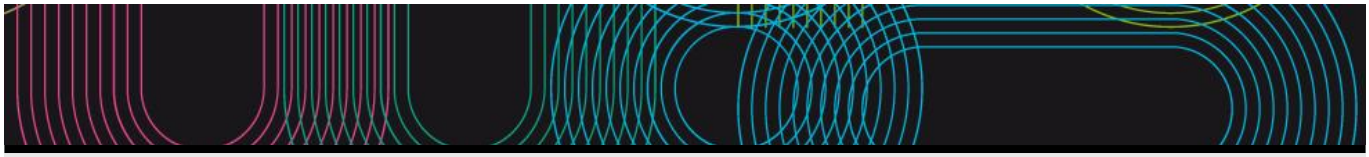

Escola de Enxeñaría de Telecomunicación

(*)Páxina web

(*)

www.teleco.uvigo.es

(*)Presentación

The School of Telecommunication Engineering (EET) is a higher education school of the University of Vigo that offers Bachelor's degrees, Master's degrees and Doctoral programs in the fields of Telecommunications Engineering.

Bachelor's Degree in Telecommunication Technologies Engineering (EUR-ACE®).

The mail goal of the Bachelor's Degree in Telecommunication Technologies Engineering is to form professionals at the forefront of technological knowledge and professional competences in telecommunication engineering. This Bachelor has been recognized with the best quality seals, like the EUR-ACE's. **It has a bilingual option: up to 80% of the degree credits can be taken in English**.

http://teleco.uvigo.es/images/stories/documentos/gett/degree_telecom.pdf

www: http://teleco.uvigo.es/index.php/es/estudios/gett

Master in Telecommunication Engineering

The Master in Telecommunication Engineering is a Master's degree that qualifies to exercise the profession of Telecommunication Engineer, in virtue of the established in the Order CIN/355/2009 of 9 of February.

http://teleco.uvigo.es/images/stories/documentos/met/master_telecom_rev.pdf

www: http://teleco.uvigo.es/index.php/es/estudios/mit

Interuniversity Masters

The current academic offer includes interuniversity master's degrees that are closely related to the business sector:

Master in Cybersecurity: www: https://www.munics.es/

Master in Industrial Mathematics: www: http://m2i.es

International Master in Computer Vision: www: https://www.imcv.eu/

(*)Equipo directivo

MANAGEMENT TEAM

Directora: Rebeca Pilar Díaz Redondo (teleco.direccion@uvigo.gal)

Secretaría e Subdirección de Novas Titulacións: Pedro Rodríguez Hernández

(teleco.subdir.secretaria@uvigo.gal;teleco.subdir.novastitulacions@uvigo.gal)

Subdirección de Organización Académica: Pedro Comesaña Alfaro (teleco.subdir.academica@uvigo.gal)

Subdirección de Relaciones Internacionais e Subdirección de Infraestructuras: María Verónica Santalla del

Río (teleco.subdir.internacional@uvigo.gal; teleco.subdir.infraestructuras@uvigo.gal)

Subdirección Difusión e Captación: Laura Docio Fernández (teleco.subdir.captacion@uvigo.gal)

Subdirección de Calidade: Ana María Cao Paz(teleco.subdir.calidade@uvigo.gal)

BACHELOR□SDEGREE IN TELECOMMUNICATION TECHNOLOGIES ENGINEERING

Generalcoordinator: Lucía Costas Pérez (teleco.grao@uvigo.gal)

https://teleco.uvigo.es/es/documentos/acordos-es/comisions-academicas-es/miembros-de-la-comision-academica-del-gett/

MASTER IN TELECOMMUNICATION ENGINEERING

Generalcoordinator: Manuel García Sánchez (teleco.master@uvigo.gal)

https://teleco.uvigo.es/es/documentos/acordos-es/comisions-academicas-es/miembros-de-la-comision-academica-del-met/

MASTER INCYBERSECURITY

General coordinator:Ana Fernández Vilas (teleco.munics@uvigo.gal)

https://teleco.uvigo.es/es/documentos/acordos-es/comisions-academicas-es/miembros-de-la-comision-academica-del-munics/

MASTER ININDUSTRIAL MATHEMATICS

Generalcoordinator: Elena Vázquez Cendón (USC)

UVigo coordinator:José Durany Castrillo (durany@dma.uvigo.es)

http://www.m2i.es/?seccion=coordinacion

INTERNATIONALMASTER IN COMPUTER VISION

General coordinator: Xose Manuel Pardo López (USC)

UVigo coordinator:José Luis Alba Castro (jalba@gts.uvigo.es)

https://www.imcv.eu/legal-notice/

MASTER'S DEGREE IN QUANTUM INFORMATION SCIENCE AND TECHNOLOGIES (MQIST)

General coordinator: Javier Mas (USC)

Coordinador UVIGO: Manuel Fernández Veiga(teleco.mqist@uvigo.es)

https://quantummastergalicia.es/info

Máster Universitario en Ciberseguridad

Subjects			
Year 1st			
Code	Name	Quadmester	Total Cr.
V05M175V11108	Information Security	1st	5
V05M175V11109	malware analysis	1st	5
V05M175V11110	Privacy and anonymity	1st	5
V05M175V11111	Application security	1st	5
V05M175V11112	Secure networks	1st	5

V05M175V11113	Distributed ledger and Blockchain technologies	1st	5
V05M175V11211	Communications security	2nd	5
V05M175V11212	Systems Fortification	2nd	5
V05M175V11213	Industrial cybersecurity and IoT	2nd	5
V05M175V11214	Ethical Hacking and Intrusion Test	2nd	5
V05M175V11215	Business in cybersecurity and entrepreneurship	2nd	4
V05M175V11216	Forensic analysis	2nd	3
V05M175V11217	Data center security	2nd	3
V05M175V11218		2nd	3
V05M175V11219	Smart Contracts and dApps	2nd	3

IDENTIFYING DATA				
Information Security				
Subject	Information Security			
Code	V05M175V11108			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language	English			
Department				
Coordinator	Fernández Veiga, Manuel			
Lecturers	Fernández Veiga, Manuel Gestal Pose, Marcos Pérez González, Fernando			
E-mail	mveiga@det.uvigo.es			
Web	http://moovi.gal			
General description	This course covers the fields of cryptography and cryptanalysis, generation of pseudorandom numbers and functions, message integrity, authenticated encryption, public key cryptography, privacy and anonymity in information systems, secure computations, steganography and watermarking.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
1. Encryption	Shannon ciphers. Perfect security. Semantic security. Information-theoretic security: the wiretap channel
2. Stream ciphers	Pseudorandom generators. Composition of PRGs. Security. Attacks. Case studies
3. Block ciphers	Block ciphers. Security. DES & AES. Pseudorandom functions. Construction of PRFs and block ciphers
4. Message integrity	Authentication codes. Message integrity. Definition of security. Keyed MACs. PRFs and MAC. Hashing, hash functions. Universal hashing. Collision resistant hashing. Case studies
5. Authenticated encryption	Definition. Composition. Attacks, examples and case studies
6. Public key cryptography	Definition. Semantic security. One-way trapdoor functions. RSA, ElGamal, McEliece crypto systems. Diffie-Hellman key agreement. Digital signatures. Case studies
7. Advanced cryptography	Elliptic curve cryptography. Lattice-based cryptography. RLWE. Quantumresistant cryptography. Homomorphic encryption
8. Identification protocols	Definitions. Passwords. Challenge-response. sigma-protocols. Okamoto and Schnorr protocols
9. Anonymization	Definitions. t-integrity and anonymity. Divergence. Analysis
10. Data hiding and steganography	Definitions. Spread-spectrum watermarking. Dirty paper coding. Digital forensics.
11. Secure computation	Computable functions. Fundamental limits. Two-way secure computation. Multiparty secure computation. Interactive communications. Homomorphic computations. Applications

Planning			
	Class hours	Hours outside the classroom	Total hours
Problem solving	0	24	24
Laboratory practical	18	36	54
Lecturing	17	51	68
Essay questions exam	2	0	2
Problem and/or exercise solving	2	0	2

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

Methodologies	
	Description
Problem solving	Students are supposed to solve problems and exercises about the curse contents. Written homework, with review and grading.
Laboratory practical	Students are expected to work in the computer laboratory doing small programs on ciphering, and a programming assignment on ciphering, authentication, anonymity or digital forensics. The programming assignment will be supervised by the instructors.
Lecturing	Lectures on the topics included in the course: definitions, concepts, main results, properties and applications.

