VNIVERSITAT DE VALÈNCIA

Course Guide
34681 Computer Security

COURSE DATA

Data Subject	
Code	34681
Name	Computer Security
Cycle	Grade
ECTS Credits	6.0
Academic year	2019 - 2020

Study (s)

Degree	Center	Acad. year	Period
1400 - Degree in Computer Engineering	School of Engineering	3	Second term
1407 - Degree in Multimedia Engineering	School of Engineering	4	Second term

Subject-matter

Degree	Subject-matter	Character
1400 - Degree in Computer Engineering	14 - Operating systems, distributed systems and networks	Obligatory
1407 - Degree in Multimedia Engineering	19 - Optatividad	Optional

Coordination

Name	Department
PEREZ CONDE, CARLOS	240 - Computer Science
SORIANO GARCIA, FRANCISCO R	240 - Computer Science

SUMMARY

Computer Security is an essential component of a computer system. Security requirements can change very quickly. On the one hand, computing dependence for daily life tasks is rapidly increasing. This brings increasing demands and expectations that indeed include security aspects, such as privacy or security in commercial transactions. On the other hand, new technologies are constantly emerging. Although these allow the construction of more sophisticated security mechanisms, they also permit the realization of more sophisticated attacks.

In this context, the subject “Computer Security” attempts to provide an overview of the essential security elements in a computer system. The contents focus on fundamental principles, and aims at teaching the student to be able to decide on and apply the most appropriate tools and techniques to accomplish the security requirements of a computer system.

The course relies on previous contents introduced in the subjects of networking, operating systems, databases and programming. These are extended with other contents related to computer security, such as security policies, vulnerability assessment, intrusion detection or forensic analysis.

“Computer Security" is taught in the second semester of the third year, as part of the module "Operating Systems, Distributed Systems and Networks."

PREVIOUS KNOWLEDGE

Relationship to other subjects of the same degree

There are no specified enrollment restrictions with other subjects of the curriculum.

Other requirements

It is recommended that the student has completed the following subjects: Programming, Data Structures and Algorithms, Operating Systems and Computer Network Architecture. Among them, the last two are particularly relevant. They address some security-related concepts that are extended in this course.

OUTCOMES

1400 - Degree in Computer Engineering

- G3 - Ability to design, develop, evaluate and ensure the accessibility, ergonomics, usability and security of computer systems, services and applications, and of the information that these manage.
- G4 - Ability to define, evaluate and select hardware and software platforms for the development and implementation of computer systems, services and applications, in accordance with both the knowledge and the specific skills acquired in the degree.
- G6 - Ability to design and develop computer systems and centralised or distributed computer architectures which integrate hardware, software and networks, in accordance with both the knowledge and the specific skills acquired in the degree.
- R1 - Ability to design, develop, select and evaluate computer applications and systems while ensuring their reliability, safety and quality, according to ethical principles and current legislation and regulations.
- R5 - Knowledge, management and maintenance of computer systems, services and applications.
- TI2 - Ability to select, design, implement, integrate, evaluate, build, manage, exploit and maintain hardware, software and network technologies, within adequate cost and quality thresholds.
- TI7 - Ability to understand, implement and manage the security and safety of computer systems.

- SI2 - Ability to determine the requirements of an organisations information and communication systems, considering safety aspects and compliance with regulations and legislation.

LEARNING OUTCOMES

- Design and evaluate the security policy of an organization, including both the previous analysis and management of security incidents.
- Design, implement, maintain and evaluate the security mechanisms needed to ensure compliance with the security policy.
- Design, implement, maintain and evaluate mechanisms to detect incidents and to address them properly.
- Evaluate new products and technologies and, where appropriate, apply them to maintain the level of security required.
- Coordinate with other technical professionals (system administrators, network, database,applications ...) to ensure proper operation of computer systems.
- Adequately report security incidents, and interpret properly the security alerts released by others.
- Explain the benefits of adopting security measures to both users and managers.

