Teaching Guide				
Identifying Data				2019/20
Subject (*)	Ubiquitous Security		Code	614530013
Study programme	Máster Universitario en Ciberseguridade			
Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	2nd four-month period	First	Optional	3
Language	SpanishGalician			
Teaching method	Face-to-face			
Prerequisites				
Department	Ciencias da Computación e Tecnoloxías da Información			
Coordinador	Rabuñal Dopico, Juan Ramon	E-mail	juan.rabunal@udc.es	
Lecturers	Martinez Perez, Maria Rabuñal Dopico, Juan Ramon Rodríguez Tajes, Álvaro	E-mail	maria.martinez@udc.es juan.rabunal@udc.es a.tajes@udc.es	
Web	faitic.uvigo.es			
General description	Coordinated by the University of Vigo. Check the guide in: https://secretaria.uvigo.gal/docnet-nuevo/guia_docent/?centre=305			

Study programme competences	
Code	Study programme competences
A4	CE4 - To understand and to apply the methods and tools of cybersecurity to protect data and computers, communication networks, databases, computer programs and information services
A9	CE9 - Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity
B2	CB2 - Students will be able to apply their knowledge and their problem-solving ability in new or less familiar situations, within a broader context (or in multi-discipline contexts) related to their field of specialization
B3	CB3 - Students will be able to integrate diverse knowledge areas, and address the complexity of making statements on the basis of information which, notwithstanding incomplete or limited, may include thoughts about the ethical and social responsibilities entailed to the application of their professional capabilities and judgements
B4	CB4 - Students will learn to communicate their conclusions ---and the hypotheses and ultimate reasoning in their support--- to expert and nonexpert audiences in a clear and unambiguous way
B6	CG1 - To have skills for analysis and synthesis. To have ability to project, model, calculate and design solutions in the area of information, network or system security in every application area
B7	CG2 - Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security
B10	CG5 - Students will have ability to apply theoretical knowledge to practical situations, within the scope of infrastructures, equipment or specific application domains, and designed for precise operating requirements
C4	CT4 - Ability to ponder the importance of information security in the economic progress of society
C5	CT5 - Ability for oral and written communication in English

Learning outcomes			
Learning outcomes	Study programme competences		
Coñecer a seguridade nas diferentes capas relacionadas cos sistemas ubicuos e as tecnoloxías que utilizan.	AJ4 AJ9	BJ2 BJ3 BJ4 BJ6 BJ7 BJ10	CJ4 CJ5

Entender os problemas de seguridade asociados ao mundo ubicuo.	AJ4 AJ9	BJ2 BJ3 BJ4 BJ6 BJ10	CJ4 CJ5
Coñecer casos reais de ataques a sistemas ubicuos.	AJ4	BJ2 BJ3 BJ4 BJ10	CJ4 CJ5

Contents	
Topic	**Sub-topic**
Seguridade física	Elementos de hardware. Compoñentes. - Buses de comunicación. - Interfaces. - Hardware criptográfico. Ataques.
Seguridade no middleware	Seguridade no proceso de arrinque. Seguridade no sistema operativo. Control de acceso. Cifrado. Actualización do firmware.
Seguridade nas comunicacións	Comunicacións sen fíos. Riscos e ameazas nas comunicacións
Seguridade na percepción do contorno	Ataques nos sistemas de posicionamento. Ataques ás medidas dos sensores. Privacidade

Planning				
Methodologies / tests	**Competencies**	**Ordinary class hours**	**Student?s personal work hours**	**Total hours**
Guest lecture / keynote speech	A4 A9 B2 B3 B4 B6 B7 B10 C5 C4	10	20	30
Laboratory practice	A4 A9 B2 B3 B4 B6 B7	10	35	45
Personalized attention		0		0
(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.				

Methodologies	
Methodologies	**Description**
Guest lecture / keynote speech	Realización en grupo do deseño, implementación e proba dun sistema IoT, poñendo especial énfase na seguridade. Realización en grupo de ataques á seguridade dos sistemas implementados por outros compañeiros ou de terceiros. Con esta metodoloxía traballaranse as competencias CB2, CB3, CB4, CG1, CG2, CG5, CE4, CE9, CT4 e CT5.
Laboratory practice	Exposición, por parte dos profesores, dos principais contidos teóricos relacionados coa seguridade para sistemas ubicuos (seguridade empotrada, nas comunicacións e nos backends) Con esta metodoloxía contribuirase a adquisición das competencias CB2, CB3, CB4, CG1, CG2, CE4 e CE9.