Personalized assistance	
Methodologies	**Description**
Problem solving	Individual office hours will be offered to answer the questions about problems and exercises assigned to the students. https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
Laboratory practical	Individual assistance will be given to the students who request guidance on the programming assignments or computer lab practice. https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
Lecturing	Individual office hours will be offered to the students who need guidance in the study, or further explanations on the course contents, clarification on the solutions to problems, etc. https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga

Assessment			
	Description	Qualification	Training and Learning Results
Problem solving	4 homework problem sets, to be worked out individually. Written submission	30	
Laboratory practical	Design and development of programming assignments. Functional and performance tests will be run	30	
Essay questions exam	Written exam. Questions, problems or exercises about the contents covered in the course	40	

Other comments on the Evaluation

The student must choose between two alternative, mutually exclusive assessment method: continuous assessment or global assessment.

The continuous evaluation option consists in a final written exam (40% of the qualification), the completion of programming assignments (30% of the qualification) and homework (30%). The global assessment option consists in a final written exam (40% of the qualification) and in the completion of assignments (two, 30% of the qualification each one). The assignments will be due the last working day preceding the start of the examination period. The examinations of the continuous and the eventual assessment options may not be equal.

The students can declare their preferred assessment type until the date of the written examination.

The students who fail the course will be given an extraordinary opportunity at the end of the academic year to do so. Their academic achievements will be re-evaluated, both with a written exam (theoretical knowledge) and a review of their engineering project looking for improvement or changes. The weights are the same they were committed to, according to their choice.

Any assigned grade will only be valid during the academic year where it is awarded.

Sources of information

Basic Bibliography

D. Boneh, V. Shoup, **A graduate course in applied cryptography**, http://toc.cryptobook.us, 2021

Complementary Bibliography

O. Goldreich, **Foundation of cryptography, vol. I,**, Cambridge University Press, 2007

O. Goldreich, **Foundation of cryptography, vol. II**, Cambridge University PRess, 2009

J. Katz, Y. Lindell, **Introduction to modern cryptography**, 2, CRC PRess, 2015

A. Menezes, P. van Oorschot, S. Vanstone, **Handbook of applied cryptography**, CRC Press, 2001

C. Dwork, A. Roth, **The algorithmic foundations of differential privacy**, NOW Publishers, 2014

W. Mazurczyk, S. Wenzel, S. Zander, A. Houmansadr, K. Szczypiorski, **Information hiding in communications networks: Fundamentals, mechanisms, applications, and countermeasures**, Wiley, 2016

I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kolker, **Digital watermarking and steganography**, Morgan Kaufmann, 2008

A. El-Gamal, Y. Kim, **Network Information Theory**, Cambridge University Press, 2011

Recommendations

Other comments

The course is given in English. Ability for mathematical reasoning is highly recommended.

IDENTIFYING DATA				
malware analysis				
Subject	malware analysis			
Code	V05M175V11109			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language	English			
Department				
Coordinator	Burguillo Rial, Juan Carlos			
Lecturers	Burguillo Rial, Juan Carlos Hernández Pereira, Elena María Rivas López, Jose Luis			
E-mail	jrial@uvigo.es			
Web	http://https://moovi.uvigo.gal			
General description	Malware uses the systems and the communication networks to disseminate virus, hijack devices or steal confidential data. The aim of this subject is to provide the student the capability to analyze, detect and erase malware. To achieve that, we will explore and evaluate, practically and with case studies, the techniques used nowadays to hide malware, together with the new tendencies to detect it and eliminate it. This course will be taught in English. However, students have the possibility to interact with teachers in Spanish or Galician if necessary. All the documentation needed for the course will be provided in English.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
Introduction to malware analysis and engineering.	a) What is malware? b) How to detect and erase it? c) What is malware engineering?
Malware types and definitions.	a) Structure. b) Components. c) Infection vectors.
Malware Engineering.	a) Propagation techniques. b) Infection processes. c) Malware persistence. d) Hiding techniques.
Reverse malware engineering.	a) How to analyze and infer malware behavior? b) Understanding how new malware types work.
Tools for malware analysis.	a) Tools for malware detection. b) Tools for malware erasing.

Planning			
	Class hours	Hours outside the classroom	Total hours
Introductory activities	2	2	4
Lecturing	10	30	40
Laboratory practical	15	40	55
Discussion Forum	0	2	2
Case studies	5	4	9
Objective questions exam	2	4	6
Problem and/or exercise solving	3	6	9
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies	
	Description

Introductory activities	We start doing a general introduction to the aims, the global contents of the subject and the expected outcomes. This activity will be performed individually.
Lecturing	We describe the different subject topics, giving the teaching material needed to follow them. Through this methodology the knowledge B2, skill C2 and competence D6 are achieved. This activity will be performed individually.
Laboratory practical	Students must perform a set of practices in the lab to better understand the contents explained along the master lessons. Through this methodology the knowledge B2, skill C2 and competencies D3 and D6 are achieved. Some practices will be performed individually and others in groups (depending on the number of students).
Discussion Forum	Students must participate in the subject forum within the MOOVI platform. Through this methodology the knowledge B2 and the competence D6 are achieved. This activity will be performed individually.
Case studies	Along master lessons students will present case studies about threats, security problems already known and nowadays technologies. Through this methodology the knowledge B2 and competencies D3 and D6 are achieved. This activity can be performed individually or in groups of two people.

Personalized assistance

Methodologies	Description
Introductory activities	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated. Students can request tutoring support through the Moovi platform (https://moovi.uvigo.gal).
Lecturing	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated. Students can request tutoring support through the Moovi platform (https://moovi.uvigo.gal).
Laboratory practical	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated. Students can request tutoring support through the Moovi platform (https://moovi.uvigo.gal).
Discussion Forum	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated. Students can request tutoring support through the Moovi platform (https://moovi.uvigo.gal).
Case studies	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated. Students can request tutoring support through the Moovi platform (https://moovi.uvigo.gal).

Assessment

	Description	Qualification	Training and Learning Results
Laboratory practical	Students will perform a set of practices (3 x 15% = 45%) at the lab, where they work with the concepts studied along the master lessons.	45	
Discussion Forum	Students must participate in the subject forum available at Moovi.	5	
Case studies	Students will provide presentations about case studies, selected by them, in order to analyse nowadays threats.	15	
Objective questions exam	Two evaluation tests will be performed along the subject for the partial contents provided in the subject. Tests will be filled individually and time limited	30	

Problem and/or exercise solving	Along master lessons, the teacher will ask questions to the students to test their knowledge level in the discussed topics.	5

Other comments on the Evaluation

The elements that are part of the evaluation of the subject are the following:

- **Questionnaires**: along the course the student will fill two questionnaires that will contribute 15% to the final mark (each one).

- **Presentation of case studies**: each student (individually or in a group) has to provide an original presentation, which contributes with a 15% to the final mark.