DESCRIPTION OF CONTENTS

1. Introduction

Security concept
What do we want to protect and why? Security Policy
What do we protect against? Risks and vulnerabilities
The security process
Regulations (ethics, law and standards, ISACA, ISO 27000, IS2)

2. Security mechanisms

This unit consists of three chapters:
- Cryptography (3 hours TP)
Symmetric cryptography
Public key cryptography
Hashes
- Host based security
Validation and authentication
Access Control
Secure programming
Server and client security
- Perimeter Security
Basic technologies
Firewall Architectures
Application Firewalls

3. Intrusion Detection and Response

Host Intrusion Detection Systems (HIDS)
Network Intrusion Detection Systems (NIDS)
Honeypots and Honeynets
Forensic Analysis

4. Audit and ethical hacking

Introduction to the audit process
Penetration tests
Phases of an attack/pentest
Tools for ethical hacking

WORKLOAD

ACTIVITY	Hours	% To be attended
Theory classes	30,00	100
Laboratory practices	20,00	100
Classroom practices	10,00	100
Development of group work	10,00	0
Study and independent work	20,00	0
Readings supplementary material	10,00	0
Preparation of evaluation activities	20,00	0
Preparing lectures	20,00	0
Preparation of practical classes and problem	10,00	0
TOTAL	**150,00**	

TEACHING METHODOLOGY

Activities will be conducted according to the following distribution:

• Theoretical activities. During theory lectures, the key and most complex aspects will be explained in detail. Student participation will be promoted

• Practical activities. They complement the theoretical activities. These include the following: exercise based lectures, discussion sessions, labs and scheduled tutorials. During the practical activities, students will apply the foundations of computer security to solve a range of practical challenging problems.

• Student's individual work. This includes the realization (outside the classroom) of monographs, literature research, questions, problems, and the preparation of classes and exams (study). These are done individually and attempt to promote autonomous learning.

• Team-Work in small groups. Team work done in small groups (2-4) outside the classroom. This type of activity attempts to develop team work skills.

EVALUATION

FIRST CALL

The subject may be evaluated in two ways. In the first scheme, both in-class quizzes and the final quiz have a weight in the final mark. In the second scheme, in-class quizzes do not compute. The final grade will be the greater of the grades obtained by using the two schemes.

In the first call the course grade will be composed of the following:

- Evaluation of theory and problems (TP). This part will account for 75% of the final grade. The student will need to obtain a minimum of 4.5 points out of 10 to be able to pass the module. Otherwise the module will be failed. The mark for this part will depend on student participation and three quizzes taken along the course. These are detailed below:

  - The Continuous Evaluation (EC) component is based on the student’s participation and involvement in the teaching-learning process. Both regular attendance and in-class activities are considered. This part cannot be recovered.
  - Quizzes. These consist of two in-class quizzes which will be conducted in the first half of the semester (called T1) and during the second half of the semester (T2), and one final quiz that will conducted outside school hours during the exam period (called T3).

Each of these tests will address all of the subject content taught until the quiz date.

To avoid penalizing students who perform better in the final quiz than in the other in-class tests, TP is calculated as follows:

TP = Maximum(0.15 * CE + 0.15 * T1 + 0.25 * T2 + 0.45 * T3, 0.15 *CE + 0.85 * T3)

- Evaluation of the laboratory activities (L), which depends on the achievement of objectives in the laboratory sessions.

Labs are carried out in pairs. Laboratory grade accounts for 25% of the final grade. As with TP, it will be necessary to obtain a minimum of 4.5 points out of 10 to be able to pass the module. Otherwise the module will be failed. All lab sessions will have the same weight on the final grade.

Were some student unable to attend a session, lab work should be submitted to the lab instructor before the laboratory session is held. Delivery shall be in person, during tutorial hours. The student should be prepared to answer questions about the work and to re-do parts of it in real-time (with minor changes). This type of delivery will be penalized by subtracting 20% of the grade obtained.

The algorithm used to compute the final grade is given below:

If TP <4.5 or L <4.5

final_grade = Minimum (TP, L)

In another case:

final_grade = 0.75 * TP + 0.25 * L

SECOND CALL

For the second call, a delivery period to submit laboratory work will be opened. Students should submit laboratory work in person, during tutorial hours. The student should be prepared to answer questions about the work and to re-do parts of it in real-time (with minor changes). A grade penalty of 30% will apply for this type of submission.

A final examination (FE) will be also be held and this exam will substitute the T3 test.

Except for these two differences, the module will be evaluated in the same way as in the first call (the EC mark will be the same as in the first call).

To apply for an advance call, students must have previously taken the course and have obtained the minimum mark required in assessing the practical laboratory activities (L). In this way, it is attempted to reconcile the right of students to an advance call with the subject's teaching methodology and evaluation criteria.

In any case, the evaluation of this subject will be done in compliance with the University Regulations in this regard, approved by the Governing Council on 30th May 2017 (ACGUV 108/2017).

