Máster en Ingeniería de Telecomunicación
60929 - Seguridad y gestión avanzadas

Guía docente para el curso 2014 - 2015

Curso: 1, Semestre: 2, Créditos: 5.0

Información básica

Profesores

- **Álvaro Alesanco Iglesias** alesanco@unizar.es

- **José Luis Salazar Riaño** jsalazar@unizar.es

Recomendaciones para cursar esta asignatura

Para seguir con normalidad esta asignatura es especialmente recomendable que el alumno que quiera cursarla, aparte de cumplir los requisitos exigidos para cursar el máster, tenga un sólido dominio en la aplicación de herramientas de seguridad y gestión en las comunicaciones y amplios conocimientos sobre sus fundamentos.

Para el óptimo aprovechamiento de la asignatura se recomienda al alumno la asistencia activa a clase (tanto de teoría como de problemas). Del mismo modo se recomienda al alumno el aprovechamiento y respeto de los horarios de tutorías del profesorado para la resolución de posibles dudas de la asignatura y un correcto seguimiento de la misma.

Actividades y fechas clave de la asignatura

La asignatura consta de un total de 5 créditos ECTS. Las actividades se dividen en clases teóricas, resolución de problemas o casos prácticos en clase y prácticas de laboratorio. Las actividades tienen como objetivo facilitar la asimilación de los conceptos teóricos complementándolos con los prácticos, de forma que se adquieran los conocimientos y las habilidades básicas relacionadas con las competencias previstas en la asignatura.

Las fechas de inicio y finalización del curso y las horas concretas de impartición de la asignatura así como las fechas de realización de las prácticas de laboratorio e impartición de seminarios se harán públicas atendiendo a los horarios fijados por la Escuela.

Inicio

Resultados de aprendizaje que definen la asignatura

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

1:

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

- 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.

- Conoce las arquitecturas seguras de gestión en redes TCP/IP.

- Analiza las necesidades de gestión para el correcto funcionamiento de redes TCP/IP.

- Aplica los nuevos sistemas de gestión segura de redes del IETF.

- Conoce las ventajas e inconvenientes de diferentes sistemas de configuración de red.

- Sabe analizar la escalabilidad de los sistemas de configuración de red.

- Reconoce la necesidad de una gestión segura y es capaz de añadir una capa extra de seguridad a aquellos servicios de gestión que no dispongan de ella.

- Sabe planificar la implantación, supervisión y mantenimiento redes, servicios y aplicaciones, así como gestionar y asegurar la calidad en el proceso de desarrollo.

Introducción

Breve presentación de la asignatura

La asignatura presenta la seguridad y la gestión de servicios desde su planteamiento inicial de planificación en los proyectos de telecomunicaciones. Si bien durante el grado, el alumno ha adquirido conceptos básicos que le van a permitir gestionar servicios seguros con soltura, es ahora donde puede plantearse proyectos de servicios en los que, con las herramientas ya adquiridas, pueda garantizar una gestión eficaz y eficiente dentro de una seguridad integral y demostrable.

Comenzaremos mostrando diferentes metodologías de trabajo para la medida de la seguridad en diferentes protocolos, para posteriormente ir analizando uno por uno su validez. Por otra parte, se estudiarán las arquitecturas existentes que consolidan la parte de gestión básica de la seguridad en las comunicaciones, y sobre las que construimos servicios y que posibilitan su gestión eficaz y más eficiente.

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:

El objetivo principal de la asignatura es ofrecer al alumno un panorama de las diversas metodologías y modelos arquitectónicos existentes para la generación de servicios de comunicaciones seguros. Ya no es suficiente conocer las herramientas básicas de seguridad (confidencialidad, integridad y autenticidad), y de gestión que podía permitir la implementación de servicios básicos. Ahora necesitamos adquirir la capacidad de poder planificar 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.

Contexto y sentido de la asignatura en la titulación

La asignatura de *Seguridad y Gestión Avanzadas* se imparte en el primer curso de la titulación, más concretamente en el

semestre de primavera y tiene una carga de trabajo de 5 ECTS. La asignatura forma parte de la materia denominada Redes y Servicios dentro del módulo de Tecnologías de Telecomunicación, que cubre competencias obligatorias dentro de la titulación del Máster Universitario en Ingeniería de Telecomunicación.

Los resultados de aprendizaje de esta asignatura servirán de complemento a las asignaturas Redes y Servicios de Comunicaciones Móviles, Redes Heterogéneas e Internet de Nueva Generación que forman parte de la materia Redes y Servicios, proporcionando al alumno los conocimientos que éste necesita para la planificación de la gestión segura de las redes de telecomunicación, aspecto fundamental para el diseño correcto de cualquier red.