- **Laboratory practice**: each student will have to perform a set of practices (by defect 3 practices with a weight of 15% each) in the laboratory that will contribute 45% to the final mark.

- **Class participation**: students will discuss in class about expositions done by the professor, and this contributes up to a 5% to the final mark.

- **Forum participation**: students should interact individually in the forum of the subject to achieve up to a 5% to the final mark. To achieve such percentage the student should provide at least two relevant contributions.

Therefore, we have:

Final Score = Questionnaires (2*x15% = 30%) + Case Study Presentation (15%) + Lab. Tasks (45%) + Class participation (5%) + Forum (5%) = 100%.

The students need to pass the questionnaires, the case studies and the practical tasks with at least 4 points over 10 to calculate the average final mark. If any of the marks is below 4, then the final mark will never be higher than 4.9 points over 10.

The schedule of the midterm/intermediate exams will be approved in the Comisión Académica de Máster (CAM) and will be available at the beginning of each academic semester.

Following the degree guidelines, the students that will follow this subject can choose between two possibilities: continuous or final assessment (at the end of the semester).

Continuous assessment: the student follows the continuous assessment since the moment he/she fulfills the two questionnaires. From that moment we assume that he/she will participate in the subject, independently of the presentation at the first call.

Global assessment: if the continuous assessment is not performed, then the student will have to perform a final exam that substitutes the questionnaires done along the course, in addition to provide the practical tasks and the equivalent work to be done as part of the continuous assessment.

Extraordinary assessment: the student will have to perform the part not passed previously.

End-of-program assessment: the student will have to perform the part not passed previously.

Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the tests or exams, the final grade will be FAIL (0), and the incident will be reported to the corresponding academic authorities for prosecution.

The questionnaires and tasks, proposed and performed along the module, are only valid for the current course.

Sources of information

Basic Bibliography

Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, **The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory**, 1, John Wiley & Sons Inc, 2014

Michael Sikorski / Andrew Honig, **Practical Malware Analysis**, 1, William Pollock, 2012

Complementary Bibliography

Recommendations

Subjects that are recommended to be taken simultaneously

Forensic analysis/V05M175V11216

IDENTIFYING DATA				
Privacy and anonymity				
Subject	Privacy and anonymity			
Code	V05M175V11110			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language	English			
Department				
Coordinator	Pérez González, Fernando			
Lecturers	Hernández Pereira, Elena María Pérez González, Fernando			
E-mail	fperez@gts.uvigo.es			
Web	http://http://moovi.gal			
General description	This subject presents the main techniques to provide privacy and anonymity in networks, systems and applications. It covers concepts and methods of differential privacy, privacy enhancing technologies (PET), geolocation privacy, machine learning privacy, and anonymity techniques. The implications of privacy by design, and ethical and legal aspects of privacy are also explored.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
Introduction. Attacks.	Introduction to privacy and anonymity. Inference attacks. Traffic analysis attacks. Online tracking.
Differential privacy.	Differential privacy. Differential privacy mechanisms. Composition theorems.
Privacy preserving and enhancing techniques.	Privacy-preserving primitives: information retrieval, set intersection. Privacy enhancement techniques with homomorphic encryption and secure multi-party computing. Bloom filters.
Anonymity.	Basic concepts. K-anonymity, l-diversity and t-proximity.
Applications in privacy and anonymity.	Geolocation privacy. Anonymous communications. Onion routing. Mixes. Anonymous authentication. Privacy in machine learning.

Planning			
	Class hours	Hours outside the classroom	Total hours
Laboratory practical	19	38	57
Lecturing	19	38	57
Problem solving	2	0	2
Problem and/or exercise solving	0	5	5
Objective questions exam	2	0	2
Report of practices, practicum and external practices	0	2	2
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies	
	Description
Laboratory practical	Students will develop privacy and anonymity projects in the laboratory as applications of the techniques presented in the master classes. The practices or projects will be supervised by the teachers.
Lecturing	Systematic presentation of the course contents: concepts, results, algorithms, examples and use cases.
Problem solving	Solving problems in the classroom by teachers.

Personalized assistance

Methodologies	Description
Laboratory practical	Questions related to laboratory practices and the development of the project will be answered individually. Office hours will be established at the beginning of the course and will be published on the subject's website.
Lecturing	Individual attention will be given to students who require orientation for the study, additional explanation on the contents of the discipline, clarification or guidance on problem solving. Office hours will be established at the beginning of the course and will be published on the subject's website.
Problem solving	Queries about solving problems and exercises raised in class or worked independently will be addressed individually. Office hours will be established at the beginning of the course and will be published on the subject's website.

Assessment

	Description	Qualification	Training and Learning Results
Problem and/or exercise solving	Resolution of questions, problems and exercises throughout the course. Individual delivery in writing.	30	
Objective questions exam	Written exam. Resolution of questions, problems or exercises.	40	
Report of practices, practicum and external practices	Reports on the practices carried out individually or in pairs.	30	

Other comments on the Evaluation

Two alternative evaluation methods in the subject are left to the discretion of the students: continuous evaluation and global evaluation.

The continuous evaluation will consist of the completion of a final exam (40% of the grade), the development of practices and projects (30% of the grade) and the delivery throughout the course and within the established deadlines of resolved exercises (30%).

The single evaluation will consist of a final written exam (70% of the grade) and the development of practices and projects (30%).

The written tests of the global and continuous assessment modalities will not necessarily be the same.

Students will be able to opt for one or another modality of evaluation until the date of the written exam of the course.

Those who do not pass the subject in the ordinary call have a second extraordinary opportunity at the end of the course in which their knowledge will be reassessed with a written test.

Sources of information

Basic Bibliography

C. Dwork, **The Algorithmic Foundations of Differential Privacy**, Now Publishers Inc., 2013

J. Morris Chang, Di Zhuang, and G. Dumindu Samaraweer, **Privacy-preserving Machine Learning**, 9781617298042, Manning Publications, 2023

Mark Craddock, Ed., **UN Handbook on Privacy-Preserving Computation Techniques**, 9781913805272, GCATI, 2020

Complementary Bibliography

Katharine Jarmul, **Practical Data Privacy**, 9781098129460, O'Reily Media, 2023

Nishant Bhajaria, **Data Privacy**, 9781617298998, Manning Publications, 2022

PALISADE, **PALISADE HOMOMORPHIC ENCRYPTION SOFTWARE LIBRARY**,

Recommendations

IDENTIFYING DATA

Application security

Subject	Application security			
Code	V05M175V11111			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language				
Department				
Coordinator	López Nores, Martín			
Lecturers	Bellas Permuy, Fernando López Nores, Martín Losada Pérez, José			
E-mail	mlnores@det.uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530104&any_academic=2023_24&any_academic=2023_24			
General description	Developing secure applications is not a trivial task. Knowing the most common vulnerabilities that affect the applications, the mechanisms of authentication, authorization and access control, as well as the incorporation of the security to the software life cycle, is essential to build secure applications. This course addresses all of these aspects, with special emphasis in the development of applications and web services.			

Training and Learning Results

Code

Expected results from this subject

Expected results from this subject	Training and Learning Results

Contents

Topic

Planning

	Class hours	Hours outside the classroom	Total hours

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

Methodologies

	Description

Personalized assistance

Assessment

Description	Qualification	Training and Learning Results

Other comments on the Evaluation

Sources of information

Basic Bibliography

Complementary Bibliography

Recommendations

IDENTIFYING DATA

Secure networks

Subject	Secure networks			
Code	V05M175V11112			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language				
Department				
Coordinator	Rodríguez Rubio, Raúl Fernando			
Lecturers	Nóvoa de Manuel, Francisco Javier Rodríguez Rubio, Raúl Fernando			
E-mail	rrubio@det.uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530105&any_academic=2023_24&any_academic=2023_24			
General description	The main objective of Secure Networks is for students to learn how to design and implement network infrastructures that are capable of providing the necessary security services in a modern corporate environment. They must know the reference security architectures and be able to configure and manage them, using technologies such as IDS / IPS and Firewalls, among others. The subject is conceived so that laboratory practices, with physical and virtual equipment, have a major importance in the learning process.			