REFERENCES

Basic

- Charles P. Pfleeger; Shari Lawrence Pfleeger; Jonathan Margulies. Security in Computing, Fifth Edition. Prentice Hall, 2015. ISBN-13: 978-0-13-408504-3.
- Stephen Northcutt et altres, Inside Network Perimeter Security. Sams; 2005, ISBN-13: 978-0672327377.

Additional

- Elizabeth D. Zwicky et altres, Building Internet Firewalls, O'Reilly Media, Inc 2nd edition;2000, ISBN-13: 978-1-56592-871-8
- C. Pogue et altres, Unix and Linux Forensic Analysis DVD Toolkit. Syngress; 2008, ISBN-13: 978-1597492690
- John Vacca, Computer and Information Security Handbook, 2nd Edition, Morgan Kaufmann, 2012, ISBN-13: 978-0-12-394397-2
- B. Carrier, File system forensic analisys, Addison-Wesley Professional; 2005, ISBN-13: 978-0321268174
- Lance Spitzner, Honeypots: tracking hackers, Addison-Wesley Professional, 2002, ISBN-13: 978-0321108951
- D. Farmer, W. Venema, Forensic Discovery, Addison-Wesley Professional; 2005, ISBN-13: 978-0201634976
- Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. John Wiley & Sons, 1996. ISBN: 978-0-471-11709-4

ADDENDUM COVID-19

This addendum will only be activated if the health situation requires so and with the prior agreement of the Governing Council

1. Contenidos

Sin cambios.

2. Volumen de trabajo y planificación temporal de la docencia

Se mantiene, en la medida de lo posible, el volumen de trabajo, sustituyendo las sesiones presenciales por videos de apoyo para la explicación de contenidos y la realización de demostraciones prácticas, y por foros específicos de Aula Virtual para discusión y resolución de dudas.

La planificación temporal se mantiene a nivel semanal, aunque se han sustituido las actividades presenciales por actividades asíncronas (videos, foros y trabajo con máquinas virtuales).

3. Metodología docente

Las actividades presenciales de teoría se sustituyen por presentaciones locutadas, videos con demostraciones y videos de resolución de problemas y casos prácticos. Además, se habilita un foro específico por tema para fomentar la discusión reflexiva y resolver dudas, completando así el aprendizaje.

Las actividades presenciales de laboratorio incluyen un guion detallado que puede llevarse a cabo usando la máquina virtual de la asignatura. Como con la teoría, se habilita un foro por práctica para fomentar la discusión reflexiva y resolver dudas, como forma de completar el aprendizaje.

4. Evaluación

Modificaciones:

- Se elimina la prueba T2.
- Se aumenta el peso de la evaluación continua (EC) dentro de la parte de teoría y práctica (TP), pasando al 25% de TP.
- Se aumenta el peso de la prueba T1, realizada presencialmente, pasando al 25% de TP.
- Se aumenta el peso de las prácticas de laboratorio (L), pasando al 30% de la nota final (NF).
- Se cambia el examen T3 (examen final) a modalidad no presencial, formado por cuestionarios en Aula Virtual que incluirán preguntas tipo test, de respuesta breve y de resolución de problemas y/o casos prácticos. Las preguntas no serán necesariamente las mismas para todo el alumnado y se podrán establecer franjas de tiempo separadas para diferentes partes de la prueba (por ejemplo, para el test y para las cuestiones). En caso de considerarlo necesario, el profesorado podrá requerir una entrevista personal telemática para que la o el estudiante pueda justificar sus respuestas y demostrar sus conocimientos.
- Se cambia la realización presencial de las prácticas de laboratorio (L) por la entrega de una memoria explicativa del trabajo realizado, que debe acompañar al resto de evidencias ya solicitadas (programas, ficheros de configuración…).

Con estas modificaciones, el cálculo de la nota final (NF) se realizará de la siguiente forma:

TP = Máximo(0,25*EC+0,25*T1+0,5*T3; 0,25*EC+0,75*T3)

L continúa siendo la media aritmética de las 8 sesiones de laboratorio.

Si TP o L < 4,5, NF es el mínimo de las dos.

Si TP y L >= 4,5, NF = 0,7*TP + 0,3*L

En 2ª convocatoria se repetirá el examen T3. Adicionalmente, se permitirá la entrega en línea de prácticas de laboratorio hasta el día de la 2ª convocatoria. Esta entrega tendrá una penalización del 30%.

5. Bibliografía

Ya se utilizaban libros y referencias electrónicas, por lo que no ha sido necesario hacer cambios.