Universidad Zaragoza

Year : 2019/20

30227 - IT Security

Syllabus Information

Academic Year: 2019/20
Subject: 30227 - IT Security
Faculty / School: 110 - Escuela de Ingeniería y Arquitectura
326 - Escuela Universitaria Politécnica de Teruel
Degree: 443 - Bachelor's Degree in Informatics Engineering
439 - Bachelor's Degree in Informatics Engineering
ECTS: 6.0
Year: 4
Semester: 439 - First semester
439 - First semester
439 - First semester
439 - First semester
439 - First semester
439 - First semester
439 - First semester
439 - First semester
439 - First semester
439 - First semester
443 - First semester
443 - First semester
443 - First semester
443 - First semester
Subject Type: Compulsory
Module: ---

1.General information

1.1.Aims of the course

In previous courses, students have learned the concepts of different areas of computer science (programming, networks, operating systems, systems administration, distributed systems, ...).
Concerning security aspects, the courses of systems administration and distributed systems have introduced some basic concepts and mechanisms.
This course consolidates the security concepts, previously introduced, and considers the main issues in security field in a comprehensive manner for the development of secure software systems.

1.2.Context and importance of this course in the degree

Computer security is a course that integrates and widens knowledge acquired in previous courses such as "Distributed Systems" and "Systems Administration".
In addition, it provides a support for the knowledge acquired in the rest of computer courses, since security aspects are widespread in most of them.
It provides essential knowledge for use of the current Information Technologies.

1.3.Recommendations to take this course

It is recommended to have previously acquired a level of knowledge equivalent to that obtained with the courses of System Administration, Operating Systems, Computer Networks, Distributed Systems, Databases, and Programming.

2.Learning goals

2.1.Competences

Problem solving and decision making with initiative, creativity and critical reasoning.

Information management, management and application of the technical specifications and the legislation necessary to the practice of Engineering.

To design, develop, select and evaluate applications and computer systems, ensuring their reliability, security and quality, in accordance with ethical principles and current legislation and regulations.

To define the technical specifications of a computer installation that meets the current standards and regulations.

To analyze, design, build and maintain applications in a robust, secure and efficient way, choosing the paradigm and the most suitable programming languages.

2.2.Learning goals

To know the basics of computer security in its organizational aspect and implementation in systems, networks, databases and software.

To acquire the ability to design a comprehensive computer security model for an organization, following a proper methodology.
To master different tools that provide support to the adopted methodology in the different stages of the software development.

To be able to evaluate the security of a computer system and its applications.
To understand and know how to apply the different norms and standards in computer security, as well as the related legislation.

2.3.Importance of learning goals

Computer security is nowadays an essential aspect of information technology, given the current wide dependence of the human activity on computer systems.

3.Assessment (1st and 2nd call)

3.1.Assessment tasks (description of tasks, marking system and assessment criteria)

In the Escuela de Ingeniería y Arquitectura de Zaragoza (EINA):

According to the evaluation regulations approved by the School of Engineering and Architecture (EINA), the evaluation of the course will follow a global evaluation procedure.

The global evaluation of the course consists of three parts:

- Written exam with problems, conceptual questions or exercises. A minimum grade of 4.0 points is required in the written exam to pass the course. The grade obtained in this part weighs 50% of the grade of the course.
- Practice in the laboratory. Assessment criteria: compliance of the solutions to the specifications, quality of the design and time devoted to the practice work. A minimum grade of 4.0 points is required in the practice in the laboratory to pass the course. The grade obtained in this part weighs 25% of the grade of the course. Students who need to obtain the minimum grade required or simply improve their grade in this part, can have a global practice exam that will be held the same day as the written exam.
- Project and/or defense of the project that deepens a topic among those proposed by the teaching staff. Assessment criteria: capacity for analysis, synthesis and originality of the work. A minimum grade of 4.0 points is required in the work to pass the course. The obtained grade weighs 25% of the grade of the course.

The final grade obtained in a given call is the weighted sum of the grades in the three parts, being limited to 4 points out of 10 in the case of not reaching a 4 out of 10 in each of them.

In the Escuela Universitaria Politécnica de Teruel:

The global evaluation of the course consists of two parts:

- Written exam with problems, conceptual questions, or exercises. A minimum grade of 4.0 points is required in the written exam to pass the course. The grade obtained in this exam weighs 60% of the grade of the course.
- Practice in the laboratory. Assessment criteria: compliance of the solutions to the specifications, quality of the design and time devoted to the practice work. A minimum grade of 4.0 points is required in the practice in the

laboratory to pass the course. The grade obtained in this part weighs 40% of the grade of the course. Students who need to obtain the minimum grade required or simply improve their grade in this part, can have a global practice exam that will be held the same day as the written exam.