Personalized attention	
Methodologies	**Description**
Laboratory practice Guest lecture / keynote speech	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse de forma presencial (durante a propia sesión maxistral, ou durante o horario establecido para as titorias). O horario de titorias establecerase ao principio do curso e publicarase na páxina web da materia.

Assessment			
Methodologies	**Competencies**	**Description**	**Qualification**
Laboratory practice	A4 A9 B2 B3 B4 B6 B7	O alumnado dividirase en grupos para a realización do deseño, implementación e proba dun sistema IoT, poñendo especial énfase na seguridade. O mesmo grupo realizará ataques á seguridade dos sistemas implementados por outros compañeiros ou por terceiros. O proxecto realizado, e o informe contendo o resultado dos ataques completados (en canto á súa calidade e ao seu éxito) serán avaliados despois da súa entrega valorando aspectos como 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. Se os resultados intermedios non son satisfactorios, poderase aplicar unha penalización de ata o 20% da nota. O seguimento será grupal e individual: cada un dos membros do grupo debe documentar as tarefas desenvolvidas dentro do seu equipo e responder sobre elas.	80
Guest lecture / keynote speech	A4 A9 B2 B3 B4 B6 B7 B10 C5 C4	Realizaranse un ou varios exames para avaliar a comprensión dos contidos presentados nas sesións maxistrais. De haber máis de un exame, a nota final será a media aritmética das distintas probas	20

Assessment comments

Para superar a materia é necesario completar as distintas partes nas que se divide (exame ou exames acerca dos contidos expostos na sesión maxistral e proxectos). 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, e a nota do proxecto é NP, a nota final será:
Nota = NT^0.2 ? NP^0.8
Durante o primeiro mes, os estudantes deberán indicar explicitamente e por escrito o seu desexo de cursar a materia seguindo a avaliación única. Noutro caso considerarase que seguen a avaliación continua. Aqueles que sigan a avaliacióncontinua non se poderán considerar "non presentados" unha vez se realice a entrega do primeiro cuestionario ou tarefa.
Os alumnos que opten pola avaliación única deberán presentar adicionalmente un dossier que deberá defender presencialmente ante os profesores, onde se inclúan tódolos detalles sobre a realización das distintas tarefas, moi especialmente o proxecto. No caso de seguir a avaliación única, os alumnos deberán realizar o traballo de forma individual, salvo que o profesorado lles comunique explicitamente a autorización para realizalo en grupo.
Segunda oportunidade
Só poderán optar á segunda oportunidade aqueles alumnos que non superaron a primeira oportunidade (ao finalizar o cuadrimestre). A avaliación será a descrita nos apartados anteriores, pero adicionalmente será preciso presentar un dossier que deberá ser defendido presencialmente ante os profesores, onde se inclúan tódolos detalles sobre a realización das distintas tarefas, moi especialmente o proxecto.
Aqueles estudantes que seguisen a avaliación continua poden 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, os alumnos deben deixar 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, considerarase a súa expulsión do mesmo e/ou poderá ser avaliado de forma individual nesta parte.
O uso de calquera material durante a realización dos exames terá que ser autorizado explicitamente polo profesorado.
En caso de detección de plaxio ou de comportamento non ético nalgún dos traballos/probas realizadas, a cualificación final da materia será de "suspenso (0)" e os profesores comunicarán o asunto ás autoridades académicas para que tome as medidas oportunas.

Sources of information	
Basic	- Brian Russell, Drew Van Duren (2016). Practical Internet of Things Security. Packt Publishing
Complementary	- Houbing Song, Glenn A. Fink, Sabina Jeschke (2018). Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.. Wiley - Bruce Schneider (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley

Recommendations
Subjects that it is recommended to have taken before
Information Security/614530003 Penetration Testing/614530008 Operating Systems Hardening/614530007 Communications Security/614530004 Applications Security/614530005 Secure Networks/614530006
Subjects that are recommended to be taken simultaneously
Subjects that continue the syllabus
Other comments

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.