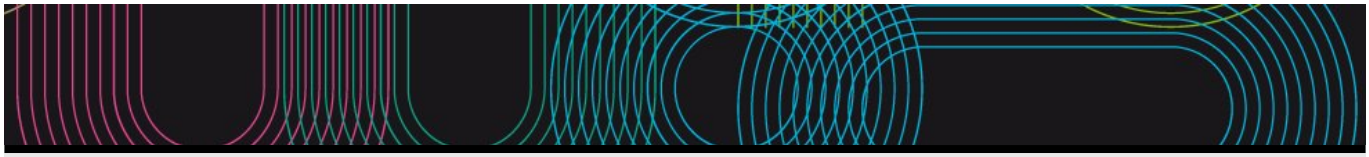

IDENTIFYING DATA				
Computer systems security				
Subject	Computer systems security			
Code	O06G151V01401			
Study programme	Grado en Ingeniería Informática			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	6	Mandatory	4th	1st
Teaching language	#EnglishFriendly Spanish Galician			
Department				
Coordinator	Ribadas Pena, Francisco José			
Lecturers	Ribadas Pena, Francisco José			
E-mail	ribadas@uvigo.es			
Web	http://moovi.uvigo.gal			
General description	The course "Computer Systems Security" is located at the fourth course of the "Grado en Ingeniría Informática". It is a compulsory course that pretends to integrate, complement and expand contents related with the computer security already studied in previous matters related with operating systems and computer networks. Since computer security is a wide and diverse field, the main aim of this subject is to provide an introduction to this branch of the computer science and give an overview of the most notable aspects the computer security, so that it could serve to the student as a starting point in case that they decide to run their professional paths in this field. English Friendly subject: International students may request from the teachers: a) materials and bibliographic references in English, b) tutoring sessions in English, c) exams and assessments in English.			

Training and Learning Results	
Code	
A2	Students will be able to apply their knowledge and skills in their professional practice or vocation and they will show they have the required expertise through the construction and discussion of arguments and the resolution of problems within the relevant area of study.
A3	Students will be able to gather and interpret relevant data (normally within their field of study) that will allow them to have a reflection-based considered opinion on important issues of social, scientific and ethical nature.
B3	Ability to design, develop, assess and ensure accessibility, ergonomics, usability and safety of computing systems, services and applications, as well as the information managed by them.
B4	Ability to define, assess and select hardware and software platforms for the development and execution of computing systems, services and applications, according to the acquired knowledge and training.
B7	Ability to learn, understand and apply the necessary legislation during professional practice as a Computer Science Engineer and to use the relevant binding specifications, regulations and norms.
B9	Ability to solve problems by taking the initiative, making decisions and acting independently and creatively. Ability to communicate the knowledge contents, skills and abilities of the Computer Science Engineer profession.
B11	Ability to analyze and assess the social and environmental impact of technical solutions, being aware of the ethical and professional responsibilities involved in the professional practice of a Computer Science Engineer.
B12	Knowledge and application of basic elements of economics and human resource management, organization and planning of projects, as well as legislation, regulation and standardization in the field of computer projects, according to the knowledge acquired.
C7	Ability to design, develop, choose and assess computer applications and systems to guarantee their reliability, safety and quality, according to ethical principles and existing legislation and regulations.
C29	Ability to identify, assess and deal with associated risks that could potentially arise.
C32	Ability to select, design, implement, integrate, assess, build, manage, exploit and maintain hardware, software and network technologies, within the appropriate costs and quality requirements.
C34	Ability to select, design, implement, integrate and manage networks and communications infrastructures in organizations.
C37	Ability to understand, apply and manage the security and safety of computing systems.

D4	Analysis, synthesis and evaluation capacity
D7	Ability to search, relate and structure information from various sources and to integrate ideas and knowledge.
D8	Ability to work in situations of lack of information and / or under pressure
D9	Ability to quickly integrate and work efficiently in unidisciplinary teams and to collaborate in a multidisciplinary environment
D11	Critical thinking
D12	Leadership
D13	Entrepreneurial spirit and professional ambition
D14	Have motivation for quality and continuous improvement

Expected results from this subject

Expected results from this subject	Training and Learning Results			
RA2: Know the security architecture of modern operating systems and know configure them and manage them in a safe way	A2	B3 B4 B7 B9 B12	C7 C29 C32 C37	D7 D9 D11 D14
RA3: Manage a computer network in a safe way	A3	B3 B4 B7 B9 B11 B12	C7 C29 C32 C34 C37	D7 D8 D9 D14
RA4: Know the most common types of computer attacks and the alternatives to protect against them	A2 A3	B3 B7 B9 B11 B12	C7 C29 C34 C37	D7 D8 D12 D13 D14
RA5: Know how manage a security incident	A2 A3	B3 B7 B9 B11 B12	C7 C29 C32 C34 C37	D4 D7 D8 D11 D12 D13 D14

