es necesaria una puntuación mínima de 4 puntos sobre 10.

Los estudiantes no superarán la asignatura si no alcanzan una calificación mínima de 5 sobre 10 puntos en la media de ambas notas: (E1A + E1B)/2.