IDENTIFYING DATA

Ubiquituous Security

Subject	Ubiquituous Security			
Code	V05M175V01208			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish Galician			
Department				
Coordinator	Gil Castiñeira, Felipe José			
Lecturers	Gil Castiñeira, Felipe José Rabuñal Dopico, Juan Ramón			
E-mail	felipe@uvigo.es			
Web	http://faitic.uvigo.es			
General description	Intelligent devices are providing new services and we are almost unaware of their presence: our car is not anymore a mechanical machine, as it became a connected device where electronics suppose an important part; in hotels, we no longer use a key as we can open our room with a card or with our mobile phone; our home thermostats can be connected to a weather forecasting service to take advantage of the temperature of the environment. Those are all examples of the applications that allow embedded technologies, wireless communication networks, and in summary, the "Internet of Things" (IoT). This subject analyzes the problems and the best practices to make this kind of systems secure.			

Competencies

Code	
A2	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.
A3	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.
A4	Students will learn to communicate their conclusions ---and the hypotheses and ultimate reasoning in their support--- to expert and non-expert audiences in a clear and unambiguous way.
B1	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.
B2	Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security.
B5	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	To understand and to apply the methods and tools of cybersecurity to protect data and computers, communication networks, databases, computer programs and information services.
C9	Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity.
D4	Ability to ponder the importance of information security in the economic progress of society.
D5	Ability for oral and written communication in English.

Learning outcomes

Expected results from this subject	Training and Learning Results

Gain knowledge of the security in the different layers of an ubiquitous system and the used technologies.	A2 A3 A4 B1 B2 B5 C4 C9 D4 D5
Understand the security problems related to the ubiquitous field.	A2 A3 A4 B1 B2 B5 C4 C9 D4 D5
To know real cases of attacks to ubiquitous systems.	A2 A3 A4 B5 C4 D4 D5

Contents

Topic	
Physical security	Hardware components. - Communication buses. - Interfaces. - Cryptographyc hardware. Attacks.
Middleware security	Security during the startup process. Security in the operating system. Access control. Cyphering. Firmware updates.
Communication security	Wireless communications. Risks and threats for communications.
Security in the perception of the environment	Attacks in the positioning system. Attacks to sensor measurements. Privacy.

Planning

	Class hours	Hours outside the classroom	Total hours
Project based learning	10	35	45
Lecturing	10	20	30

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

Methodologies

	Description
Project based learning	Work in groups in the design, implementation and validation of an IoT system, with a special emphasis in the security. Perform attacks to the security of the systems implemented by the other groups or implemented by third parties. This methodology will contribute to acquire competences CB2, CB3, CB4, CG1, CG2, CG5, CE4, CE9, CT4 and CT5.

Lecturing	Professors will present the main theoretical contents related to the security for ubiquitous systems (security for embedded systems, communications and backends). This methodology will contribute to the acquisition of competences CB2, CB3, CB4, CG1, CG2, CE4 and CE9.

Personalized assistance

Methodologies	Description
Lecturing	The professors of the course will provide individual attention to the students during the course, solving their doubts and questions. Questions will be answered during the master sessions or during tutorial sessions. Professors will establish timetables for this purpose at the beginning of the course. This schedule will be published on the subject website.
Project based learning	The professors of the course will provide individual attention to the students during the course, solving their doubts and questions. The professors will guide and help the students to complete the assigned project. Questions will be answered during the supervising sessions, group supervising 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 subject website.

Assessment

	Description	Qualification	Training and Learning Results
Project based learning	The students will work in groups in the design, implementation and proof of an IoT, with a special emphasis in security. The same group of students will perform attacks to the security of the systems implemented by other groups or by third parties. The results (project and reports containing the outcomes of the attacks) will be evaluated after the delivery, having into account key aspects such as the correction, the quality, the performance and the functionalities. It will be mandatory to deliver the code, prototypes and documentation. It will be also necessary make a public presentation of the results. In addition, during the implementation of the project, the design and the evolution of the development will be evaluated. If the intermediate results are not satisfactory, a penalization of the 20% of the grade could be applied. The evaluation will be by group and by person: each one of the members of a team must document his/her tasks and answer the questions related to them.	80	A2 B1 C4 D4 A3 B2 C9 D5 A4 B5
Lecturing	Students will complete one or several exams to asses what they have learned in master lessons. In case there is more than one exam, the result will be the arithmetic mean of the different tests.	20	A2 B1 C4 A3 B2 C9 A4

Other comments on the Evaluation

In order to pass the course it is necessary to complete the different parts of the subject (exam or exams about the master sessions and project). The final grade will be the **weighted geometric mean** of the grades of the different parts. For example, If "NT" is the grade obtained for the master sessions and "NP" for the project, the final grade will be:

Grade = NT^0.2 × NP^0.8

During the first month, students must provide a written declaration to opt for single evaluation. In other case, it will be considered that they opt for continuous evaluation. Students who select continuous evaluation and submit the first task or questionnaire may not be listed as "Absent".

Students who opt for the final assessment procedure have to submit also a dossier that must be defended in-person in front of the professors, with detailed information about the events and issues that arose during the execution of the different tasks, and especially the project. In addition, during the first month of the course, professors will notify students who opted for final assessment if they have to do the tutored work individually.

Second call to pass the course

Students can opt to the second call only if they didn't pass the first call (at the end of the semester).

The evaluation procedure is the presented in the previous sections, but t will be necessary to submit an additional dossier that must be defended in-person in front of the professors, with detailed information about the events and issues that arose during the execution of the different tasks, and especially the project.

Students that have opted by the continuous evaluation procedure, can decide to maintain the grades of the different parts of the subject obtained in the first call or discard them.

Other comments

Although the project will be completed (if possible) in groups, each student should keep a record of his or her activities. In the case in which the performance of a member of the group wouldn't be adequate compared with the performance of his or her team mates, he or she could be excluded from the group and/or qualified individually.

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

In case of detection of plagiarism or unethical behavior in any of the tasks/tests done, the final grade will be "failed (0)" and the professors will communicate the incident to the academic authorities to take the appropriate measures.

Sources of information

Basic Bibliography

Brian Russell, Drew Van Duren, **Practical Internet of Things Security**, 1, Packt Publishing, 2016

Complementary Bibliography

Houbing Song, Glenn A. Fink, Sabina Jeschke, **Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.**, 1, Wiley, 2018

Bruce Schneider, **Applied Cryptography: Protocols, Algorithms and Source Code in C**, 2, Wiley, 2015

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

Recommendations

Subjects that it is recommended to have taken before

Hardening of Operating Systems/V05M175V01202
Secure Networks/V05M175V01105
Applications Security/V05M175V01104
Information Security/V05M175V01102
Secure Communications/V05M175V01103
Intrusion tests/V05M175V01203