Course guide
270123 - SI - Computer Security

Last modified: 30/01/2024

Unit in charge: Barcelona School of Informatics
Teaching unit: 701 - DAC - Department of Computer Architecture.

Degree: BACHELOR'S DEGREE IN INFORMATICS ENGINEERING (Syllabus 2010). (Optional subject).

Academic year: 2023 **ECTS Credits:** 6.0 **Languages:** Catalan, Spanish

LECTURER

Coordinating lecturer: RENÉ SERRAL GRACIÀ

Others:

Primer quadrimestre:
ROBERTO BARREDA ORENGA - 11, 13
DAVIDE CAREGLIO - 12
RENÉ SERRAL GRACIÀ - 11, 12, 13

Segon quadrimestre:
ROBERTO BARREDA ORENGA - 11, 12
MARC CATRISSE I PÉREZ - 11, 12

PRIOR SKILLS

Those obtained at the Operating Systems and Computer Networks subjects.

Knowledge of technical English.

REQUIREMENTS

- Pre-Corequisite SO
- Pre-Corequisite XC

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
CT6.4. To demonstrate knowledge and capacity to apply the characteristics, functionalities and structure of the Distributed Systems and Computer and Internet Networks guaranteeing its use and management, as well as the design and implementation of application based on them.
CT7.1. To demonstrate knowledge about metrics of quality and be able to use them.
CT7.2. To evaluate hardware/software systems in function of a determined criteria of quality.
CT7.3. To determine the factors that affect negatively the security and reliability of a hardware/software system, and minimize its effects.
CT8.1. To identify current and emerging technologies and evaluate if they are applicable, to satisfy the users needs.
CTI1.1. To demonstrate understanding the environment of an organization and its needs in the field of the information and communication technologies.
CTI1.2. To select, design, deploy, integrate and manage communication networks and infrastructures in a organization.
CTI1.3. To select, deploy, integrate and manage information system which satisfy the organization needs with the identified cost and quality criteria.
CTI2.3. To demonstrate comprehension, apply and manage the reliability and security of the computer systems (CEI C6).
CTI3.1. To conceive systems, applications and services based on network technologies, taking into account Internet, web, electronic commerce, multimedia, interactive services and ubiquitous computation.

Generical:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

TEACHING METHODOLOGY

This course should give an overview and a technical view of the problems and possible solutions to computer systems and networks security. For this reason, it covers many topics and has a great descriptive component.

However, the teaching methodology will use examples and problems for introducing the concepts to which students attain the necessary skills. Also, we will try to encourage interactivity with students considering real situations in class to discuss possible solutions.

Moreover, the laboratory will complete the skills and knowledge acquired in theory / problems class.

LEARNING OBJECTIVES OF THE SUBJECT

1.Being able to understand the threats and security risks of computer systems.
2.Being able to analyze malicious code such as viruses, Trojans, etc..
3.Being able to understand and identify mechanisms for access control of an operating system.
4.Knowing the problems of security in computer networks and be able to find solutions to protect them.
5.Being able to design protection mechanisms for distributed applications.
6.Being able to understand the need and operation of forensic computer security mechanisms.
7.Being able to use cryptographic mechanisms to protect resources.
8.Being able to understand, design and implement public key infrastructure (PKI).
10.Being able to understand the mechanisms of protection and security policies.
11.Be able to manage the acquisition, structuring, analysis and visualization of data and information in the field of computer engineering, critically evaluating the results of this management.

STUDY LOAD

Type	Hours	Percentage
Guided activities	6,0	4.00
Hours small group	15,0	10.00
Hours large group	45,0	30.00
Self study	84,0	56.00

Total learning time: 150 h

CONTENTS

Introduction

Description:
Threats, risk analysis, protection mechanisms, security of communications, security forensics, politicies, recovery, legal aspects, ...

Cryptography

Description:
Basics of cryptography. Public key. Electronic signatures.

PKI Infrastructure

Description:
Certificates. Directories. Protocols.

Security in applications

Description:
Security on the web. Secure application protocols.

Security in operating systems

Description:
Threat analysis. Operation of malicious codes. Viruses and worms. Protection. virus. Structure of an OS.

Forensic analysis

Description:
Collection of evidence. Analysis.

ACTIVITIES

Development of theme 1. Introduction.

Description:
Learning the concepts and objectives associated with this item.

Specific objectives:
1, 10

Full-or-part-time: 5h
Theory classes: 1h
Self study: 4h

Development Topic 2. Cryptography.

Description:
Learning the concepts and objectives associated with this item.

Specific objectives:
7

Full-or-part-time: 18h
Theory classes: 6h
Practical classes: 4h
Self study: 8h

Development of item 3. Infrastructure PKI.

Description:
Learning the concepts and objectives associated with this item.

Specific objectives:
8

Full-or-part-time: 9h
Theory classes: 3h
Practical classes: 1h
Self study: 5h

Lab 1. Using digital certificates and apache (HTTPS)

Description:
Being able to create a X.509 certificate with openssl and install it on an Apache web server to configure HTTPS

Specific objectives:
8

Full-or-part-time: 6h
Laboratory classes: 2h
Self study: 4h

First theory exam

Description:
Theory exam of the following topics: Introduction, Criptography, PKI infrastructure and network security

Specific objectives:
1, 4, 7, 8, 10

Full-or-part-time: 7h 30m
Guided activities: 1h 30m
Self study: 6h

Development of item 4. Security applications.

