ASIGNATURA DE MÁSTER:

DESARROLLO DE SOFTWARE SEGURO (MÁSTER EN INGENIERÍA INFORMÁTICA)

Curso 2016/2017

(Código:31106205)

1.PRESENTACIÓN

Lamentablemente los denominados “ciberataques” son noticia frecuente en los medios de comunicación. Según los datos publicados por el CERT (Computer Emergency Response Team) las vulnerabilidades de los sistemas informáticos reportadas cada año crecen y aumentan su grado de sofisticación.

En este curso se presentan métodos rigurosos, técnicas y herramientas para desarrollar e implantar software seguro. Los métodos incluyen el análisis de código para detectar las vulnerabilidades habituales, la revisión de código fuente mediante herramientas de análisis estático y buenas prácticas para desarrollar código seguro en lenguajes concretos de programación.

Los métodos y herramientas que se estudian sirven para la realización de pruebas, verificación y validación de software y sistemas, comprobando que se cumplen los requisitos funcionales y de seguridad. Con todos ellos, se aprende a validar y verificar el aseguramiento de la seguridad así como a establecer la diferencia entre vulnerabilidades y errores de programación. Las técnicas de test incluyen las pruebas de caja blanca, caja negra, pruebas contra ataques, amenazas y penetración, pruebas de resiliencia, etc.

2.CONTEXTUALIZACIÓN

La asignatura “Desarrollo de Software Seguro” se enmarca en el Máster Universitario en Ingeniería Informática, dentro del Módulo “Complementos en tecnología informática”. Es una asignatura optativa de 6 créditos que se imparte en el primer semestre. La relación con estas otras asignaturas del máster:

- Planificación y gestión de proyectos informáticos de I+D+i
- Sistemas empotrados
- Temas avanzados de redes e internet
- Cloud computing y gestión de los servicios de red
- Sistemas operativos de dispositivos móviles.

Se puede resumir indicando que esta asignatura de “Desarrollo de Software Seguro” supone una extensión de todas ellas cuando se trata de desarrollar un sistema software que debe tener la cualidad adicional de ser seguro. Obviamente esta cualidad debería ser exigible en cualquier desarrollo de software actual. Sin embargo, lamentablemente los aspectos de seguridad no son tenidos en cuenta y las vulnerabilidades de los sistemas aumentan cada día más.

Las Competencias de la asignatura se pueden consultar en la guía del máster.

3.REQUISITOS PREVIOS RECOMENDABLES

La formación previa que deberían tener los alumnos para el adecuado seguimiento de esta asignatura son los propios de ingreso al posgrado, haciendo especial recomendación en conocimientos de ingeniería de software y lenguajes de programación.

Se recomienda que el alumno tenga preferiblemente alguna experiencia previa de programación con lenguajes C y C++.

Además es necesario dominar el inglés técnico (leer y escribir) para manejar con facilidad las fuentes bibliográficas.

4.RESULTADOS DE APRENDIZAJE

La asignatura está enfocada al desarrollo y mantenimiento de software seguro y sin vulnerabilidades. Por tanto, los resultados de aprendizaje que se espera que el estudiante pueda alcanzar son:

- Identificar las principales causas de vulnerabilidad conocidas y desarrollar el código seguro que las evite.
- Conocer y saber aplicar un conjunto de métodos, técnicas y herramientas que permitan probar que el software desarrollado cumple los requisitos de funcionalidad y seguridad.
- Aplicar métodos para verificar formalmente la corrección de componentes de software crítico seguro.
- Realizar, junto con las pruebas tradicionales, otras adicionales específicas de seguridad.
- Usar modelos de penetración, patrones de ataque, de abuso o mal uso del sistema en la fase de pruebas.
- Conocer los procedimientos y programas de mantenimiento de software para que continúe cumpliendo con los requisitos de funcionalidad y seguridad.

5.CONTENIDOS DE LA ASIGNATURA

Tema 1: Estudio de Vulnerabilidades

Los aspectos estudiados en este tema son los siguientes:

- Errores de programación más peligrosos según el CWE/SANS Top 25
- Conceptos de seguridad

Tema 2: Prácticas de Desarrollo

Los aspectos estudiados en este tema son los siguientes:

- Prácticas recomendadas:
  - El ciclo de vida del desarrollo seguro
  - Entrenamiento en seguridad
  - Requisitos
  - Diseño
  - Implementación
  - Verificación

Tema 3: Gestión de Memoria en C y C++

Los aspectos estudiados en este tema son los siguientes:

- Errores más comunes de gestión de memoria
  - Buffer overflow
  - Stack smashing
- Validación de entradas

Tema 4: Strings, Punteros y Manejo de Enteros

Los aspectos estudiados en este tema son los siguientes:

- Errores de manejo de strings
- Errores de overflow de enteros
- Subterfugios con punteros

