Mobile devices security

Academic Year: (2019 / 2020) **Review date: 22-04-2020**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: FUENTES GARCIA ROMERO DE TEJADA, JOSE MARIA

Type: Compulsory ECTS Credits : 6.0

Year : 5 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Cryptography and Computer Security
Computer Networks
Security Engineering

OBJECTIVES

The inner features of mobile devices such as their size (small and usually constrained in terms of energy and computational resources) and their use of a wireless channel, makes many of the traditional security mechanisms useless. As a consequence lightweight mechanisms and physical security become important.

The goal of the course is to make the student able to manage the particular techniques needed to guarantee security in a mobile computing scenario.

In order to fulfill this goal, students must acquire certain knowledge, capacities and attitudes. (PO: a, b, c, d, e, f, g, h,, j, k)

Regarding knowledge, students will be able to:
- Understand the security risks inherent to a mobile scenario. (PO: b, e, j)
- Know the physical security measures that can be applied to mobile devices. (PO: b, e, j)
- Master the fundamental techniques to protect the information stored in mobile devices. (PO: a, b, c, e, f, j, k)
- To have a good command of the main security protocols that rule mobile communications. (PO: a, e)

Regarding capacities, students will be able to:
- Analyze the vulnerabilities in a mobile computing scenario. (PO: b, e, j, k)
- Design and deploy the appropriate security mechanisms to guarantee a predefined security level. (PO: a, b, c, d, e, j, k)

Regarding attitudes, students will adopt:
- A suspicious attitude towards security in mobile devices. (PO: e, g, h, j)
- A curious attitude in order to find new vulnerabilities in the open systems where these devices are usually deployed. (PO: e, j, k)
- An analytical perspective of technology that allows them to apply appropriate solutions to the particular security problems this kind of devices faces. (PO: e, h, j, k)

DESCRIPTION OF CONTENTS: PROGRAMME

The course is divided into five blocks:

1. Introduction to the security of wireless networks
1.1. Measures and security mechanisms in mobile devices
1.2. Types of Networks in wireless communications.
1.3. fundamental in the provision of information security primitives:
confidentiality, integrity, authentication, non-repudiation, etc.
1.4. Objectives of security in wireless communications.
1.5. Vulnerabilities, risks, threats in wireless communications.

2. Measures and security mechanisms on mobile devices
2.1. technical security measures on Android and iOS systems

2.1.1. ID
2.1.2. Authentication
2.1.3. Access control
2.1.4. Confidentiality
2.1.5. Non-repudiation
2.1.6. Traceability
2.2. Security mechanisms on Android and IOS systems
2.2.1. Process Isolation (Sandboxing)
2.2.2. Credential-based access control
2.2.3. Origin of applications
2.2.4. Confidentiality
2.2.5. Kill switch
2.2.6. Remote wipe and location
2.2.7. Backups (backups)
2.2.8. Updates

3. Security in Wireless Local Area Networks (WLAN)
3.1. Fundamentals of Network Security WLAN- Authentication, Integrity Management
Key, Encryption, Attacks
3.2. Wired Equivalent Privacy (WEP)
3.3. Wi-Fi Protected Access (WPA - WPA2)
3.4. Extensible Authentication Protocol (EAP)
3.4.1. IEEE 802.1x technology
4. Security in mobile communications
4.1. Technical Security on Android and iOS systems
4.1.1. GSM
4.1.2. GPRS - EDGE
4.1.3. UMTS, LTE
4.1.4. 5G
5. Security systems based on radio frequency identification devices
(RFID) in mobile communications
5.1. Specific mechanisms for low power devices computing
5.1.1. Authentication
5.1.2. Confidentiality
5.1.3. Encryption

LEARNING ACTIVITIES AND METHODOLOGY

(1) Lectures to explain the main theoretical and practical concepts. Slides and documentation will be provided to students. Complementary bibliography will be pointed out to complete each topic. (PO: a, e, j, k)
(2) Projects will be developed through a design problem under initial specifications, where the students have to analyze requirements and provide a working solution (P.O: a, b, c, d, e, g, j, k)
(3) Critical analysis of a research paper or security-related technology. Report and, eventually, oral presentation by the students (P.O: a, d, f, g, h, i, j).

ASSESSMENT SYSTEM

1. ORDINARY SITTING
1.1. CONTINUOUS ASSESSMENT
The assessment process will be based on the following criteria:
- Practical case resolution during the course (compulsory): 40% (P.O: a, b, c, d, e, f, g, j, k)
- Presentation of a report about a specific topic (compulsory): 20% (P.O: a, d, f, g, h, i, j).
- Final examination (compulsory): 40% (P.O: a, b, c, e, f, g, h, j).
Attendance and active participation in class may be considered to obtain extra points.

In order to pass, the student must fulfill two conditions:
- To obtain in the final examination a grade equal or higher than 4 points over 10.
- The sum of the grades of every part must be, at least, the 50% of the maximum possible mark.
1.2. NON-CONTINUOUS ASSESSMENT
The assessment process will be based on the following criteria:
- Final examination (compulsory): 60% (P.O: a, b, c, e, f, g, h, i, j, k).
The exam will contain specific parts to assess the knowledge that should have been acquired by performing the requested assignments.

In order to pass, the student must fulfill two conditions:
- The student must get 5.0 marks out of 10.0
2. EXTRAORDINARY SITTING

2.1. IF THE STUDENT FOLLOWED THE CONTINUOUS ASSESSMENT IN THE ORDINARY SITTING
The assessment process will be based on the following criteria:
- Grades from the practical case and the report are preserved (60%)
- Final examination (compulsory): 40% (P.O: a, b, c, e, f, g, h, j).

In order to pass, the student must fulfill two conditions:
- To obtain in the final examination a grade equal or higher than 4 points over 10.
- The sum of the grades of every part must be, at least, the 50% of the maximum possible mark.

2.2. NON-CONTINUOUS ASSESSMENT
The assessment process will be based on the following criteria:
- Final examination (compulsory): 100% (P.O: a, b, c, e, f, g, h, i, j, k).

The exam will contain specific parts to assess the knowledge that should have been acquired by performing the requested assignments.

In order to pass, the student must fulfill two conditions:
- The student must get 5.0 marks out of 10.0

% end-of-term-examination:	40
% of continuous assessment (assigments, laboratory, practicals…):	60

BASIC BIBLIOGRAPHY

- Frank Thornton, Chris Lanthem. RFID Security., Syngress (July 7, 2005).
- Matthew Gast 802.11 Wireless Networks The Definitive Guide. , O'Reilly, 2005
- Noureddine Boudriga. Security of Mobile Communications., Auerbach Publications., 2009
- Praphul Chandra Bulletproof wireless security, Newnes, 2005

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