Máster en Tecnologías de la Información y Comunicación en Redes Móviles
62531 - T3-Seguridad en redes inalámbricas

Guía docente para el curso 2010 - 2011

Curso: 1, Semestre: 2, Créditos: 4.5

Información básica

Profesores

- **José Luis Salazar Riaño** jsalazar@unizar.es
- **María Victoria Higuero Aperribai** marivi.higuero@ehu.es
- **Eduardo Jacob Taquet** eduardo.jacob@ehu.es

Recomendaciones para cursar esta asignatura

Es imprescindible conocer los fundamentos generales de redes de comunicación y experiencia en el uso de redes WiFi.

Actividades y fechas clave de la asignatura

La planificación y horarios se encontrarán disponibles en la página web propia del máster:

http://www.ticrm.es/

Inicio

Resultados de aprendizaje que definen la asignatura

El estudiante, para superar esta asignatura, deberá demostrar los siguientes resultados...

1:
Comprende los peligros que acechan en el mundo de las comunicaciones inalámbricas y las herramientas que se encuentran disponibles para luchar contra ellos.

2:
Es capaz de seleccionar y utilizar los bloques criptográficos básicos en función de los objetivos que se persiguen.

3:
Comprende el procedimiento de diseño de protocolos de seguridad y conocer de manera básica la validación de los mismos por medio de herramientas automatizadas.

4: Conoce los mecanismos de autenticación y autorización que se emplean en las tecnologías inalámbricas más comunes y ser capaz de entender nuevos protocolos.

5:
Comprende y aplica las aplicaciones de la criptografía y el desarrollo de protocolos de seguridad a aplicaciones que se dan en entornos móviles como son los pagos y aplicaciones avanzadas.

Introducción

Breve presentación de la asignatura

Esta asignatura se enmarca dentro de los cursos de Telemática y su objetivo principal es dotar al alumno de conocimientos avanzados en técnicas y servicios de seguridad en comunicaciones inalámbricas, primero desde un punto de vista genérico para a continuación concretar los mismos en distintos casos.

- Concienciar al alumno de los diferentes tipos de peligros que pueden aparecer en las comunicaciones.

- Describir las técnicas criptográficas disponibles y que permiten implementar los mecanismos de seguridad necesarios para luchar contra los peligros existentes.

- Describir técnicas para el desarrollo de protocolos de seguridad y de los procedimientos para valorar el correcto diseño de los mismos.

- Describir soluciones existentes a diversos niveles (enlace, red, aplicación) para garantizar implantaciones seguras.

Contexto y competencias

Sentido, contexto, relevancia y objetivos generales de la asignatura

La asignatura y sus resultados previstos responden a los siguientes planteamientos y objetivos:

Su objetivo principal es dotar al alumno de conocimientos avanzados en técnicas y servicios de seguridad en comunicaciones inalámbricas, primero desde un punto de vista genérico para a continuación concretar los mismos en distintos casos.

Contexto y sentido de la asignatura en la titulación

El Máster TICRM está dividido en seis grupos de asignaturas:

1. Cursos Metodológicos (M#).
2. Cursos de Tratamiento de Señal (S#).
3. Cursos de Telemática (T#).
4. Cursos de Electromagnetismo (EM#).
5. Cursos de Sistemas de Telecomunicación (ST#).
6. Cursos de Radiocomunicaciones (R#).

Esta asignatura se enmarca dentro de los cursos de Telemática en los que se abordan los métodos de aumento de capacidad de los sistemas de comunicaciones móviles e inalámbricos y se profundizará en el estudio de distintos procedimientos de gestión de recursos radio. Asimismo, se ahonda en los aspectos que están marcando la evolución de Internet hacia las redes de comunicaciones de 4ª Generación. Se ofertan 6 cursos con un total de 30 créditos ECTS.

Al superar la asignatura, el estudiante será más competente para...

1:
Describir los peligros que soportan las comunicaciones inalámbricas, comprender los algoritmos criptográficos y los protocolos de seguridad básicos empleados en diversas tecnologías de comunicación inalámbricas, conocer los principios básicos para el diseño y validación de protocolos de seguridad y dominio de la implantación de los mismos en diversas aplicaciones en entorno inalámbrico.

Importancia de los resultados de aprendizaje que se obtienen en la asignatura:

Los resultados de aprendizaje de esta asignatura dotan al alumno de conocimientos y habilidades en el marco de la seguridad en redes inalámbricas, y en general, responden al objetivo general de la titulación de formación de profesionales de la investigación en el área de las Tecnologías de la Información y Comunicaciones en Redes Móviles que puedan incorporarse en los proyectos de investigación que se desarrollan en empresas y Universidades.

Evaluación

Actividades de evaluación

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

1:

Se pretende que la evaluación para los alumnos que asisten con regularidad al curso (más de un 75% de las horas presenciales) sea continuada a través de la evaluación de los ejercicios propuestos a lo largo del curso. Sobre estos ejercicios, se realizarán preguntas en una sesión de examen que podrá ser oral o por escrito. Por el perfil de los alumnos es posible que alguno de los mismos, por motivos profesionales, no pueda asistir a las clases con la regularidad deseada. En estos casos, será posible obtener la calificación por medio de un examen final, que reflejará los contenidos vistos en la asignatura.

Actividades y recursos

Presentación metodológica general

El proceso de aprendizaje que se ha diseñado para esta asignatura se basa en lo siguiente:

CE: Clase magistral participativa donde se expondrán los contenidos fundamentales de la materia. Esta actividad se realizará en el aula de forma presencial.