Training and Learning Results

Code

Expected results from this subject

Expected results from this subject	Training and Learning Results

Contents

Topic

Planning

	Class hours	Hours outside the classroom	Total hours

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

Methodologies

	Description

Personalized assistance

Assessment

Description	Qualification	Training and Learning Results

Other comments on the Evaluation

Sources of information

Basic Bibliography

Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Distributed ledger and Blockchain technologies				
Subject	Distributed ledger and Blockchain technologies			
Code	V05M175V11113			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language				
Department				
Coordinator	Fernández Iglesias, Manuel José			
Lecturers	Álvarez Sabucedo, Luis Modesto Fernández Caramés, Tiago Manuel Fernández Iglesias, Manuel José			
E-mail	manolo@uvigo.es			
Web	http://bit.ly/gd_trdb			
General description	In this course, the basic concepts about distributed ledger and blockchain technologies are introduced.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents
Topic

Planning			
	Class hours	Hours outside the classroom	Total hours
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies	
	Description

Personalized assistance

Assessment		
Description	Qualification	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Communications security				
Subject	Communications security			
Code	V05M175V11211			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Rodríguez Rubio, Raúl Fernando			
Lecturers	Fernández Iglesias, Diego Rodríguez Rubio, Raúl Fernando Suárez González, Andrés			
E-mail	rrubio@det.uvigo.es			
Web	http://https://moovi.uvigo.gal			
General description	This subject reviews the layers of the Internet communications architecture, showing its main weaknesses from a security point of view and providing the necessary techniques and tools to mitigate them. Students will acquire a detailed understanding of the network protocols that provide security for the transmission of information, and the implications derived from the place they occupy within the networking architecture.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
Internet architecture and protocols	Fundamental concepts
Link level security	Wired security/Ethernet networks: Access control and port-based authentication Confidentiality in Ethernet networks Wireless Security/WiFi networks: WPA/2/3: Personal & Enterprise security
Network level security	IPsec security protocols IPsec dynamic key management IPsec authentication mechanisms
Securing Internet infrastructure	Routing protocols security DNS security TCP security
Data transmission security	The TLS protocol Cryptographic suites WebPKI infrastructure Certificate validation
Mobile networks security	System architecture Association and authentication of the user/terminal Privacy

Planning			
	Class hours	Hours outside the classroom	Total hours
Lecturing	21	21	42
Laboratory practical	19	19	38
Practices through ICT	0	58	58
Essay questions exam	2	0	2
Report of practices, practicum and external practices	0	10	10
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies	
	Description
Lecturing	Master sessions follow the usual scheme for this type of teaching. In these sessions the CG3, CE1, CE2, CE4, CE8 competences are worked out
Laboratory practical	There will be several practical sessions guided by the teachers where the concepts learned in the theoretical classes will get entrenched. Such practices, will use network devices (routers and switches) and / or virtualization software that will allow students to learn and practice at home. The practices to be considered will be sized to be approachable during their respective classroom sessions; although any student that needs so will be able to reproduce them at home with free virtualization software that will allow them to virtualize the behaviour of the network hardware used in the laboratory. Students will acquire competencies CB2, CB4, CG1, CG3, CG5, CE1, CE4, CE8
Practices through ICT	Beyond the guided practices, the student will have to deploy / configure / implement some specific solutions, for certain scenarios, in an autonomous way. In these activities CB2, CB4, CB5, CG1, CG3, CG5, CE1, CE4, CE8 are worked out.

Personalized assistance	
Methodologies	**Description**
Lecturing	During the office hours teachers will provide personalized attention to strengthen or guide students in the understanding of the theoretical concepts explained in the lectures or practical demonstration sessions; and to correct or reorient the small optional practical works derived from said laboratory classes. Office hours: Raúl Rodríguez Rubio https://moovi.uvigo.gal/user/profile.php?id=11315 Andrés Suárez González https://moovi.uvigo.gal/user/profile.php?id=11340 Diego Fernández Iglesias https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614
Laboratory practical	This activity is interactive by definition, so it is expected that questions will flow naturally between teachers and students, and may involve other students in the answers.
Practices through ICT	Although the autonomous work is targeted to make students solve situations / challenges to be found in real systems on their own, during office hours, teachers will guide them by questioning the chosen solutions or suggesting alternative paths.

Assessment			
	Description	Qualification	Training and Learning Results
Laboratory practical	They will be qualified as apt / unfit. Students will pass them if they attend all sessions of this type. If for some reason they miss any, they must do some complementary practical that teachers will establish. In some of the sessions / activities the student may be asked for an additional autonomous work (and its associated report) that will be quantitatively evaluated within the more general element called "Autonomous practices through ICT".	0	
Practices through ICT	Students must perform, in presence of the teachers, a practical demonstration showing the resolution of the different technical challenges posed, and face questions about the adopted solutions and their degree of completeness. This defense/interview will take place, in a general way, after the delivery deadline of the last ordered task, and before the beginning of the official exams period in the corresponding call, and its definite date will be agreed on time between students and teachers. Every challenge or autonomous activity will require a written report, whose structure, composition and readability will affect final mark.	60	
Essay questions exam	A written exam will be carried out at the end of the semester, where the theoretical concepts taught in the lectures are evaluated, as well as the practical foundations derived from the classes / practical work carried out.	40	
Report of practices, practicum and external practices	The student's autonomous work should be reported appropriately with pertinent docs whose evaluation will be part of the more general evaluation of the documented task.	0	

Other comments on the Evaluation

The evaluation of the subject can either follow a continuous assessment strategy (EC) or a general assessment one (EG). The students choose EC if they deliver the solution to the first challenge or autonomous work that they must attend during the course. The percentages expressed in the previous section only reflect the maximum mark obtainable in each type of test in the EC modality; and they are only indicative. The detailed evaluation form is expressed below:

For EC (first call), the final grade will be the weighted geometric mean between the autonomous work grade (TA, 60%) and the corresponding grade for the essay questions exam (E, 40%). The grade of TA will be the arithmetic mean of the marks obtained in each of the challenges / autonomous practical that students have to solve during the semester, which will never be less than two.
FINAL GRADE (EC) = (TA ^ 0.6) × (E ^ 0.4)
If the laboratory practices assessment is unfit, the grade will be the minimum between the written test score (E) and 3.
Students who choose EG must take a final exam consisting of three parts: a written test analogous to the continuous assessment test (E), a proficiency test in the laboratory and one or more practical tasks (T). The final grade, in this case, is the weighted geometric mean between the theory grade (E, 80%) and practical work (T, 20%), with the condition that the aptitude test is passed. For any student that fails the aptitude test, the final grade will be the minimum between E and 3.
FINAL GRADE (EU) = (T ^ 0.2) × (E ^ 0.8)
Finally, for the extra call (June / July), students will be able to continue with the evaluation mode that they had already chosen (keeping the mark of the part -E or TA / T- that they had passed), facing only the failed part - though with possible modifications in the specifications of the practical works; or they may choose to follow EU doing just a final exam as the one just described. The aptitude test will only be necessary if they did not attend all laboratory sessions.

