UniversidadeVigo

IDENTIFYING DATA

Security in Mobile Devices				
Subject	Security in Mobile Devices			
Code	V05M175V01206			
Study programme	(*)Máster Universitario en Ciberseguridade			
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://faitic.uvigo.es			
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.			

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.
C6	To develop and apply forensic research techniques for analysing incidents or cybersecurity threats.
C9	Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity.
C15	Ability to identify the value of information for an institution, economic or of other sort; ability to identify the critical procedures in an institution, and the impact due to their disruption; ability to identify the internal and external requirements that guarantee readiness upon security attacks.
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

Knowing the fundamental concepts associated with security in mobile operating systems and the development of secure apps.	A2 B1 C4 C15 D4 D5
Identifying an app with malicious behavior and vulnerabilities in operating systems and apps	A4 B2 C4 D4 D5
Being able to perform a forensic analysis of a mobile device	A3 B2 C6 D5
Knowing the fundamentals of mobile device management systems	A2 B1 B2 B5 C9 D5

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 assurance	
Devices assurance	
Network assurance	
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	10	10	20
Objective questions exam	2	14	16
Problem and/or exercise solving	0	11	11
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	The professors of the course present the main theoretical contents related to security in mobile devices. Through this methodology competencies CB3, CG1, CE4, CE15, and CT4 get developed.
Practices through ICT	Students will complete guided and supervised practices. Through this methodology the competencies CG2, CG5, CB2, CB4, CE4, CE6, and CE9 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 bimester.	50	A3 C4 A4
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 bimester, with partial deliveries on the dates indicated by teachers.	20	A2 B1 C4 A4 B2
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.	30	A4 B5 C4 D4 C6 C9 C15

Other comments on the Evaluation

FIRST CALL

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

Before the end of the second week of the course, students must declare if they opt for the continuous assessment or the eventual 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.

Eventual 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 bimester. To pass the course the final grade must be greater or equal to five.

SECOND CALL

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, John Wiley & Sons, 2014

Charles Miller, **iOS hacker's handbook**, 1, John Wiley & Sons, 2012

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

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.

Contingency plan

Description

In case of online tuition, the methodologies used and the tests performed will be the same as in the case of in-person tuition. The only expected modification is that they will be carried out via Remote Camnpus and Faitic, instead of the School classrooms and laboratories.

In case of online assessment, the weight of the different evaluation proofs would be the following:

- Objective questions exam: 30 %
- Problem and/or exercise solving: 30 %
- Report of practices: 40 %

COMPLEMENTARY REFERENCES
- Platform Architecture - Android Developers: https://developer.android.com/guide/platform/ - Android Secure: https://source.android.com/security
- Android Enterprise: https://www.android.com/enterprise/
- Mobile Threat Catalogue - NIST: https://pages.nist.gov/mobile-threat-catalogue/
- OWASP Mobile Security Project: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- ENISA: Smartphone Secure Development Guidelines: https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016
- Guía de Seguridad de las TIC CCN-STIC 453E. SEGURIDAD DE DISPOSITIVOS MÓVILES: ANDROID 9.x. Centro Criptográfico Nacional. NIPO: 083-19-015-2: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/3588-ccnstic-453g-guia-practica-de-seguridad-en-dispositvos-moviles-android-9/file.html
- Guía de seguridad de las TIC (CCN-STIC-457): Gestión de dispositivos móviles: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-accesopublico-ccn-stic/14-ccn-stic-457-herramienta-de-gestion-dedispositivos-moviles-mdm/file.html