PA: Prácticas de aula:

PA1: Problemas y casos prácticos: cada profesor propondrá a los alumnos tareas relacionadas con la materia impartida donde se ponga de manifiesto su comprensión de la misma así como su capacidad para buscar información y sintetizarla. Estas actividades se proponen y se exponen en el aula, pero pueden elaborarse o realizarse fuera de ella por los alumnos de forma individual o en grupo, tutorizados por el profesor.

PA2: Elaboración y presentación de trabajos: cada profesor de la asignatura propondrá una serie de trabajos pata profundizar sobre un aspecto del tema o temas que ha impartido. Cada alumno deberá de elegir una de estas propuestas

para desarrollarla y ampliarla elaborando un informe donde se ponga de manifiesto su capacidad para buscar, organizar, y sintetizar información. De la misma forma que la actividad anterior estos trabajos se propondrán y se expondrán en el aula pero se realizarán de forma individual por el alumno tutorizado por el profesor. Estos trabajos deberán de presentarse a los profesores y al resto de los alumnos en forma de seminario participativo de forma que se pueda valorar la capacidad del alumno para transmitir información y hasta qué punto ha profundizado en el tema escogido.

PL: Prácticas de laboratorio o aula de informática: para completar algunos temas se realizarán actividades prácticas utilizando diversos entornos de simulación lo que permitirá valorar la capacidad para el auto-aprendizaje del alumno.

TG: Tutorías: dado que los alumnos de cada asignatura pueden pertenecer a cualquiera de las

universidades participantes, las tutorías se realizarán a lo largo de todo el curso y podrán ser en grupo o individualizadas, presenciales o a distancia a través de videoconferencia, correo electrónico, etc.

Actividades de aprendizaje programadas (Se incluye programa)

El programa que se ofrece al estudiante para ayudarle a lograr los resultados previstos comprende las siguientes actividades...

1:

Contenidos:

Tema 1 — Conceptos de seguridad en sistemas distribuidos
- Ataques y amenazas: Modelo de Red (Dolev-Yao)
- Concepto de servicios y mecanismos.

Tema 2 — Conceptos de criptografía)
- Bloques criptográficos
  - Cifradores de bloque
  - Cifradores de flujo
  - Resúmenes criptográficos
  - Generadores de números aleatorios.
  - Técnicas de cifrado
    - Criptografía de clave simétrica.
    - Criptografía de clave asimétrica.
    - Ataques criptoanalíticos

Tema 3 — Estructuras de certificación

Tema 4 — Diseño de protocolos criptográficos
- Conceptos básicos.
- Métodos no formales.
- Métodos formales de evaluación.
- Estudio de casos.
  - WiFi
  - WiMax
  - Bluetooth

Tema 5 — Seguridad a nivel de aplicaciones
- eCommerce
- ePagos
- mPagos

Tema 6 — Aplicaciones avanzadas de la criptografía en comunicaciones inalámbricas
- Encaminamiento seguro

2:

Planificación:

MODALIDADES		Horas	%	**Totales**
Presencial	Clases Expositivas	18	40	**45**
	Práctica de aula / Seminarios / Talleres	10,5	23	
	Prácticas de laboratorio / campo / aula de informática / aula de idiomas	3	7	
	Prácticas clínicas hospitalarias			
	Tutorías grupales/individuales	9	20	
	Prácticas Externas			
	Sesiones de evaluación	4,5	10	
No presencial	Trabajo en Grupo			**67,5**
	Trabajo Individual	67,5	100	

	Total	**112,5**		

Planificación y calendario

Calendario de sesiones presenciales y presentación de trabajos

La planificación y horarios se encontrarán disponibles en la página web propia del máster:

http://www.ticrm.es/

Bibliografía y recursos

Como recursos, se dispone de las bibliotecas de los distintos centros, en las que la bibliografía propuesta se encuentra disponible, también se dispone del servidor WWW del Máster, donde se colgarán los apuntes con antelación suficiente y de un aula de ordenadores de libre acceso desde la que realizar los trabajos relacionados con la asignatura y las búsquedas en Internet.

Bibliografía básica, bibliografía de profundización, direcciones de Internet de interés, revistas, etc.

- R. Anderson: *Security engineering*. John Wiley & Sons Inc. 2001.
- D. Gollman: *Computer security*. 1st Edition, John Wiley & Sons Inc. 1999.
- S. Hagen: *IPv6 essentials*. O'Reilly, July 2002.
- Feghhi: *Digital certificates*. Addison-Wesley, 1999.
- J. Pastor, M. A. Sarasa, J. L. Salazar: *Criptografía digital: fundamentos y aplicaciones*. 2ª Edición. Prensas Universitarias de Zaragoza, 2001.
- A. J. Menezes, P. C. Van Oorchot, S. A. Vanstone: *Handbook of applied cryptography*. CRC Press, 1997.
- C. Gehrmann, J. Persson, B. Smeets: *Bluetooth security*. Artech House, 2004.
- J. Khan, A. Khwaja: *Building secure wireless networks with 802.11*. Wiley Publishing, 2003.
- M. Walker, *On the security of 3GPP Networks*. Disponible en:

http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000/mike_walker.pdf

- M. Mouly, M. Pautet: *The GSM system for mobile communications*. Telecom Publishing, 1992.
- Red temática Iberoamericana de Criptografía y Seguridad de la Información:

http://www.criptored.upm.es

- Herramienta Cryptool: http://www.cryptool.com/
- Herramienta Span: http://www.irisa.fr/celtique/genet/span/

Referencias bibliográficas de la bibliografía recomendada