Sources of information

Basic Bibliography

I. Ristic, **Bulletproof SSL and TLS, ser. Computers/Security**, London: Fesity Duck, 2015

A. Liska and G. Stowe, **DNS Security: Defending the Domain Name System**, Boston: Syngress, 2016

Yago Fernández Hansen, Antonio Angel Ramos Varón, Jean Paul García-Moran Maglaya, **RADIUS / AAA / 802.1x**, RA-MA Editorial, 2008

Graham Bartlett, Amjad Inamdar, **IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS**, CISCO PRESS, 2016

Madhusanka Liyanage, Ijaz Ahmad, Ahmed Abro, Andrei Gurtov, Mika Ylianttila, **A Comprehensive Guide to 5G Security**, Wiley, 2018

Complementary Bibliography

D. J. D. Touch, **Defending TCP Against Spoofing Attacks**, IETF, 2007

R. R. Stewart, M. Dalal, and A. Ramaiah, **Improving TCP□s Robustness to Blind In-Window Attacks**, IETF, 2010

D. J. Bernstein, **SYN cookies**,

P. McManus, **Improving syncookies**, 2008

C. Pignataro, P. Savola, D. Meyer, V. Gill, and J. Heasley, **The Generalized TTL Security Mechanism (GTSM)**, IETF, 2007

D. J. D. Touch, R. Bonica, and A. J. Mankin, **The TCP Authentication Option**, IETF, 2010

S. Rose, M. Larson, D. Massey, R. Austein, and R. Arends, **DNS Security Introduction and Requirements**, IETF, 2005

R. Arends, R. Austin, M. Larson, D. Massey, S. Rose, **Resource Records for the DNS Security Extensions**, IETF, 2005

R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, **Protocol Modifications for the DNS Security Extensions**, IETF, 2005

Cloudflare Inc., **How DNSSEC works**,

P. E. Hoffman and P. McManus, **DNS Queries over HTTPS (DOH)**, IETF, 2018

E. Jones and O. L. Moigne, **OSPF security vulnerabilities analysis**, IETF, 2006

M. Khandelwal and R. Desetti, **OSPF security: Attacks and defenses**, 2016

J. Durand, I. Pepelnjak, and G. Doering, **BGP operations and security**, IETF, 2015

R. Kuhn, K. Sriram, and D. Montgomery, **Border gateway protocol security**, NIST, 2007

C. Pelsser, R. Bush, K. Patel, P. Mohapatra, and O. Maennel, **Making route flap damping usable**, IETF, 2014

Y. Rekhter, J. Scudder, S. S. Ramachandra, E. Chen, and R. Fernando, **Graceful restart mechanism for BGP**, IETF, 2007

IEEE 802.1 Working Group, **IEEE Std 802.1X - 2010. Port-Based Network Access Control**, IEEE Computer Society, 2010

Security Task group of IEEE 802.1, **IEEE Std 802.1AE. Medium Access Control Security**, IEEE Computer Society, 2018

S. Kent, K. Seo, **Security Architecture for the Internet Protocol**, IETF, 2005

S. Kent, **IP Authentication Header**, IETF, 2005

S. Kent, **IP Encapsulating Security Payload**, IETF, 2005

C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen, **Internet Key Exchange Protocol Version 2 (IKEv2)**, IETF, 2014

J. Cichonski, J. M. Franklin, M. Bartock, **Guide to LTE Security**, NIST Special Publication 800-187,

Recommendations

IDENTIFYING DATA				
Systems Fortification				
Subject	Systems Fortification			
Code	V05M175V11212			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Blanco Fernández, Yolanda			
Lecturers	Blanco Fernández, Yolanda Yáñez Izquierdo, Antonio Fermín			
E-mail	yolanda@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530108&any_academic=2023_24			
General description	A newly installed operating system is inherently insecure. It presents certain vulnerabilities based on factors such as the age of the OS, the presence of backdoors, the services it provides, and the use of default policies that do not prioritize security. When we refer to the fortification of an operating system, we mean the act of configuring this OS with the intention of making it as secure as possible, aiming to minimize the risk of it being compromised and exploited by any vulnerabilities. This typically involves applying security patches, changing certain default OS policies, and removing (or deactivating) non-essential applications and services. The document of the teaching guide can be consulted at the UDC link specified above.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents
Topic

Planning			
	Class hours	Hours outside the classroom	Total hours
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies
Description

Personalized assistance

Assessment		
Description	Qualification	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Ciberseguridade industrial e IoT				
Subject	Ciberseguridade industrial e IoT			
Code	V05M175V11213			
Study programme	Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1	2c
Teaching language				
Department				
Coordinator	Diaz-Cacho Medina, Miguel Ramón			
Lecturers	Diaz-Cacho Medina, Miguel Ramón Fernández Caramés, Tiago Manuel Gil Castiñeira, Felipe José			
E-mail	mcacho@uvigo.es			
Web				
General description	(*)Los dispositivos inteligentes nos están prestando cada vez más servicios casi sin que nos demos cuenta de su presencia: el coche ha dejado de ser una simple máquina mecánica para convertirse en un sistema conectado con un enorme control electrónico; en los hoteles ya no usamos llave, sino que podemos abrir nuestra habitación con una tarjeta o nuestro teléfono móvil; Nuestros termostatos domésticos se pueden conectar a un servicio de pronóstico del tiempo y ajustarse al clima en las próximas horas. Los entornos industriales son casos de uso particularmente importantes, ya que la conexión en red de dispositivos que miden y controlan procesos permite la Industria 4.0. Todos son ejemplos de las aplicaciones habilitadas por tecnologías "integradas", redes de comunicaciones inalámbricas y, en última instancia, "Internet de las cosas" (IoT). Esta asignatura analiza los problemas y las mejores prácticas para hacer que este tipo de sistemas sean seguros, con especial énfasis en la seguridad de las tecnologías de la Industria 4.0, como los sistemas IoT/IioT, los sistemas robóticos, la computación en la nube/borde, la realidad aumentada, la cadena de bloques o los AGV.			

Resultados de Formación e Aprendizaxe
Code

Resultados previstos na materia	
Expected results from this subject	Training and Learning Results

Contidos	
Topic	
Introdución á ciberseguridade industrial.	Introdución á ciberseguridade industrial.
Introdución aos sistemas ciberfísicos e IoT: hardware, firmware, comunicacións e cloud	Introdución aos sistemas ciberfísicos e IoT: hardware, firmware, comunicacións e cloud
Ciberseguridade de sistemas de control e comunicacións industriais.	Ciberseguridade de sistemas de control e comunicacións industriais.
Ciberseguridade de tecnoloxías da Industria 4.0/5.0.	Ciberseguridade de tecnoloxías da Industria 4.0/5.0.
Ciberseguridade de dispositivos IoT/IIoT hardware, firmware e middleware.	Ciberseguridade de dispositivos IoT/IIoT hardware, firmware e middleware.
Ciberseguridade en contornas IIoT: sistemas de posicionamento e sensórica.	Ciberseguridade en contornas IIoT: sistemas de posicionamento e sensórica.
Ciberseguridade en comunicacións inalámbricas para dispositivos IoT/IioT.	Ciberseguridade en comunicacións inalámbricas para dispositivos IoT/IioT.

Planificación			
	Class hours	Hours outside the classroom	Total hours
Aprendizaxe baseado en proxectos	5	45	50
Lección maxistral	14	20	34
Prácticas con apoio das TIC	15	25	40
Exame de preguntas obxectivas	1	0	1
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Metodoloxía docente	
	Description
Aprendizaxe baseado en proxectos	Implementación grupal do deseño, implementación e probas dun sistema IoT, con especial énfase na seguridade. Realizar ataques grupales á seguridade dos sistemas implementados por outros compañeiros ou terceiros.
Lección maxistral	Presentación, por parte do profesorado, dos principais contidos teóricos relacionados coa seguridade industrial e IoT (seguridade embebida, en comunicacións e backends, con especial foco en contornas industriais)
Prácticas con apoio das TIC	Realización por parte dos alumnos de prácticas guiadas e supervisadas.