Description:
Learning the concepts and objectives associated with this item.

Specific objectives:
5

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 25h
Theory classes: 6h
Practical classes: 4h
Self study: 15h

Lab 2. Vulnerabilities in web applications

Description:
Understanding the secure programming techniques described in the session. Understanding the webscarab and webgoat applications included in the OWASP linux distribution

Specific objectives:
1, 5

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 8h
Laboratory classes: 4h
Self study: 4h

Development of item 5. Security in operating systems.

Description:
Learning the concepts and objectives associated with this item.

Specific objectives:
2, 3

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 23h
Theory classes: 6h
Practical classes: 4h
Self study: 13h

Lab 5. Malware analysis

Description:
Understanding the different forms to analyze a malicious code. Being able to properly use the analysis tool IDAPro

Specific objectives:
1, 2

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 8h
Laboratory classes: 4h
Self study: 4h

Development issue 7. Security forensics.

Description:
Learning the concepts and objectives associated with this item.

Specific objectives:
6

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 8h
Theory classes: 3h
Practical classes: 2h
Self study: 3h

Lab 6. Investigation of a forensic case

Description:
Students will learn the basic procedures and methodologies that must be taken into account when performing a forensic analysis. It is also expected that after the lab you will increase your understanding of the forensic tools and applications needed to solve most of the security incidents where a digital evidence is involved.

Specific objectives:
6

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 6h
Laboratory classes: 2h
Self study: 4h

Lab CT. Solvent use of bibliographic resources

Description:
Manage the acquisition, structuring, analysis and visualization of data and information in the field of computer engineering, and critically evaluate the results of this management.
- Plan and use the information needed for an academic project (for example, for the final degree project) based on a critical reflection on the information resources used.
- Manage information competently, independently and autonomously.
- Evaluate the information found and identify the gaps.

Specific objectives:
11

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 4h
Laboratory classes: 2h
Self study: 2h

Questionnaire on the solvent use of bibliographic resources

Description:
Questionnaire on the solvent use of bibliographic resources

Specific objectives:
11

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 3h
Guided activities: 1h
Self study: 2h

Second theory exam

Description:
Theory exam of the subjects of the subject: Security in applications, security in operating systems and forensic analysis.

Specific objectives:
2, 3, 5, 6

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 7h 30m
Guided activities: 1h 30m
Self study: 6h

Final exam lab

Description:
Review on all laboratory practices carried out throughout the course.

Specific objectives:
2, 3, 4, 5, 7, 8

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 5h
Guided activities: 1h
Self study: 4h

Final exam

Description:
Exam exclusively for students who have taken both controls but have not passed the subject. The exam is mostly the syllabus.

Specific objectives:
1, 2, 3, 4, 5, 6, 7, 8, 10

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 7h
Guided activities: 1h
Self study: 6h

GRADING SYSTEM

1. A mid-term exam (C1) in the middle of the semester and a second exam at the end (C2) on the material exposed in the theory classes.
Theory = 0.5 x C1 + 0.5 x C2

2. Realization of labs:
2.1 The student will fullfill some personal tasks or individual questionnaires through Atenea (NQ)
2.2 There will be a laboratory exam (EL)
The laboratori grade will be computed through: Lab = 0.5 * NQ + 0.5 EL

3. Carrying out an individual activity dedicated to the transversal competence (TC) proposed by the theory and/or laboratory professors related to "Proper use of bibliographic resources"

The final mark (NF) of the subject will be calculated as follows:
NF = 0.7 x Theory + 0.25 x Lab + 0.05 x TC

There will not be a final exam. Nevertheless there is the possibility of repeating the first midterm during the second one, which will take place during the exam period alloted at the end of the semester.

The level of achievement of transversal competence is evaluated from the TC and will be calculated as follows:
A if TC >= 8.5; B if TC >=7; C if TC >= 5; D if TC

BIBLIOGRAPHY

Basic:
- Stallings, W. Network security essentials: applications and standards. 6th ed. Pearson Education, 2017. ISBN 9781292154916.
- Stallings, W. Cryptography and network security: principles and practice. 7th ed. Prentice Hall, 2017. ISBN 9781292158587.
- Stallings, W. Computer Security: Principles and Practice. 4th ed. Prentice Hall, 2018. ISBN 9781292220611.
- Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A. Handbook of applied cryptography. CRC Press, 1997. ISBN 0-8493-8523-7.
- Adams, C.; Lloyd, S. Understanding PKI: concepts, standards, and deployment considerations. 2nd ed. Addison-Wesley, 2003. ISBN 0-672-32391-5.

Complementary:
- Medina, M.; Molist, M. Cibercrimen : ¡protégete del Bit-Bang!, los ataques en el Ciberespacio a : tu ordenador, tu móvil, tu empresa... aprende de víctimas, expertos y CiberVigilantes. Barcelona: Tibidabo, 2015. ISBN 9788416204823.