DEGREE CURRICULUM

APPLICATIONS AND COMMUNICATIONS SECURITY

Coordination: OJEDA CONTRERAS, JESUS

Academic year 2022-23

APPLICATIONS AND COMMUNICATIONS SECURITY 2022-23

Subject's general information

Subject name	APPLICATIONS AND COMMUNICATIONS SECURITY
Code	102380
Semester	1st Q(SEMESTER) CONTINUED EVALUATION
Typology	<table><tr><th>Degree</th><th>Course</th><th>Character</th><th>Modality</th></tr><tr><td>Bachelor's degree in Digital Interaction and Computing Techniques</td><td>3</td><td>COMPULSORY</td><td>Attendance-based</td></tr></table>
Course number of credits (ECTS)	6
Type of activity, credits, and groups	<table><tr><th>Activity type</th><td>PRALAB</td><td>TEORIA</td></tr><tr><th>Number of credits</th><td>3</td><td>3</td></tr><tr><th>Number of groups</th><td>1</td><td>1</td></tr></table>
Coordination	OJEDA CONTRERAS, JESUS
Department	COMPUTER SCIENCE AND INDUSTRIAL ENGINEERING
Teaching load distribution between lectures and independent student work	6 ECTS = 25x6 = 150 hours of work 40% -> 60 in-class hours 60% -> 90 autonomous work hours
Important information on data processing	Consult this link for more information.
Language	Spanish / Catalan

APPLICATIONS AND COMMUNICATIONS SECURITY 2022-23

Teaching staff	E-mail addresses	Credits taught by teacher	Office and hour of attention
OJEDA CONTRERAS, JESUS	jesus.ojedacontreras@udl.cat	6	

Subject's extra information

For any doubt and/or question, you can send an email to the teacher of the subject.

Learning objectives

- Understand the concepts, problems and procedures of computer security
- Understand the main concepts and mechanisms of cryptography
- Understand and be able to do a risk analysis
- Design and configure firewall schemes

Competences

- CT3. Implement new technologies and information and communication technologies.
- CG2. Ability to design, develop, evaluate and guarantee the accessibility, ergonomics, usability and security of computer systems.
- CG3. Ability to use appropriate hardware and software platforms for the development and execution of interactive digital applications.
- CE7. Know, manage and maintain interactive computer systems, services and applications.
- CE12. Know and know how to apply the characteristics, functionality and structure of computer networks and the internet, and design and implement interactive applications based on them.

Subject contents

1. Fundamentals of information security
2. Cryptography
    - Hash functions (MD5, SHA)
    - Symmetric cryptography (DES, AES)
    - Asymmetric cryptography (RSA, ElGamal)
3. Security of the operating system
    - Sandboxing (chroot)
    - Firewalls (iptables)
4. Risks, vulnerabilities and attacks

Methodology

According to the schedule of the subject, each week the student attends 2 hours of Theory and 2 hours of laboratory (PRALAB).

The Theory sessions present the topics that can be consulted in the content section. They incorporate illustrative examples and problem proposals to solve in the laboratory classes.

PRALAB sessions are taught in the laboratory and present problems and discuss the proposed solutions. They can also present the practices of the subject and carry out the corresponding laboratory work.

APPLICATIONS AND COMMUNICATIONS SECURITY 2022-23

The student's autonomous work consists of solving the proposed exercises and the practical tasks when indicated.

The programming language used in class is Python. Virtual machines like VirtualBox will also be used.

Development plan

Week	Description	Theory Activity	PRALAB Activity	Automous work
1	Fundamentals	T1: Fundamentals	Python Review	Bibliography and program consultation, Python Review
2	Hash Functions	T2: Cryptography	Python, Presentation P1	P1, T2 problems
3	Hash Functions	T2: Cryptography	T2 problems	P1, T2 problems
4	Symmetric crypto	T2: Cryptography	P1	P1, T2 problems
5	Symmetric crypto	T2: Cryptography	T2 problems	P1, T2 problems
6	Asymmetric crypto	T2: Cryptography	P1	P1, T2 problems
7	Asymmetric crypto	T2: Cryptography	P1 - Delivery P1	T2 problems
8	Sandboxing	T3: SO Security	Doubts T1	T3 problems
9		1st Partial		Study
10	Sandboxing	T3: SO Security	Presentation P2	P2, T3 problems
11	Firewalls	T3: SO Security	P2, Problems T3	P2, T3 problems
12	Firewalls	T3: SO Security	P2	P2, T3 problems
13	Risks and Attacks	T4: Risks and Attacks	P2, Problems T4	P2, Problems T4
14	Risks and Attacks	T4: Risks and Attacks	Delivery P2	T4 problems
15	Risks and Attacks	T4: Risks and Attacks	Doubts T3 and T4	T4 problems
16/17		2nd Partial		Study
18				
19		Recovery		Study

Evaluation

Acr	Assessment activity	Weight	Minimum Grade	In group	Mandatory	Recoverable
PE1	1st Partial Exam	25%	-	No	No	Yes
PE2	2nd Partial Exam	25%	-	No	No	Yes
P1	Practice 1	25%	-	Yes (<= 2)	No	No
P2	Practice 2	25%	-	Yes (<= 2)	No	No

Final Grade = 0.25 * PE1 + 0.25 * PE2 + 0.25 * P1 + 0.25 * P2

Recovery of written tests 1 and 2: If the final grade obtained in the course is <5, then the student can choose to improve / recover the 50% that the written tests represent (the student will be able to choose which part they want to recover, or to choose both parts).

Except for a new exceptional situation, the written tests will be face-to-face.

Bibliography

- William Stallings. Cryptography and Network Security. Prentice Hall. 2005.
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press. 1996.
- Adam Shostack. Threat modeling: designing for security. Wiley. 2014.
- Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams. Gray Hat Hacking: The Ethical Hackers Handbook. McGraw-Hill. 2011.