Atención personalizada	
Methodologies	**Description**
Aprendizaxe baseado en proxectos	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. Así mesmo, o profesorado orientará ao alumnado durante a realización do proxecto. As dúbidas resolveranse durante as titorías en grupo, ou no horario establecido para as titorías. O horario de titorías establecerase ao comezo do curso e publicarase na web da materia.
Lección maxistral	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. As dúbidas resolveranse durante a propia sesión maxistral, ou no horario establecido para as titorías. O horario de titorías establecerase ao comezo do curso e publicarase na web da materia.
Prácticas con apoio das TIC	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. Así mesmo, o profesorado orientará e guiará ao alumnado durante a realización das tarefas que lles foron asignadas, tanto nas prácticas. As dúbidas resolveranse ben durante as propias clases ou ben no horario establecido para as titorías.

Avaliación			
	Description	Qualification	Training and Learning Results
Aprendizaxe baseado en proxectos	O alumnado dividirase en grupos para a realización do deseño, implementación e proba dun sistema IoT, pondo unha énfase especial na seguridade e/ou realizará ataques á seguridade dos sistemas implementados por outros compañeiros/as ou por terceiros. O proxecto realizado, e o informe que contén o resultado dos ataques completados (en canto á súa calidade e ao seu éxito) serán avaliados despois da súa entrega valorando aspectos como a corrección, a calidade, as prestacións e as funcionalidades. Deberase entregar o código, prototipos e documentación realizados. Así mesmo, será necesario realizar unha presentación dos resultados. Durante a realización do proxecto realizarase un seguimento continuo do deseño e da evolución da implementación. Si os resultados intermedios non son satisfactorios, poderase aplicar unha penalización de até o 20% da nota. O seguimento será grupal e individual: cada un do membros do grupo debe documentar as tarefas desenvolvidas dentro do seu equipo e responder sobre elas.	40	
Prácticas con apoio das TIC	Resolución de prácticas e realización de informes cos resultados obtidos.	30	
Exame de preguntas obxectivas	Exame escrito sobre os contidos teóricos e prácticos impartidos durante o curso.	30	

Other comments on the Evaluation

Para superar a materia é necesario completar as distintas partes nas que se divide (exame ou exámenes acerca dos contidos expostos na sesión maxistral e o proxecto). A nota final será o resultado de aplicar a **media xeométrica ponderada** da nota de cada unha das partes.

Así, se a nota das sesións maxistrais é NT, a nota do proxecto é NP e a nota das prácticas é NL, a nota final será:

Nota = NT^0.3 × NP^0.4 × NL^0.3

Durante o primeiro mes, o estudiantado deberá indicar explícitamente e por escrito o seu desexo de cursar a materia seguindo a evaluación global. Noutro caso se considerará que seguen a availiación continua. Quen sigan a avaliación continua non se podrán considerar "non presentados" así que realicen a entrega do primeiro cuestionario ou tarefa.

O alumnado que opte pola avaliación global deberá presentar adicionalmente un *dossier* que deberá defender presencialmente ante o profesorado, no que se inclúan todos os detalles sobre a realización das distintas tarefas, e moi especialmente o proxecto. No caso de seguir a avaliación global, os alumnos/as deberán realizar o traballo de forma individual, salvo que o profesorado comuníquelles explícitamente a autorización para realizalo en grupo.

Avaliación extraordinaria

Só podrán optar á avaliación extraordinaria quen non supere a primeira oportunidade (ao finalizar o cuadrimestre). A avaliación será a descrita nos apartados anteriores, pero adicionalmente será necesario presentar un *dossier,* que deberá ser defendido presencialmente ante o profesorado, no que se inclúan todos os detalles sobre a realización das distintas tarefas, moi especialmente o proxecto.

Quen seguise a avaliación continua pode optar por manter as notas obtidas na primeira oportunidade para as distintas partes da materia ou descartalas.

Outros comentarios

As puntuacións obtidas só son válidas para o curso académico en vigor. Aínda que o proxecto se desenvolverá (na medida do posible) en grupos, o alumnado debe gardar evidencias do seu traballo individual dentro do grupo. No caso no que o rendemento dun alumno ou alumna non sexa acorde ao dos seus compañeiros de grupo, se considerará a súa expulsión do mesmo e/ou podrá ser avaliado/a de forma completamente individual nesta parte.

O uso de calquera material durante a realización dos exámenes tendrá que ser autorizado explícitamente polo profesorado.

En caso de detección de plaxio ou de comportamento non ético nalgún dos traballos/probas realizadas, a calificación da materia será de "suspenso (0)" e os profesores comunicarán o asunto ás autoridades académicas para que tomen as medidas oportunas.

Bibliografía. Fontes de información

Basic Bibliography

Brian Russell, Drew Van Duren,, **Practical Internet of Things Security**, 978-1788625821, 2, Packt Publishing, 2018

Eric Knapp, Joel Thomas Langill, **Industrial Network Security**, Elsevier, 2014

Junaid Ahmed Zubairi, **Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies.**, GI Global, 2012

Tyson Macaulay,, **Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.,**, Auerbach Publications, 2012

Josiah Dykstra, **Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems**, O'Reilly, 2015

Pascal Ackerman, **Industrial Cybersecurity,**, Packt, 2017

Complementary Bibliography

Houbing Song, Glenn A. Fink, Sabina Jeschke, **Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.**, 978-1-119-22604-8, 1, Wiley, 2015

Adam Shostack, **Threat Modeling. Designing for Security**, 978-1118809990, 1, Wiley, 2014

Peng Cheng, Heng Zhang, Jiming Chen, **Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop.**, CRC Press, 2016

Recomendacións

IDENTIFYING DATA				
Ethical Hacking and Intrusion Test				
Subject	Ethical Hacking and Intrusion Test			
Code	V05M175V11214			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Costa Montenegro, Enrique			
Lecturers	Carballal Mato, Adrián Costa Montenegro, Enrique			
E-mail	kike@gti.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530110&any_academic=2023_24			
General description	There is no better way to prove the strength of a system than to attack it. The Intrusion Tests serve to reproduce access attempts of an attacker using the vulnerabilities that may exist in a given infrastructure. In this course the fundamental topics oriented to the intrusion tests (pentesting) will be covered, covering the different phases of an attack and exploitation (from the recognition and control of access to the erasure of tracks).			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents
Topic

Planning			
	Class hours	Hours outside the classroom	Total hours

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

Methodologies
Description

Personalized assistance

Assessment		
Description	Qualification	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA

Business in cybersecurity and entrepreneurship

Subject	Business in cybersecurity and entrepreneurship			
Code	V05M175V11215			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	4	Mandatory	1st	2nd
Teaching language				
Department				
Coordinator	Fernández Vilas, Ana			
Lecturers	Carneiro Díaz, Victor Manuel Fernández Vilas, Ana			
E-mail	avilas@uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530111&any_academic=2023_24&any_academic=2023_24			
General description	In the subject Business in cybersecurity and entrepreneurship, security is approached as a transversal element in the organization, from the strategic and business generation point of view. Different approaches to the monetization of data and their security are presented, as well as the different professional profiles present in the organization, focusing on the operation of a Security Operation Center (SOC) and its associated tools. Finally, different cases of success and business opportunities oriented to different productive sectors are addressed, with special attention to entrepreneurship.			

