Mobile Security

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

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: SEDANO JARILLO, FCO JAVIER

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Identification and Authentication
Data Protection

OBJECTIVES

After the course, the students will be able to:

- Analyze mobile systems and communications from a security point of view.

- Apply appropriate security services, mechanisms and protocols according to a concrete case.

- Apply acquired knowledge to solve problems under novel situations or within broader (multidisciplinar) contexts related with mobile systems and terminals, and wireless communications.

- Analyze risks and threats of introducing personal mobile devices (BYOD) in an enterprise environment. Know and apply measures to control such risks.

- Discuss in a public audience about their acquired knowledge, and the conclusions from the work. Students will be able to give their foundational and most convincing reasons to a specialized and non specialized audience in a clear way, without ambiguities.

- Elaborate reports in a clear, concrete and reasoned way. Such reports include threats and risks modeling in a specific scenario, where mobile systems, terminals and communications take part.

- Continue studying in a autonomous or self-directed way

LEARNING OUTCOMES
This course contributes to the following learning outcomes:

Design strategies to distribute sensors in a network and analyze observed events to determine which are relevant in a particular case.

Given a system with security requirements established to propose mechanisms and protocols required to provide some basic security services: authentication, authorization, privacy and access control. Give a measure of their effectiveness and limitations.

Explain the security issues related to personal mobile devices in a given professional environment and apply the studied techniques to the secure systems engineering

Evaluate the security architecture of a given vulnerable system and propose improvements.

Understand the principles of development of secure systems, including the development and acquisition of software components during all the lifecycle

DESCRIPTION OF CONTENTS: PROGRAMME

This course presents and elaborates security aspects and protection mechanisms against attacks related to systems and communications in wireless networks, both local area and wide area, and mobile devicies. The course program is organized as follows:

1. Cellular communications

1.1. Introduction to celullar communications
1.2. Security in cecullar communicationes
1.3. Known attacks to celullar communications

2. Wireless Communications
2.1. Bluetooth
2.2. Wireless LAN

3. Security in VoLTE convergence

4. Security in mobile platforms
4.1. Security design in mobile platforms
4.2. Mobile Device Management (MDM)
4.3. Mobile Malware & Application Development

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES
Theoretical lectures
Practical lectures
Mixed theoretical and practical lectures
Laboratory practices
Tutoring sessions
Teamwork

The teaching methodology consists of following learning activities:

- Lectures given by the professor using audiovisual elements to develope the main concepts and to provide additional references for further learning.

- Analysis of recommended lectures (e.g., news, papers, reports).

- Complementary activities to broaden and consolidate the acquired knowledge. Such activities could be of different nature: problems, discussion of practical cases, and/or exercises using the computers in order to test tools that are useful for the attacks simulation and development of mobile applications.

- Elaboration and oral presentation of technical works (i.e., individual and team work) by the students.

- Individual tutoring.

ASSESSMENT SYSTEM

The continuous evaluation system consists of:

1. Final exam (40%)

2. Student work and participation (60%):

2.1. Students must elaborate a team work on attacks to mobile systems and communications, including report, oral presentation and defense (30%)

2.2. Guided laboratory work and participation (30%)

Similarly, the "Convocatoria Extraordinaria" (Extra Examination Session) consists of:

a) If non-continuous evaluation, an exam (50% or 100%) and, under the criteria of the teacher, an individual work on attacks to mobile systems and communications (50%) will be carried out.

b) If continous evaluation, the pending ("failed") part will be carried out.

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

BASIC BIBLIOGRAPHY

- Boudriga, Noureddine Security of Mobile Communications, Auerbach, 2010

- D. Forsberg, G. Horn, W.D. Moeller, V. Niemi LTE Security, John Wiley & Sons, 2012

- Dwivedi, Himanshu. Mobile application security., McGraw-Hill., 2010

- Neil Bergman; Mike Stanfield; Jason Rouse; Joel Scambray; Sarath Geethakumar; Swapnil Deshmukh; Scott Matsumoto; John Steven; Mike Price. Hacking Exposed Mobile Security Secrets & Solutions., McGraw-Hill., 2013

ADDITIONAL BIBLIOGRAPHY

- Lee Barken. How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN., Prentice Hall., 2003.

- Ollie Whitehouse; Shaun Colley; Tyrone Erasmus; Dominic Chell. The Mobile Application Hacker's Handbook., Chell. John Wiley & Sons., 2015