Contents

Topic	
BLOCK I. Information security	.
1. Context of the security in computer systems	1.1 Concepts and terminology 1.2 Levels of the security: physics, logical, organisational 1.3 Norms and recommendations
2. Cryptography	2.1 Foundations and evolution 2.2 Symmetric encryption 2.3 Asymmetric encryption 2.4 Criptographic infraestructure: certificates, digital signatures, PKI
3. Secure application development	3.1 Software vulnerabilities and threats 3.2 Exploitation of vulnerabilities 3.3 Safe programming
BLOCK II. Operating systems security	.
4. Safe administration of O.S.	4.1 Authentication mechanisms 4.2 Monitoring tools 4.3 Typical vulnerabilities 4.4 Security incident response
BLOCK III. Network security	.
5. Secure network protocols	5.1 Vulnerabilities in TCP/IP networks 5.2 Security at network layer: IPSec 5.3 Security at transport layer: SSL/TLS 5.4 Security at application layer: SSH
6. Perimeter protection	6.1 Firewalls: types and topologies 6.2 Intrusion detection systems 6.3 Virtual private networks 6.4 Network security analysis

PRACTICAL ASSIGMENTS	- Use of encryption APIs - Security analysis in networks, systems and services - Design and deployment of perimeter protection solutions - Web application security analysis and countermeasures deployment

Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	20	20	40
Laboratory practical	26	52	78
Mentored work	0	15	15
Presentation	1	3	4
Objective questions exam	2	10	12
Essay	1	0	1

*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies

	Description
Lecturing	Presentation by the teacher and discussion of the theorical contents in the course's didactic guide. It includes activities such as study of practical cases and examples, presentation of studies and / or research, review and evaluation of security tools.
Laboratory practical	Practical works to realize in the laboratory. It will consist of a collection of guided exercises (individual or in couples) related with secure systems administration of operative systems and computer networks. CONTINUOUS ASSESSMENT Character: mandatory Attendance: not mandatory GLOBAL ASSESSMENT Character: not mandatory
Mentored work	Small research work, individual or in couples, related with aspects of the computer security not cobered by the main topics of this subject. Research themes can be proposed by students. The result of the work will reflect in a writtern report and a short public presentation. CONTINUOUS ASSESSMENT Character: mandatory Attendance: not mandatory GLOBAL ASSESSMENT Character: not mandatory
Presentation	Public presentation and discussion of the more relevant aspects of students research works. CONTINUOUS ASSESSMENT Character: not mandatory Attendance: not mandatory

Personalized assistance

Methodologies	Description
Mentored work	Autonomous work (or in couples) with teacher tutoring and development guides
Laboratory practical	Autonomous work (or in couples) with teacher tutoring and development guides

Assessment

	Description	Qualification	Training and Learning Results			
Laboratory practical	Evaluation of the programming project with cryptographic APIs. Evaluation of guided exercises about network and operative systems security. - LEARNING OUTCOMES: RA1, RA2, RA3, RA4, RA5	45	A2	B3 B4 B7	C7 C29 C32 C34	D7 D8 D9 D11 D12 D14
Presentation	Evaluation of the presentation of research work. It will evaluate synthesis and communication skills, as well as the encouragement of the discussion around questions from teacher and other students. - LEARNING OUTCOMES: RA2, RA3, RA4, RA5	5	A3	B7 B11 B12	C7 C29 C37	D4 D7 D13

Objective questions exam	Written multiple selection test, also with short answer questions, regarding contents from theoretical sessions and practical exercises. - LEARNING OUTCOMES: RA1, RA2, RA3, RA4, RA5	40	A3	B3 B7	C7 C29 C32 C34 C37	D4 D7 D8
Essay	Evaluation of the written report with the results of the research work. - LEARNING OUTCOMES: RA2, RA3, RA4, RA5	10	A3	B7 B11 B12	C7 C29 C37	D4 D7 D9 D11

Other comments on the Evaluation

(1) CONTINUOUS ASSEMENT SYSTEMTEST 1: Java Encryption API Project

Description: Evaluation of the code and memory of the development project employing the JCA encryption API.

Applied methodology: Laboratory practical

% Qualification: 10%

Minimum %: grade equal to or greater than 4 points (out of 10)

Evaluated learning results: B3, C7, C32

Expected results: RA1

TEST 2: Guided practices

Description: Evaluation of the deliverables and questions corresponding to the security practices in networks and OS.

Applied methodology: Laboratory practical

% Qualification: 35%

Minimum %: grade equal to or greater than 4 points (out of 10)

Evaluated learning results: A2,B3,B4,B7,C7,C29,C32,C34,D7,D8,D9,D11,D12,D14

Expected results: RA2, RA3, RA4, RA5

TEST 3: Tutored work/essay

Description: Evaluation of the report/essay from the tutored research work.

Applied methodology: Essay

% Qualification: 10%

Minimum %: no minimum

Evaluated learning results: A3,B7,B11,B12,C7,C29,C37,D4,D7,D9,D11

Expected results: RA2, RA3, RA4, RA5

TEST 4: Presentation

Description: Evaluation of the presentation of the supervised research work.

