Mobile devices security

Academic Year: (2023 / 2024) **Review date: 28-04-2023**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: PERIS LOPEZ, PEDRO

Type: Compulsory ECTS Credits : 6.0

Year : 4 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Cryptography and Computer Security (course 3 / semester 1).
Computer Networks (course 3 / semester 1).
Security Engineering applied to computer engineering / to information systems (course 3 / semester 2).

OBJECTIVES

CG2 - Being able to generate new ideas (creativity) and anticipate new situations and adapt to Working in a team and interacting with others, but at the same time having the ability to work autonomously.
CGB4 - Basic knowledge of the use and programming of computers, operating systems, databases and software with application in engineering.
CGB5 - Knowledge of the structure, organisation, operation and interconnection of computer systems, the fundamentals of their programming, and their application to the resolution of engineering problems.
CG9 - Efficient use of ICT resources to write technical reports and project and work reports on IT and quality presentations.
CGO3 - Ability to design, develop, evaluate and ensure the accessibility, ergonomics, usability and security of computer systems, services and applications, as well as the information they manage.
CGO6 - Ability to conceive and develop centralised or distributed computer systems or architectures integrating hardware, software, and networks according to the knowledge acquired.
CGO8 - Knowledge of basic subjects and technologies, which enable them to learn and develop new methods and technologies and those that provide them with great versatility to adapt to new situations.
CGO9 - Ability to solve problems with initiative, decision-making, autonomy and creativity. Ability to know how to communicate and transmit the knowledge, skills and capabilities of the Technical Engineer in Computer Science.
CB3 - Students can gather and interpret relevant data (normally within their area of study) to make judgments that include reflection on relevant social, scientific or ethical issues.
CB5 - Students have developed those learning skills necessary to undertake further study with a high degree of autonomy.
CECRI10 - Knowledge of the characteristics, functionalities and structure of Operating Systems and design and implement applications based on their services.
CECRI11 - Knowledge and application of the characteristics, functionalities and structure of Distributed Systems, Computer Networks and the Internet and design and implement applications based on them.
CECRI18 - Knowledge of the regulation of Computer Science in the national, European and international contexts

DESCRIPTION OF CONTENTS: PROGRAMME

1. Mobile computing security overview
2. Mobile infrastructure vulnerabilities
   a. Vulnerabilities
   b. Mitigation techniques
3. Mobile communication vulnerabilities
   a. Vulnerabilities
   b. Mitigation techniques
4. Mobile device vulnerabilities
   a. Vulnerabilities
   b. Mitigation techniques
5. Mobile platform vulnerabilities
   a. Vulnerabilities
   b. Mitigation techniques
6. Mobile application vulnerabilities
   a. Vulnerabilities

b. Mitigation techniques

LEARNING ACTIVITIES AND METHODOLOGY

AF1. THEORETICAL-PRACTICAL CLASSES. 1.5 ECTS with full attendance. They will present the knowledge that students should acquire. They will receive the class notes and will have basic reference documents to facilitate the follow-up of the classes and the development of the subsequent work. Exercises and problems that students may have, will be solved and workshops and evaluation tests will be carried out to develope the necessary skills.
AF2. TUTORIALS. 0.25 ECTS with full attendance. Individualized (individual tutorials) or group (collective tutorials) assistance to students will be provided by the teacher.
AF3. INDIVIDUAL OR GROUP STUDENT WORK. 3.75 ECTS with 0% attendance
AF8: WORKSHOPS AND LABORATORIES 0.25 ECTS with full attendance
AF9: FINAL EXAM. 0.25 ECTS with full attendance. In which the knowledge, skills and abilities acquired throughout the course will be assessed globally.

MD1: CLASS THEORY. Exhibitions in the teacher's class with support of computer and audiovisual media, in which the main concepts of the subject are developed and materials and bibliography are provided to complement the students' learning.
MD2: PRACTICES. Resolution of practical cases, problems, etc. raised by the teacher individually or in groups.
MD3: TUTORIALS. Individualized assistance (individual tutorials) or group (collective tutorials) to students by the teacher.
MD6: LABORATORY PRACTICES. Applied / experimental teaching to workshops and laboratories under the supervision of a tutor.

ASSESSMENT SYSTEM

SE1: FINAL EXAMINATION In which the knowledge, skills and abilities acquired throughout the course will be assessed globally.

SE2: CONTINUOUS EVALUATION. Work, presentations, debates, exhibitions in class, exercises, practices and work in the workshops throughout the course will be evaluated.

% end-of-term-examination:	30
% of continuous assessment (assigments, laboratory, practicals…):	70

BASIC BIBLIOGRAPHY

- Androulidakis, I. Mobile Phone Security and Forensics: A Practical Approach. , Springer, 2012

- Bergman, N., Stanfield, M., Rouse, J., Scambray, J., et al. Hacking Exposed Mobile: Security Secrets & Solutions. , McGraw Hill Osbourne Media: New York, NY, 2013
- Buttyan, L. and Hubaux, J. Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing. , Cambridge University Press, 2007

ADDITIONAL BIBLIOGRAPHY

- Jeff Six Application Security for the Android Platform, O'Really Media, Inc, 2011

- Johnny Cache, Joshua Wright, Vincent Liu. Hacking wireless exposed: wireless security secrets and solutions., McGraw-Hill, 2010
- Pragati Ogal Rai Android Application Security Essentials, Packt Publishing, 2013

BASIC ELECTRONIC RESOURCES

- Apple Inc. . iOS security guide: https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf
- Google Inc. . Android security for developers: https://developer.android.com/topic/security