Training and Learning Results

Code

Expected results from this subject

Expected results from this subject	Training and Learning Results

Contents

Topic

Planning

	Class hours	Hours outside the classroom	Total hours

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

Methodologies

	Description

Personalized assistance

Assessment

Description	Qualification	Training and Learning Results

Other comments on the Evaluation

Sources of information

Basic Bibliography

Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Forensic analysis				
Subject	Forensic analysis			
Code	V05M175V11216			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Suárez González, Andrés			
Lecturers	Suárez González, Andrés Vázquez Naya, José Manuel			
E-mail	asuarez@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530112&any_academic=2023_24			
General description	Computer forensic analysis is the application of scientific and analytical techniques to identify, preserve, analyse and present data that is valid in legal proceedings. This subject has a strong practical component. It will begin with an introduction to computer forensics, explaining key concepts. Next, the fundamentals and methodologies of forensic analysis will be studied from a generic point of view and applicable to new cases, but also specific examples based on real cases will be studied. In the laboratory practicals, students will learn how to use different forensic analysis tools and will carry out practices simulating real problems.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents
Topic

Planning			
	Class hours	Hours outside the classroom	Total hours
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies	
	Description

Personalized assistance

Assessment		
Description	Qualification	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Data center security				
Subject	Data center security			
Code	V05M175V11217			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Suárez González, Andrés			
Lecturers	Dafonte Vázquez, José Carlos López Rivas, Antonio Daniel Suárez González, Andrés			
E-mail	asuarez@det.uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530113&any_academic=2023_24			
General description	Security in a data processing centre involves the implementation of a variety of physical and logical measures to protect the infrastructure and the data stored in the DPC, with the aim of guaranteeing the availability, confidentiality and integrity of the information and systems critical to an organisation. This course will introduce the different architectures of data centres as well as the auxiliary physical facilities that are necessary for their operation.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents
Topic

Planning			
	Class hours	Hours outside the classroom	Total hours

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

Methodologies	
	Description

Personalized assistance

Assessment		
Description	Qualification	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA				
(*)Seguridade en dispositivos móviles				
Subject	(*)Seguridade en dispositivos móviles			
Code	V05M175V11218			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish Galician English			
Department				
Coordinator	López Bravo, Cristina			
Lecturers	Fernández Caramés, Tiago Manuel López Bravo, Cristina Rivas López, Jose Luis			
E-mail	clbravo@det.uvigo.es			
Web	http://http://moovi.uvigo.gal			
General description	This course presents a general view of security in mobile devices with different characteristics. Based on the study of the architecture of these devices, we will discover their internal operation and which are the main security tools that they include, along with the risks and threats they suffer. We will study how to find, analyze and mitigate the vulnerabilities that affect mobile devices, using forensic analysis tools, secure application development and device management in business environments. The documentation of this course will be in English.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
Introduction: Threats and vulnerabilities that affect mobile devices	
Mobile devices architectures	
Security models in mobile devices	
Writing secure Applications	Permissions Packages management Users management APIs
Data security	
Devices security	
Network security	
Vulnerabilities, exploits and malicious applications	
Forensic analysis of mobile operating systems	
Enterprise Mobile Management Systems (EMM)	

Planning			
	Class hours	Hours outside the classroom	Total hours
Lecturing	9	9	18
Practices through ICT	12	12	24
Objective questions exam	2	14	16
Problem and/or exercise solving	0	5	5
Report of practices, practicum and external practices	0	12	12
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies	
	Description
Lecturing	The professors of the course present the main theoretical contents related to security in mobile devices. Through this methodology competencies B14 and C14 get developed.
Practices through ICT	Students will complete guided and supervised practices. Through this methodology the competencies C14, D3, D8 and D9 get developed.

Personalized assistance	
Methodologies	**Description**
Practices through ICT	The professors of the course will provide individual attention to the students during the course, solving their questions. Questions will be answered during the lab sessions or during tutorial sessions. Teachers will establish timetables for this purpose at the beginning of the course. This schedule will be published on the course website. The tutorial sessions could also be agreed with the teacher by appointment.
Lecturing	The professors of the course will provide individual attention to the students during the course, solving their questions. Questions will be answered during the master sessions or during tutorial sessions (also virtually). Teachers will establish timetables for this purpose at the beginning of the course. This schedule will be published on the course website. The tutorial sessions could also be agreed with the teacher by appointment.

Assessment			
	Description	Qualification	Training and Learning Results
Objective questions exam	Short-questions exam on the theoretical and practical contents reviewed throughout the course, both in the lectures and in the laboratory practices. This exam will be done at the end of the term.	40	
Problem and/or exercise solving	Problem-solving tests where students make use of the acquired knowledge, in both theoretical and practical sessions. This test will be carried out throughout the term, with partial deliveries on the dates indicated by teachers.	25	
Report of practices, practicum and external practices	Students will individually fill questionnaires and/or write practice reports, where the right development and understanding of the practice get probed.	35	

Other comments on the Evaluation

ORDINARY EXAM

Following the guidelines of the degree, two evaluation systems will be offered to students attending this course: continuous assessment and global assessment.

Before the end of the fourth week of the course, students must declare if they opt for the continuous assessment or the global assessment. Those who opt for the continuous assessment system may not be listed as "not presented" if they make a delivery or an assessment test after the communication of their decision.

Continuous assessment system

The final grade of the course will be equal to the weighted arithmetic average of the tests previously indicated. To pass the course the final grade must be greater or equal to five.

Global assessment system

The final grade of the course will be equal to the weighted arithmetic average of the tests previously indicated. In this case, the problem-solving test (troubleshooting) will be done in a single test at the end of the term. To pass the course the final grade must be greater or equal to five.

EXTRAORDINARY EXAM

The assessment will consist in an objective questions exam, a problem-solving exam and delivering the practice reports of all the practices carried out throughout the course.

OTHER COMMENTS

The obtained grades are only valid for the current academic year.

The use of any material during the tests will have to be explicitly authorized.

Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the tests or exams, the final grade will be FAIL (0), and the incident will be reported to the corresponding academic authorities for prosecution.

Sources of information

Basic Bibliography

Dominic Chell, **The mobile application hacker´s handbook**, 1, Jonh Wiley & Sons, 2015

Complementary Bibliography

Joshua Drake, **Android hacker's handbook**, 1, Jonh Wiley & Sons, 2014

Charles Miller, **iOS hacker's handbook**, 1, Jonh Wiley & Sons, 2013

Abhishek Dubey, Anmol Misra, **Android security: attacks and defenses**, 1, CRC Press, 2013

David Thiel, **iOS application security: the definitive guide for hackers and developers**, 1, No Starch Press, 2016

Nikolay Elenkov, **Android security internals: an in-depth guide to Android's security architecture**, 1, No Starch Press, 2015

Andrew Hoog, **iPhone and iOS forensics: investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices**, 1, Syngress/Elsevier, 2011

Recommendations

Other comments

It is recommended to have Linux OS and Java programming skills. It is also recommended, but not indispensable, to have Android programming skills.

IDENTIFYING DATA				
Smart Contracts and dApps				
Subject	Smart Contracts and dApps			
Code	V05M175V11219			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Fernández Iglesias, Manuel José			
Lecturers	Álvarez Sabucedo, Luis Modesto Fernández Caramés, Tiago Manuel Fernández Iglesias, Manuel José			
E-mail	manolo@uvigo.es			
Web				
General description	This course offers students an introductory understanding of the concepts and practices related to the development and deployment of secure smart contracts and decentralized applications. Students will explore the specificities of smart contract programming, and examine various security vulnerabilities and threats specific to smart contracts and decentralized applications. Through hands-on exercises, real-world case examples and classroom discussions, students will learn how to employ best practices to mitigate risks and protect against attacks in the blockchain ecosystem. By the end of the course, students will be equipped with the knowledge and skills to develop secure smart contracts and design resilient decentralized applications that can withstand the challenges of these technologies.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
Basic concepts	Discussion of the basic concepts related to the development of smart contracts and decentralized applications.
Design and development of smart contracts	The development of smart contracts is addressed, taking into account the most relevant security aspects.
Peer-to-peer file systems	The basic characteristics of peer-to-peer networks are presented, followed by a description of the essential elements of decentralized file systems and their relationship with blockchain technologies. IPFS is presented as a case study.
Oracles. Good practices	Oracles are presented as third-party services that provide external data or events to a smart contract in a blockchain. Best practices for their development and use are identified.
Non-fungible tokens	A specific use case very popular in the world of smart contracts and decentralized applications is discussed: non-fungible tokens or NFTs.
BaaS as an outsourcing model	The basic elements of Blockchain as a Service (BaaS) to develop, deploy and manage blockchain applications without the need to set up and maintain blockchain infrastructure are discussed.
Cybersecurity aspects	A recap of the key elements for designing secure smart contracts, oracles and decentralized applications is offered.