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

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.

CB7 Los estudiantes sabrán 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

CB8 Los estudiantes serán 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.

CB9 Los estudiantes sabrán 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.

CB10 Los estudiantes poseerán las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

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

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 de Telecomunicación y campos multidisciplinares afines.

CG7 Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos electrónicos y de telecomunicaciones, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.

CG11 Capacidad para saber comunicar (de forma oral y escrita) las conclusiones- y los conocimientos y razones últimas que las sustentan- a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CG12 Poseer habilidades para el aprendizaje continuado, autodirigido y autónomo.

CE4 Capacidad para diseñar y dimensionar redes de transporte, difusión y distribución de señales multimedia.

CE6 Capacidad para modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.

CE7 Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.

CE8 Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de Internet de nueva generación, los modelos de componentes, software intermediario y servicios.

CE9 Capacidad para resolver la convergencia, interoperabilidad y diseño de redes heterogéneas con redes locales, de acceso y troncales, así como la integración de servicios de telefonía, datos, televisión e

interactivos.

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

La asignatura la podemos calificar como fundamental dentro de la materia en la que se ubica, ya que no se puede entender el diseño, análisis e implementación de un proyecto de telecomunicaciones sin una metodología de evaluación de la seguridad y de las posibilidades y alcance de los servicios. La asignatura permite al alumno conocer y ser capaz de diseñar y evaluar el alcance y la seguridad de un sistema de comunicaciones y/o modificar un sistema previo para dotarlo de nuevas capacidades de gestión y seguridad.

Evaluación

Actividades de evaluación

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

1:

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:

E1: Examen final (100%). Puntuación de 0 a 10 puntos. Consta de dos partes:

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 4,5 puntos sobre 10 en el Examen de Contenidos Teórico/Prácticos.

E1B: Prueba final de prácticas de laboratorio (50%). Puntuación de 0 a 10 puntos. Sólo deberá ser realizada por los estudiantes que no hayan superado las prácticas durante el periodo docente. Consiste en la resolución de un ejercicio práctico en el laboratorio que será evaluado oralmente y mediante un cuestionario escrito. Este ejercicio podrá incluir contenidos de todas las prácticas realizadas durante el periodo docente, sin excluir aspectos específicamente relacionados con el manejo de las herramientas utilizadas en las mismas. La prueba se realizará en el laboratorio el mismo día en el que se realicé el examen de contenidos teórico/práctico, si bien, dado el carácter individualizado de la evaluación, podría ser necesario programar estas pruebas en días diferentes, lo que será notificado a los estudiantes afectados con suficiente antelación. En cualquier caso, un alumno que tiene liberada esta parte, siempre puede optar por realizar la prueba final. En ese caso, la calificación obtenida será la de la prueba final.

Para superar la asignatura es necesaria una puntuación mínima de 4,5 puntos sobre 10 en la Prueba final de prácticas de laboratorio.

E2: Pruebas intermedias de evaluación

E2B: Prácticas de laboratorio (50%): Puntuación de 0 a 10 puntos. Se recomienda encarecidamente a los alumnos matriculados la realización de las prácticas de laboratorio a lo largo del curso. La evaluación de las prácticas de laboratorio, en las sesiones programadas durante el curso, se realizará, para los alumnos que asistan a todas ellas, mediante la presentación de estudios o trabajos previos cuando estos sean necesarios para el desarrollo de la práctica, el informe de seguimiento de la misma y la resolución de una serie de cuestiones al finalizar la práctica (unidad completa de una o más sesiones). La calificación de estas pruebas representará el 20% de la nota final. La obtención de una calificación igual o superior a 4,5 puntos eximirá al alumno de realizar la prueba final práctica en el laboratorio. Los alumnos que no asistan a las prácticas deberán realizar la prueba final de prácticas de laboratorio de acuerdo con el procedimiento descrito en E1B.

En resumen:

La nota final se calculará mediante la siguiente expresión:

0,8xE1A+0,2xEB siempre que se cumplan las tres condiciones siguientes:

(0,8xE1A+0,2xEB)≥5 y E1A≥4,5 EB≥4,5

Donde

EB corresponde a la nota de las prácticas de laboratorio obtenida bien mediante la asistencia a las sesiones programadas y la evaluación continua (E2B) o bien mediante la prueba final de prácticas de laboratorio (E1B) de acuerdo a los procedimientos descritos anteriormente. Así:

EB=E1B si realiza la prueba final de laboratorio.

