Universidad de La Laguna
Escuela Técnica Superior de Ingeniería Informática

Asignatura

Código	Nombre de la asignatura
135213902	**TÉCNICAS Y APLICACIONES EN SEGURIDAD INFORMÁTICA (plan 2008)**

Programa Oficial de Posgrado (**Optativa**)
y de **3** créditos
Impartido en el departamento **Estadística, Investigación Operativa y Computación**

Pertenece al área de conocimiento **CCIA y LSI**

Objetivos

Del análisis de las competencias generales y específicas asociadas al perfil de los alumnos de este posgrado se desprende la necesidad de los futuros profesionales de saber desenvolverse tanto en la implementación como en el uso de las diferentes técnicas y aplicaciones de seguridad relacionadas con la protección de la información y de servicios. De este modo, se hace imprescindible el poseer conocimientos de nivel avanzado en el manejo de las técnicas que la Criptología y la Seguridad Informática proponen con este fin.

Con esta asignatura se persigue que el alumno se familiarice con diferentes entornos y herramientas informáticas que facilitan la consecución de las competencias específicas relacionadas con la protección de la información durante cualquier proceso de tratamiento automático de la información. Por esto se analizan tanto técnicas relacionadas con el Criptoanálisis de los sistemas más utilizados como medidas de protección específicamente diseñadas para entornos particulares como puede ser el caso de las infraestructuras PKI, tarjetas inteligentes, contratos electrónicos, pago electrónico, e-voting, e-cash, etc.

Metodología

La metodología propuesta se orienta al desarrollo de la enseñanza basada en ECTS. Se contemplan las siguientes actividades:

Clases magistrales. Su objetivo es la divulgación de los contenidos teóricos de la materia que permitirán al alumnado realizar diferentes actividades, tales como la evaluación de diferentes herramientas de seguridad.

Prácticas en aula informática. Prácticas realizadas en grupos reducidos, en las cuales el alumno realizará distintos tipos de actividades en función de los objetivos a alcanzar. Estas prácticas serán principalmente tutorizadas, en las que el profesor explica al alumno cómo utilizar y desarrollar procedimientos y herramientas software. Los alumnos dispondrán con, al menos, una semana de antelación de la documentación necesaria para la realización de la práctica.

Ejercicios. Cada tema incluido en el programa tiene una colección de ejercicios que será entregada al alumno antes de comenzar el tema correspondiente para que pueda ir realizando la resolución de los mismos. Una vez finalizado el tema deberá entregar la resolución de los mismos. Dependiendo del número de ejercicios planteados y de su dificultad habrá casos en los que se requiera el trabajo en grupo en esta actividad.

Trabajos monográficos. En esta actividad el alumno desarrollará de manera individual o en grupos reducidos una memoria sobre un tema particular escogido por ellos de entre una lista proporcionada por el profesor. Para ello se le facilitará un pequeño dossier de documentación y se le exhortará a que utilice otras fuentes de documentación. Además deberá realizar una presentación de dicha memoria.

Seminarios. El seguimiento del alumno es imprescindible para obtener una evaluación lo más objetiva del aprendizaje del alumno, es por esto por lo que en esta actividad la participación del estudiante será primordial. Las actividades a realizar en las sesiones de seguimiento se dividen en actividades en el aula y en el laboratorio de informática.
1. Actividades en aula de teoría: Un listado específico de cuestiones relacionadas con cada uno de los temas será planteado de manera individual al alumno. La respuesta de las mismas se podrá realizar oralmente, cuando los contenidos del tema así lo permitan. De esta manera se podrá establecer un debate en el aula del que el alumno podrá extraer las conclusiones más significativas relacionadas con el tema tratado. También se reservará tiempo para que los alumnos planteen sus propias cuestiones.
2. Actividades en el laboratorio de informática: distinguimos entre actividades en las que los alumnos reciben una serie de cuestiones que tiene que llevar a cabo utilizando algún software particular y actividades en las que el alumno debe explicar al profesor un trabajo que ha realizado previamente. En el primer caso se establecerán las oportunas comparaciones entre las diferentes soluciones encontradas con la intención de que el alumno desarrolle una opinión crítica obteniendo juicios de valor relacionados con la materia.