Planning			
	Class hours	Hours outside the classroom	Total hours
Lecturing	10.5	22.5	33
Practices through ICT	2.5	5.5	8
Practices through ICT	4	8.5	12.5
Practices through ICT	4	8.5	12.5
Essay questions exam	1.5	3	4.5
Essay questions exam	1.5	3	4.5

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

Methodologies	
	Description
Lecturing	Theoretical concepts and their practical application will be presented in class. Students will be encouraged to participate in the resolution of practical cases (case studies), in such a way that in each class session the teacher's presentation will be combined with the students' participation.
Practices through ICT	Small projects or programming exercises of smart contracts or decentralized applications will be proposed, to be carried out in the laboratory and/or through autonomous work, under the supervision of the teacher. Reference platforms and languages in the field of blockchain will be utilized.
Practices through ICT	Small projects or programming exercises of smart contracts or decentralized applications will be proposed, to be carried out in the laboratory and/or through autonomous work, under the supervision of the teacher. Reference platforms and languages in the field of blockchain will be utilized.
Practices through ICT	Small projects or programming exercises of smart contracts or decentralized applications will be proposed, to be carried out in the laboratory and/or through autonomous work, under the supervision of the teacher. Reference platforms and languages in the field of blockchain will be utilized.

Personalized assistance	
Methodologies	**Description**
Lecturing	Students will have the opportunity to attend personalized tutorial sessions in accordance with the procedure that will be established for this purpose at the beginning of the semester. This procedure will be published on the course website.
Practices through ICT	Students will have the opportunity to attend personalized tutorial sessions in accordance with the procedure that will be established for this purpose at the beginning of the semester. This procedure will be published on the course website.

Assessment			
	Description	Qualification	Training and Learning Results
Practices through ICT	The solution offered to the first course assignment will be evaluated, taking into account the correctness of the proposed solution, the quality of the code, the efficiency of the code, the problem-solving skills and the documentation of the code.	10	
Practices through ICT	The solution offered to the second course assignment will be evaluated, taking into account the correctness of the proposed solution, the quality of the code, the efficiency of the code, the problem-solving skills and the documentation of the code.	20	
Practices through ICT	The solution offered to the third course assignment will be evaluated, taking into account the correctness of the proposed solution, the quality of the code, the efficiency of the code, the problem-solving skills and the documentation of the code.	20	
Essay questions exam	Each student will sit, individually and without any supporting material, a classroom exam in the middle of the semester (the exact date will be published at the beginning of the semester at the course web) about the contents explained up to the week before the exam.	20	
Essay questions exam	Each student will sit, individually and without any supporting material, a classroom exam at the end of the semester (the exact date will be published at the beginning of the semester at the course web) on the totality of the course syllabus.	30	

Other comments on the Evaluation

There are two assessment modalities, continuous assessment (CA) and global assessment (GA), which must be chosen by the students considering the following conditions:

- Both the classroom and lab parts will be evaluated according to the same mechanism, CA or GA, as selected by the student.
- CA includes the exams described in the previous section: two theory exams, design and development of three programming assignments.
- Students will confirm the final evaluation modality (CA or GA) when submitting lab deliverables, depending on the submission date. The chosen evaluation modality will also be applied to the theory/classroom part. Therefore, in the case that a student finally chooses GA, the grade of the first classroom exam, if any, would be discarded.

- Regardless of the chosen evaluation modality, lab assignments will always be carried out individually.
- A minimum grade of 2 points (out of 5) in both theory/classroom and lab parts is required to pass the course.
- If the grade resulting from adding the classroom and lab grades is equal or higher than 5 points, but the student does not reach the minimum grade required in any of them, his/her final grade will be Fail (4.5).
- If a student attends any of the evaluation tests of the course, he/she will not be able to appear in transcripts as "no-show".
- The CA tests will only take place on the dates established by the lecturers, and cannot be resit or delayed.
- Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the tests or exams, the final grade will be *Fail(0)*, and the incident will be reported to the corresponding academic authorities for prosecution.

Assessment procedure for the ordinary call for students who opt for Continuous Assessment (CA)

- **Theory/classroom part (50%)**: The grade of this part (5 points) is obtained by adding the corresponding grades of the two classroom exams (midterm and end-of-semester), with maximum grades of 2 and 3 points, respectively.
- **Lab part (50%)**: The grade for this part depends on the grades obtained in each lab assignment (up to 1, 2 and 2 points respectively, up to 5 points in total).

Students who do not pass the course in the ordinary opportunity, may redeem the grade obtained in both theory and lab for the extraordinary opportunity, as long as they have achieved the minimum grade required in the part they wish to keep (2 points out of 5, in both cases).

Assessment procedure for the ordinary call for students who opt for Global Assessment (GA):

- **Classroom part (50%)**: The grade of this part (5 points) corresponds to an individual exam without any type of supporting material at the end of the academic semester (on the date approved by the school).
- **Lab part (50%)**: The grade for this part depends on the grades obtained in the three assignments (up to 1, 2 and 2 points respectively, up to 5 points in total). The deliverables may be identical to those required in CA or include modifications in the functionalities to be developed. They will be delivered in digital format and will be evaluated by lecturers outside lab sessions.

Assessment procedure for the extraordinary call and end-of-program call:

- **Classroom part (50%)**. Individual exam on the date to be approved by the school, requiring a minimum grade of 2 points (out of 5).
- **Lab part (50%)**. The corresponding assignments must be submitted in digital. Assignments may be the same CA/GA assignments or may include modifications in functionality and/or scoring. As there is no CA, assessment procedures are the same as as ordinary call's GA.

Sources of information

Basic Bibliography

Lorne Lantz e Daniel Cawrey, **Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications**, 978-1492054702, O□Reilly Media., 2020

Daniel Drescher, **Blockchain Basics:A Non-Technical Introduction in 25 Steps**, 978-1484226032, Apress, 2017

Don Tapscott e Alex Tapscott, **Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World**, 978-1101980149, New enlarged edition, Penguin Publishing Group, 2018

Paul Vigna e Michae lJ. Case, **The Truth Machine: The Blockchain and the Future of Everything**, 978-0008301774, Harper Collins, 2019

Manuel J. Fernández Iglesias, **Introduction to Blockchain, Smart Contracts and Decentralized Applications**, bit.ly/intro_ciad, 2023

Complementary Bibliography

Andreas M. Antonopoulos, **The Internet of Money**, 978-1537000459, CreateSpace Independent Publishing Platform, 2016

Ethereum.org, **Ethereum Development Tutorials**, https://ethereum.org/en/developers/tutorials/, 2023

Bina Ramamurthy, **Blockchain Basics**, https://www.coursera.org/learn/blockchain-basics, Coursera, 2023

Mark Parzygnat, **IBM Blockchain 101: Quick-start guide for developers**, https://bit.ly/ibm_bc_basics, IBM Developer, 2023

Recommendations

Subjects that it is recommended to have taken before

Distributed ledger and Blockchain technologies/V05M175V11113