GUÍA DOCENTE **2010 - 2011**

Asignatura (30753) CRIPTOGRAFÍA Y SEGURIDAD

Resumen

Índice

Descripción general de la asignatura

La asignatura permite adquirir unos conocimientos fundamentales sobre las necesidades de seguridad y como se debe diseñar cualquier protocolo de comunicación si se desea que sea seguro. Para ello, se presentan los ataques más habituales en el diseño de protocolos (man-in-the-middle, ataques de DoS, y DDoS¿) y el uso de algoritmos criptográficos como elemento clave para garantizar la autenticación, integridad y confidencialidad de los documentos intercambiados. También se tratan las dificultades añadidas que conlleva las limitaciones de los dispositivos al diseñar un protocolo de seguridad; se analizará brevemente la situación en redes de sensores inalámbricas y en dispositivos RFID. Este entorno permitirá enlazar con otro aspecto clave: la privacidad del individuo. De la misma forma que un buen sistema de seguridad no debería ir en detrimento de la disponibilidad de servicios, tampoco debería ir en contra de la privacidad de los usuarios. Se presentarán distintas herramientas, y un nuevo entorno en el que se puede identificar fácilmente esta necesidad de privacidad: las votaciones por Internet. En este nuevo escenario se presentarán las distintas soluciones con ejemplos prácticos

Competencias

Titulación	Competencia	Nivel
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS, SISTEMAS Y REDES DE COMUNICACIÓN	Formar investigadores y profesionales de alta cualificación en el conocimiento y diseño de sistemas de tiempo real distribuidos, y en particular de las arquitecturas y protocolos necesarios para las comunicaciones multimedia y sus mecanismos de distribución y seguridad utilizados.	Necesaria (2)
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS, SISTEMAS Y REDES DE COMUNICACIÓN	Formar investigadores y profesionales de alta cualificación en el diseño de elementos y subsistemas que formen parte de un sistema de comunicaciones.	Indispensable (1)
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS, SISTEMAS Y REDES DE COMUNICACIÓN	Formar investigadores y profesionales de alta cualificación en el diseño, implementación y evaluación de prestaciones de las redes de comunicaciones tanto fijas como móviles, así como en el proceso de creación de la Sociedad de la Información.	Necesaria (2)

Titulación	Materia	Competencia	Nivel

Conocimientos recomendados

Previos

Titulación	Asignatura

Simultaneos

Titulación	Asignatura

Selección y estructuración de las Unidades Didácticas

1. Seguridad en redes
    1. Introducción a la seguridad en redes
    - Mecanismos de seguridad
    - Conceptos básicos de criptografía
    2. Servicios de seguridad
    - Confidencialidad
    - Integridad
    - Autenticidad
    - Control de acceso
    - No repudio
    3. PKI/PMI Infraestructuras de clave pública y gestión de privilegios
    4. Seguridad en IP
    5. Seguridad perimetral
    6. Seguridad en pagos
    7. Seguridad en comunicaciones de grupo
    8. Seguridad en redes de sensores
    9. Votaciones electrónicas seguras

Distribución

Unidad didáctica	Trab. Presencial	Trab. no presencial
Seguridad en redes	30,00	45,00
Total horas	**30,00**	**45,00**

Metodología de enseñanza-aprendizaje

Presenciales

Nombre	Descripción	horas
Clase presencial	Exposición de contenidos mediante presentación o explicación por parte de un profesor (posiblemente incluyendo demostraciones).	25,00
Aprendizaje basado en problemas	Enfoque educativo orientado al aprendizaje y a la instrucción en el que los alumnos abordan problemas reales en pequeños grupos y bajo la supervisión de un tutor.	5,00
	Total horas	**30,00**

Autónomas

Nombre	Descripción	horas
Estudio teórico	Estudio de contenidos relacionados con las "clases teóricas": Incluye cualquier actividad de estudio que no se haya computado en el apartado anterior (estudiar exámenes, trabajo en biblioteca, lecturas complementarias, hacer problemas y ejercicios, etc.).	45,00
	Total horas	**45,00**

Evaluación

Nombre	Descripción
Prueba escrita de respuesta abierta	Prueba cronometrada, efectuada bajo control, en la que el alumno construye su respuesta. Se le puede conceder o no el derecho a consultar material de apoyo.
Pruebas objetivas (tipo test)	Examen escrito estructurado con diversas preguntas o ítems en los que el alumno no elabora la respuesta; sólo ha de señalarla o completarla con elementos muy precisos.

Recursos

· pizarra

· copia de las transparencias

· transparencias

Bibliografía