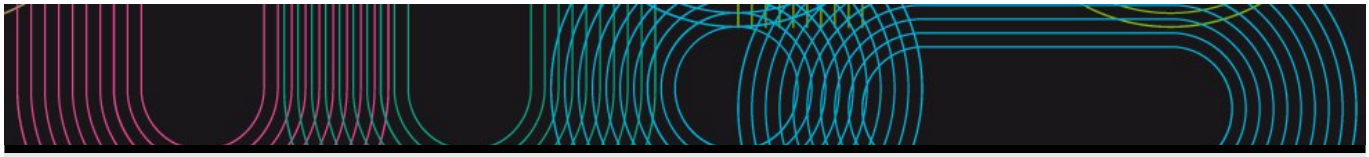

IDENTIFYING DATA				
Communications security				
Subject	Communications security			
Code	V05M175V11211			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Rodríguez Rubio, 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