Applied methodology: Presentation

% Qualification: 5%

Minimum %: no minimum

Evaluated learning results: A3,B7,B11,B12,C7,C29,C37,D4,D7,D13

Expected results: RA2, RA3, RA4, RA5

TEST 5: Final exam

Description: Multiple-choice exam on the theoretical contents of the subject.

Applied methodology: Objective questions exam

% Qualification: 40%

Minimum %: grade equal to or greater than 4 points (out of 10)

Evaluated learning results: A3,B3,B7,C7,C29,C32,C34,C37,D4,D7,D8

Expected results: RA1, RA2, RA3, RA4, RA5

ADDITIONAL CLARIFICATIONS

- To pass the subject it is necessary to reach the minimums indicated in the previous tests and to add in the final weighted grade a minimum of 5 points out of 10.
- In the case of finding unethical behavior (copying, plagiarism) in any of the deliveries made (total or partial), the total contribution of the corresponding evaluation element on the final grade will be annulled.

(2) GLOBAL ASSEMENT SYSTEMProcedure for selecting the global assessment modality:

- The continuous assessment modality is assumed by default.
- Students who opt for the global evaluation must communicate it via Moovi, using the mechanisms that are enabled and within the stipulated period, once the period of one month from the beginning of the term has passed.

TEST 1: Java Encryption API Project

Description: Evaluation of the code and memory of the development project employing the JCA encryption API.

Applied methodology: Laboratory practical

% Qualification: 10%

Minimum %: grade equal to or greater than 5 points (out of 10)

Evaluated learning results: B3, C7, C32

Expected results: RA1

TEST 2: Guided practices

Description: Evaluation of the deliverables and questions corresponding to the security practices in networks and OS.

Applied methodology: Laboratory practical

% Qualification: 35%

Minimum %: grade equal to or greater than 5 points (out of 10)

Evaluated learning results: A2,B3,B4,B7,C7,C29,C32,C34,D7,D8,D9,D11,D12,D14

Expected results: RA2, RA3, RA4, RA5

TEST 3: Final exam

Description: Multiple-choice exam on the theoretical contents of the subject.

Applied methodology: Objective questions exam

% Qualification: 55%

Minimum %: grade equal to or greater than 5 points (out of 10)

Evaluated learning results: A3,B3,B7,C7,C29,C32,C34,C37,D4,D7,D8

Expected results: RA1, RA2, RA3, RA4, RA5

ADDITIONAL CLARIFICATIONS

- To pass the subject it is necessary to reach the minimums indicated in the previous tests and to add in the final weighted grade a minimum of 5 points out of 10.
- In the case of finding unethical behavior (copying, plagiarism) in any of the deliveries made (total or partial), the total contribution of the corresponding evaluation element on the final grade will be annulled.

(3) ASSESSMENT CRITERIA FOR EXTRAORDINARY AND FINAL CALLS- The continuous and global evaluation systems described above will be used.
- In these calls, students must only take the tests in which they have not obtained the minimum grade indicated.

(4) GRADING PROCESS In the case of students who pass part of the evaluated elements, but do not reach the minimum required to pass the whole
subject, the grade to be included in the respective minutes will be calculated as the minimum between the weighted
average of the parts passed and 4.9.

(5) EVALUATION DATES

The official exam dates of the different calls, officially approved by the Xunta de Centro of the ESEI, are published on

the ESEI website https://esei.uvigo.es/docencia/horarios/.

(6) USE OF MOBILE DEVICES All students are reminded of the prohibition of the use of mobile devices in exercises and practices, in compliance with
article 13.2.d) of the University Student Statute, regarding the duties of university students, which establishes the
duty to "Refrain from using or cooperating in fraudulent procedures in the assessment activities, in the delivered
assignments or in official documents of the university."

(7) TUTORING SCHEDULE AND PERSONAL TUTORING REQUEST The tutoring schedule, and the way to request a personal tutoring, is published in the personal page of the teaching
staff, accessible through https://esei.uvigo.es/docencia/profesorado/.

Sources of information

Basic Bibliography

W. Stallings, **Cryptography and Network Security: Principles and Practice**, 978-1292158587, 7th edition, Prentice Hall, 2017

W. Stallings, L. Brown, **Computer Security: Principles and Practice**, 978-0134794105, 4rd edition, Prentice Hall, 2018

J. L. García Rambla, **Ataques en redes de datos IPv4 e IPv6**, 978-8409240630, 2da edición, 0xWORD, 2014

Complementary Bibliography

Carlos Álvarez Martín y Pablo González Pérez, **Hardening de servidores GNU / Linux**, 978-84-09-24061-6, 4ª edición, 0xWORD, 2020

Darril Gibson, **Microsoft Windows Security Essentials**, 978-1118016848, 1st Edition, John Wiley & Sons, 2011

Recommendations

Other comments

Basic knowledge on OS administration, GNU/Linux and TCP/IP networks is assumed.

Programming assignment will require knowledge of Java language.

Network security exercises will employ virtual machines on VirtualBox (www.virtualbox.org). Basic knowledge of this tool is mandatory.