Tema 5: Otras vulnerabilidades en C y C++

Los aspectos estudiados en este tema son los siguientes:

- Errores de formateado de Entrada/Salida de datos
- Errores de secuenciado de Entrada/Salida de datos
- Errores de manejo de ficheros
- Errores de concurrencia

6.EQUIPO DOCENTE

- DAVID JOSE FERNANDEZ AMOROS
- JOSE ANTONIO CERRADA SOMOLINOS

7.METODOLOGÍA

La docencia de esta asignatura se impartirá a distancia, siguiendo el modelo educativo propio de la UNED. El principal instrumento docente será la plataforma aLF en la que se habilitarán diversos foros para canalizar las consultas y comentarios.

Las actividades a realizar por parte del alumno se desglosan de la siguiente manera:

Actividades formativas	Horas
Estudio de contenidos	60
Tutorías	10
Actividades en la plataforma virtual	5
Trabajos individuales	30
Trabajos en equipo	15
Prácticas informáticas	30
Elaboración de informes	0
Resolución de casos	0

Además, el estudiante podrá realizar consultas al equipo docente a través del correo, teléfono y presencialmente en los horarios establecidos para estas actividades. Ver apartado de *Tutorización* en esta guía docente.

8.BIBLIOGRAFÍA BÁSICA

ISBN(13): 9780321822130
Título: SECURE CODING IN C AND C++ (Second Edition)
Autor/es: Robert C. Seacord ;
Editorial: ADDISON WESLEY

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9781439826966

Título: SECURE AND RESILENT SOFTWARE DEVELOPMENT
Autor/es: Mark S. Merkow And Lakshmikanth Raghavan ;
Editorial: CRC Press

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

Comentarios y anexos:

Los dos libros están accesibles desde el portal de la UNED. Hay que autenticarse, y a partir de ahí.

- El libro de Seacord está aquí: (enlace). En este primer libro se estudian los aspectos generales relativos a todo el ciclo de vida del desarrollo de software seguro y sus particularidades.
- El libro de Merkow está aquí: (enlace). Este segundo libro está dedicado específicamente a estudiar las vulnerabilidades y las técnicas de programación segura en el lenguaje C y C++.

Hay un artículo que forma parte de la biblografía recomendada:

- Tsipenyuk, Katrina; Chess, Brian & McGraw, Gary. *Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors.* IEEE Security & Privacy, 2005

Este artículo se utiliza para clasificar los ciberataques y está disponible en la plataforma aLF de la asignatura.

9.BIBLIOGRAFÍA COMPLEMENTARIA

Comentarios y anexos:

Aunque no se consideran necesarios para el estudio de la asignatura, los libros y documentos de esta bibliografía complementaria pueden ser muy interesantes para un estudio en mayor profundidad de la asignatura. La relación de documentos se incluye en la parte 2 de esta guia de la asignatura.

10.RECURSOS DE APOYO AL ESTUDIO

Se ofrecerán las herramientas necesarias para que, tanto el equipo docente como el alumnado, encuentren la manera de compaginar el trabajo individual y el aprendizaje cooperativo (Skype, Moodle, Alf, etc.) si este se considerará necesario.

11.TUTORIZACIÓN Y SEGUIMIENTO

La tutorización de los alumnos se llevará a cabo fundamentalmente a través de la plataforma aLF. Además se puede utilizar el correo electrónico y las consultas telefónicas:

Profesor: *David Fernández Amorós*

Horario: Jueves de 16:00 a 20:00

david@issi.uned.es,

Teléfono: 91 398 8241

Profesor: *José Antonio Cerrada*

Horario: Jueves de 16:00 a 20:00

jcerrada@issi.uned.es,

Teléfono: 91 398 6478

También es posible una asistencia personalizada (preferentemente previo aviso) en los días y horas de tutorización en la siguiente dirección:

Dpto. de Ingeniería de Software y Sistemas Informáticos

ETSI Informática, UNED

C/ Juan del Rosal, 16

28040 MADRID

12.EVALUACIÓN DE LOS APRENDIZAJES

Para evaluar los conocimientos adquiridos, el alumno deberá realizar una Prueba de Evaluación a Distancia (PEC) que determinará el 30% de la nota final de la asignatura junto con un examen que determinará el 70% restante de la nota. La PEC constará de una actividad práctica informática consistente en la elaboración de un sistema de complejidad media. El alumno aplicará sus conocimientos para comprobar las vulnerabilidades del desarrollo y cómo se puede mejorar su diseño e implementación para hacerlo seguro. Todos los desarrollos se realizarán con herramientas libres y disponibles en internet para los lenguajes más habituales: C/C++, Java etc. Se valorará de manera especial la realización completa de todo el proyecto.

13.COLABORADORES DOCENTES

Véase equipo docente.