EB=E2B si NO realiza la prueba final de laboratorio.

Si no se cumplen las condiciones anteriores, en la nota final figurará suspenso.

Las notas de E2B se mantendrán para su cómputo en la siguiente convocatoria del mismo año académico. No se guardarán las notas de la prueba final de la primera convocatoria para segunda convocatoria.

Actividades y recursos

Presentación metodológica general

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

Las metodologías de enseñanza-aprendizaje que se realizarán para conseguir los resultados de aprendizaje propuestos son las siguientes:

M1: Clase magistral participativa (25 horas). Exposición por parte del profesor de los principales contenidos de la asignatura, combinada con la participación activa del alumnado. Esta actividad se realizará en el aula de forma presencial. Esta metodología, apoyada con el estudio individual del alumno (M14) está diseñada para proporcionar a los alumnos los fundamentos teóricos del contenido de la asignatura.

M8: Prácticas de aula (5 horas). Resolución de problemas y casos prácticos 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. Esta actividad se realizará en el aula de forma presencial, y puede exigir trabajo de preparación por parte de los alumnos (M13).

M9: Prácticas de laboratorio (20 horas). Los alumnos realizarán sesiones de prácticas de 2 horas de duración cada semana. Esta actividad se realizará de forma presencial en el Laboratorio de Prácticas 2.03 (Laboratorio de Telemática), del edificio Ada Byron. El trabajo a desarrollar se realizara en pequeños grupos.

M10: Tutoría (6 horas)**.** Horario de atención personalizada al alumno con el objetivo de revisar y discutir los materiales y temas presentados en las clases tanto teóricas como prácticas.

M11: Evaluación (3 horas). Conjunto de pruebas escritas teórico-prácticas y presentación de informes o trabajos utilizados en la evaluación del progreso del estudiante. El detalle se encuentra en la sección correspondiente a las actividades de evaluación

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:

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

2.- Principios de diseño de servicios seguros.

3.- Herramientas de análisis de servicios seguros.

3.1.- Lógica BAN y GYN

3.2.- Probadores de teoremas

3.3.- Model checking.

4.- Servicios seguros.

4.1.- Confidencialidad, autenticidad e integridad

4.2.- Distribución de claves

4.3. Compartición de secretos

4.4.- Pruebas de conocimiento cero (ZKP)

4.5.- Compromiso con un bit y transferencia inconsciente

4.6.- Votación electrónica

4.7.- Juegos de azar en la red.

5.- Arquitectura de gestión segura SNMPv3.

5.1.- Arquitectura, seguridad y administración

5.2.- Procesado del mensaje y entrega

5.3.- Aplicaciones snmpv3

5.4.- Modelo de seguridad basado en usuario

5.5.- Control de acceso basado en vistas (VACM)

Prácticas de Laboratorio:

Esta actividad se realizará de forma presencial en un aula informática. Comprenderá 10 sesiones de 2 horas de duración cada una de ellas. Los alumnos presentarán posteriormente los resultados exigidos para cada una de las prácticas.

Planificación y calendario

Calendario de sesiones presenciales y presentación de trabajos

El calendario de la asignatura, tanto de las horas presenciales, como las sesiones de laboratorio estará definido por el centro en el calendario académico del curso correspondiente.

Referencias bibliográficas de la bibliografía recomendada

- Caballero, Pino. Introducción a la criptografía / Caballero, Pino. - 2ª ed. Ra-Ma, Textos Universitarios, Madrid. Año 2002
- Kurose, James F.. Computer networking : a top-down approach / James F. Kurose, Keith W. Ross ; international edition adapted by Bhojan Anand . - 4th ed. Boston : Pearson, cop. 2008
- Menezes, Alfred J.. Handbook of applied cryptography / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone . - [1st ed.] Boca Raton [etc.] : CRC, cop. 1997
- Pastor Franco, José. Criptografía digital : fundamentos y aplicaciones / José Pastor Franco, Miguel Angel Sarasa López, José Luis Salazar Riaño . - 2a. ed. Zaragoza : Prensas Universitarias de Zaragoza, 2001
- Schneier, Bruce. Applied cryptography : protocols, algorithms and source code in C / Bruce Schneier New York [etc.] : John Wiley and Sons, cop. 1994
- Stallings, William. Cryptography and network security : principles and practice / Williams Stallings . - 3rd ed. Upper Saddle River : Prentice Hall , cop. 2003

- Técnicas criptográficas de protección de datos / Amparo Fúster Sabater...[et al.] . - 2a. ed. rev. y act. Madrid : Ra-ma, D.L. 2000