Metodología de evaluación

A continuación se enumeran las herramientas utilizadas en la evaluación, así como la contribución de cada una de ellas a la calificación final obtenida por el alumno en la asignatura.

Pruebas escritas (40%) + prácticas (20%) + ejercicios (20%) + trabajos monográficos (presentados en las horas de seminario práctico o en las tutorías) (20%).

Es imprescindible que el alumno asista al menos al 80% de las actividades vinculadas a la asignatura. Para superar la asignatura el alumno debe superar la prueba teórica escrita y la parte práctica. La parte práctica se supera obteniendo la calificación de Apto en el 75% de las prácticas realizadas.

Contenidos de teoría

Los contenidos han sido estructurados según bloques temáticos diferenciados debido a que cada uno de ellos está asociado a un propósito específico.
-Bloque 1: Criptoanálisis clásico y moderno.
-Bloque 2: Soluciones de autenticación basadas en infraestructuras PKI: estándar X.509, PGP, funciones hash.
-Bloque 3: Protocolos criptográficos avanzados: firma de contratos electrónicos, pago electrónico, e-voting, e-cash.
-Bloque 4: Protección de la información multimedia: watermaking, fingerpriting.
-Bloque 5: Seguridad en tarjetas inteligentes.
-Bloque 6: Herramientas de seguridad en la e-administración: DNI electrónico, time stamping.
-Bloque 7: Seguridad en protocolos de conexión punto a punto: SSH, SSL, TLS.

El primer bloque se dedica a la descripción de los conceptos y técnicas de Criptoanálisis con el fin de que el alumno se familiarice con las debilidades presentes en algunos sistemas y las técnicas que ayudan a la explotación de las mismas.

Seguidamente se presta especial atención al problema de la autenticación analizando las soluciones basadas en infraestructuras PKI y Funciones Hash.

El tercer bloque introduce al alumno en el diseño de protocolos criptográficos avanzados de propósito particular tales como la Firma de Contratos Electrónicos. Con este bloque el alumno estará en condiciones de valorar la infinidad de entornos diferentes que requieren medidas de protección de la información.

La protección de la información multimedia es analizada en el siguiente bloque dedicado principalmente a las técnicas de watermaking y fingerpriting.

Además se describirán y analizarán herramientas de seguridad utilizadas actualmente en las administraciones públicas como es el caso del DNI electrónico.

La última parte de la asignatura aborda el tema de protocolos de comunicaciones tales como SSH, SSL, TLS, etc. que poseen medidas de protección embebidas.

Bibliografía

- *Network and Internetwork Security*: Principles and practice. Stallings, William. Prentice-Hall, International Edition, 1995.
- *Fundamentals of Computer Security*, Pieprzyk, Josef, Hardjono, Thomas, Seberry, Jennifer, 2003
- *Cryptanalysis of Number Theoretic Ciphers, Wagstaff, S.S.*, Chapman &Hall/CRC, 2003
- *Foundations of Security Analysis and Design*, Focardi, R, Gorrieri, R., Springer, 2001

- *Protocols for Authentication and Key Stablishment*, Boyd, C., Mathuria, A., Springer, 2003

Además de la bibliografía listada anteriormente, el profesorado de la asignatura aporta material didáctico específico para cada bloque de contenidos en el que incorporan tanto apuntes como colecciones de problemas, informes, documentos de trabajo, etc.

Compiladores de diferentes lenguajes de programación para que el alumno implemente sus propias herramientas de seguridad.

Herramientas para la manipulación de tarjetas inteligentes

Profesores

HERNÁNDEZ GOYA, Mª CANDELARIA (coordinador)

Teléfono : 922318637
Correo Electrónico : mchgoya@ull.es

Localización	Tutorías
Facultades de Física y Matemáticas 4º planta	Martes y Jueves 9:00-12:00

CABALLERO GIL, PINO

Teléfono : 81-76
Correo Electrónico : pcaballe@ull.es

Localización	Tutorías

Firma Profesor **Firma director del departamento**