VNIVERSITAT DE VALÈNCIA

Course Guide
34896 Computer Security

COURSE DATA

Data Subject	
Code	34896
Name	Computer Security
Cycle	Grade
ECTS Credits	6.0
Academic year	2019 - 2020

Study (s)

Degree	Center	Acad. year	Period
1403 - Degree in Telematics Engineering	School of Engineering	3	Second term

Subject-matter

Degree	Subject-matter	Character
1403 - Degree in Telematics Engineering	16 - Management of systems	Obligatory

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.

"Information Security" is taught in the second semester of the third year, as part of the module "Computer Systems Administration".

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: Computer Science, Advanced Computer Science, 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

COMPETENCES (RD 1393/2007) // LEARNING OUTCOMES (RD 822/2021)

1403 - Degree in Telematics Engineering

- R1 - Ability for self-learning of new knowledge and techniques appropriate for the conception, development and exploitation of telecommunications systems and services.
- G4 - Ability to solve problems with initiative, decision-making and creativity, and to communicate and transmit knowledge, abilities and skills, understanding the ethical and professional responsibility of the activity of a telecommunications technical engineer.
- E1 - Ability to construct, exploit and manage telecommunication networks, services , processes and applications, understood as systems for the acquisition, transport, representation, processing, storage, management and presentation of multimedia information, from the perspective of telematics services.
- E2 - Ability to apply the techniques under the telematic networks, services and applications, such as management systems, signaling and switching, routing, security (cryptographic protocols, tunneling, firewall, collecting mechanisms, authenticating and protecting contents), traffic engineering (graph theory, queuing theory and teletraffic) pricing and reliability and quality of service, in fixed, mobile, personal, local or long distance environments, with different bandwidths, and including telephony and data.

- E3 - Ability to construct, operate and manage telematic services using analytical tools for planning, dimensioning and analysis.

LEARNING OUTCOMES (RD 1393/2007) // NO CONTENT (RD 822/2021)

- Design and evaluate the security policy of an organization, including both the previous analysis and management of security incidents G-4, E-2).
- Design, implement, maintain and evaluate the security mechanisms needed to ensure compliance with the security policy G-4, R-1, E-2).
- Design, implement, maintain and evaluate mechanisms to detect incidents and to address them properly G-4, E-2).
- Evaluate new products and technologies and, where appropriate, apply them to maintain the level of security required G-4, R-1, E-2).
- Coordinate with other technical professionals (system administrators, network, database, applications ...) to ensure proper operation of computer systems G-4, E-2).
- Adequately report security incidents, and interpret properly the security alerts released by others G-4, E-2).
- Explain the benefits of adopting security measures to both users and managers G-4, E-2).

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:
A- Cryptography
-- Symmetric cryptography
-- Public key cryptography
-- Hashes
-- Lab
B- Host based security
-- Validation and authentication
-- Access Control
-- Secure programming
-- Server and client security
-- Lab
C- Perimeter Security

-- Basic technologies
-- Firewall Architectures
-- Application Firewalls
-- Lab

3. Intrusion Detection and Response

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

4. Audit and Ethical Hacking

Introduction to the audit process
The penetration test and types
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 (E-2).
- 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 (G-4, E-2).
- 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. (G-4, R-1, E-2).
- 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 (G-4, R-1, E-2).

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 is not recoverable. (G-4, R-1, E-2)
- 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). (G-4, E-2)

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(0.20 * CE + 0.1 * T15 + 0.25 * T2 + 0.4 * T3, 0.25 *CE + 0.75 * T3)

- Evaluation of the laboratory activities (L), which depends on the achievement of objectives in the laboratory sessions. (G-4, E-2)

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 = 0.80 * TP + 0.20 * 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 the final grade mark will be calculated as:

If FE <4.5 or L <4.5

final_grade = Minimum (FE, L)

In another case:

final_grade = 0.75 * FE + 0.25 * L

For the part EC it will be maintained the student mark.

Advance 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 system of evaluation will be ruled by the established in the Regulation of Evaluation and Qualification of the University of Valencia for Degrees and Masters. (http://www.uv.es/graus/normatives/2017_108_Reglament_avaluacio_qualificacio.pdf).

REFERENCES

Basic

- Referencia b1: Charles P.Pfleeger et altres, Security in Computing, Fifth Edition, Prentice Hall, 2015, ISBN-13: 978-0-13-408507-4
- Referencia b2: Stephen Northcutt et altres, Inside Network Perimeter Security. Sams; 2005, ISBN-13: 978-0672327377
- Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition.John Wiley & Sons, 1996. ISBN: 978-0-471-11709-4

Additional

- Referencia c1:Elizabeth D. Zwicky et altres, Building Internet Firewalls, O'Reilly Media, Inc 2nd edition;2000, ISBN-13: 978-1-56592-871-8
- Referencia c2: C. Pogue et altres, Unix and Linux Forensic Analysis DVD Toolkit. Syngress; 2008, ISBN-13: 978-1597492690
- Referencia c3: John Vacca, Computer and Information Security Handbook, 2nd Edition, Morgan Kaufmann, 2012, ISBN-13: 978-0-12-394397-2
- Referencia c4: B. Carrier, File system forensic analysis, Addison-Wesley Professional; 2005, ISBN-13: 978-0321268174
- Referencia c5:Lance Spitzner, Honeypots: tracking hackers, Addison-Wesley Professional, 2002, ISBN-13: 978-0321108951
- Referencia c6: D. Farmer, W. Venema, Forensic Discovery, Addison-Wesley Professional; 2005, ISBN-13: 978-0201634976

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

Se mantienen los contenidos inicialmente recogidos en la guía docente

2. Volumen de trabajo y planificación temporal de la docencia

Mantenimiento del peso de las distintas actividades que suman las horas de dedicación en créditos ECTS marcadas en la guía docente original

3. Metodología docente

A principios de la semana se proponen las transparencias que deben ser revisadas por los alumnos. Se pone posteriormente en un foro unas cuantas preguntas o problemas para comprobar si se han entendido los conceptos principales. Al finalizar la semana el profesor indica la respuesta correcta y los errores cometidos.

Además, se cuelga un video locutado de algunas transparencias y se realizan algunas pruebas de examen online con carácter no puntuable.

Todas las prácticas de laboratorio se pueden hacer desde casa usando la máquina virtual NETinVM.

Para tutorías, vía e-mail a cualquier hora, uso de aula virtual y foros.

Todas las tareas de cada semana están puestas el lunes a primera hora y deben ser realizadas hasta sábado a última hora.

4. Evaluación

Criterio de evaluación único:

02EC + 0,15T1 + 0,2T3 + 0,45Lab

Se ha pasado peso de examen T3 a Lab. Los otros apartados ya estaban hechos antes de la interrupción de clases presenciales.

Además, alternativamente el examen T3 puede ser sustituido por Trabajo individual para alumnos que indiquen problemas de recursos de hardware o de red. Si una persona no dispone de los medios para establecer esta conexión y acceder al aula

virtual, deberá contactar con el profesorado por correo electrónico en el momento de publicación de este anexo a la guía docente

No hay nota mínima en ningún apartado.

Para segunda convocatoria:

Se pueden volver a entregar todos o algunos laboratorios (Lab) y realizar un nuevo examen (T3) o trabajo y desaparece el T1 siendo el nuevo criterio de evaluación:

02EC + 0,2T3 + 0,6Lab

5. Bibliografía

La bibliografía recomendada se mantiene