4.Methodology, learning tasks, syllabus and resources

4.1.Methodological overview

The learning process of this course is designed upon:

The learning of concepts and methodologies for the correct design of systems, programs and databases, though on-site classe

The application of such concepts in the problem class to solve different situations and tasks of computer security.

In the lab classes, the student will implement different aspects of risk analysis, specification, design and implementation of secu

The development of a project to deepen a topic among those proposed by the teaching staff (in the School of Engineering and Architecture of Zaragoza).

4.2.Learning tasks

The presentation of the syllabus in the on-site classes.

Problem-solving applying the concepts and techniques presented in the syllabus during problem classes.

Development of lab sessions, in a computing facility, to apply the theory in a real environment.

Tutoring sessions to supervise the development of the project and/or its defence (in the School of Engineering and Architecture of Zaragoza).

4.3.Syllabus

The course will address the following topics:

- Foundations: Risks, threats, vulnerabilities and attacks. Secure design principles. Authentication and authorization. Standards, regulations and laws.
- Computer security: Security models. Access control. Unix security. Security-Enhanced Linux.
- Network security: Design principles. Firewalls. Virtual private networks. Intrusion detection systems.
- Confidence management and input validation.
- Database security.
- Web security.
- Security audits.

4.4.Course planning and calendar

The schedule for the class is as follows:

In the Escuela de Ingeniería y Arquitectura de Zaragoza (EINA):

On-site and problem classes (3 hours weekly)

Lab sessions (2 hours every other week). Those are tutored sessions in which students carry out practice work in small groups

Tutoring sessions to supervise the development of the project and/or its defense according to the calendar defined by the teaching staff.

In the Escuela Universitaria Politécnica de Teruel:

Type 1 activities (on-site classes) 2 hours weekly 1 group

Type 2 activities (participative character classes) 1 hour weekly 2 groups

Type 2 activities (lab sessions) 1 hour weekly

Student work

To achieve the learning goals, students are assumed to spend 150 hours distributed as follows.

56 hours, roughly, on-site activities:

- class (theory and problems) and lab sessions
- tutoring sessions (in the Escuela de Ingeniería y Arquitectura de Zaragoza)

91 hours of self effective study:

- study of teaching material, problem solving, class and lab preparation, and programming
- project development (in the Escuela de Ingeniería y Arquitectura de Zaragoza)

3 hours dedicated to exams

4.5.Bibliography and recommended resources

[BB: Bibliografía básica / BC: Bibliografía complementaria]

Zaragoza:

http://psfunizar7.unizar.es/br13/egAsignaturas.php?codigo=30227&Identificador=14678

- [BB] Viega, John. Building secure software : how to avoid security problems the right way / John Viega, Gary McGraw Boston : Addison-Wesley, cop. 2002
- [BB] Anderson, Ross J. Security engineering : a guide to building dependable distributed systems / Ross J. Anderson . - 2nd ed. Indianapolis (Indiana) : Wiley, cop. 2008
- [BB] Huseby, Sverre H. Innocent code : a security wake-up call for Web programmers / Sverre H. Huseby Chinchester (England) : John Wiley & Sons, cop. 2004
- [BB] Goodrich, Michael T. Introduction to computer security / Michael Goodrich, Roberto Tamassia . Harlow : Pearson, cop. 2014
- [BB] Pfleeger, Charles P. Security in computing / Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies . Fifth edition. Upper Saddle River, NJ : Prentice Hall, 2015
- [BB] Wenliang Du. Computer Security: A Hands-on Approach, CreateSpace Independent Publishing Platform, 2017, ISBN: 978-1548367947
- [BC] Kaufman, C . Network Security / C. Kaufman, R. Perlman, and M. Speciner, . Second Edition Prentice Hall, 2002

Teruel:

http://psfunizar7.unizar.es/br13/egAsignaturas.php?codigo=30227&Identificador=13598

- [BB] Anderson, Ross J.. Security engineering : a guide to building dependable distributed systems / Ross J. Anderson . 2nd ed. Indianapolis (Indiana) : Wiley, cop. 2008
- [BB] Goodrich, Michael T.. Introduction to computer security / Michael Goodrich, Roberto Tamassia . Harlow : Pearson, cop. 2014
- [BB] Huseby, Sverre H.. Innocent code : a security wake-up call for Web programmers / Sverre H. Huseby . Chinchester (England) : John Wiley & Sons, cop. 2004
- [BB] KAUFMAN, Ch. Network Security / Charles Kaufman, Radia Perllman, Mike Speciner. New Jersey : Prentice Hall,
- [BB] Pfleeger, Charles P.. Security in computing / Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies . Fifth edition Upper Saddle River, NJ : Prentice Hall, 2015
- [BB] Viega, John. Building secure software : how to avoid security problems the right way / John Viega, Gary McGraw . Boston : Addison-Wesley, cop. 2002