Secure Communications

Academic Year: (2021 / 2022) **Review date: 29-06-2021**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: PASTOR PERALES, ANTONIO AGUSTIN

Type: Compulsory ECTS Credits : 6.0

Year : 1 Semester : 1

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

This course assumes previous knowledge about TCP/IP computer networks and cryptography.

OBJECTIVES

PROGRAM OUTCOMES
To have a deeply understanding of knowledge so it can be employed to develop original ideas and/or applying them, in a research environment.

To be able to apply acquired knowledge and their problem-solving abilities in new or unknown environments within broader (or multidisciplinary) contexts in relation with the area of study.

To have the self-learning abilities that enable students keep studying.

To write concise, clear and well-reasoned documentation, plans or working projects in the area of Cybersecurity.

To apply the appropriate services, mechanisms and security protocols for a particular case.

To design and evaluate security architectures for systems and networks.

To know and be able to apply the appropriate cryptographic and steganography mechanisms in order to protect stored data or in trasit through a network.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Security principles for communication networks
   1.1. Concepts and definitions. Security services vs. Security mechanisms
   1.2. Common attacks to communication networks
   1.3. Countermeasures. Cost of security.

2. Security at physical and link layers. Attacks and defences.
   2.1. Ethernet networks. Attacks and defences.
   2.2. PPP and EAP protocolos. Authentication, Authorization and Accounting (AAA)
   2.3. Security of IEEE 802.11

3. Security at network layer.
   3.1. Security in IPv4 and IPv6.
   3.2. Auxiliary protocols (ICMP, DHCP). Attacks and defences.
   3.3. Routing protocols. Attacks and defences.
   3.4. IPsec

4. Security at transport layer
   4.1. TLS/SSL.
   4.2. SSL Virtual Private Networks (VPNs)

5. Security at application layer.
   5.1. DNS security
   5.2. HTTP security
   5.3. Email security
   5.4. Security in other applications: remote execution, file transfer, network file systems.

LEARNING ACTIVITIES AND METHODOLOGY

TEACHING ACTIVITIES:
- Lectures
- Practical session in the lab
- Tutoring
- Group work
- Individual work

TEACHING METHODOLOGIES
Class presentations by the lecturer, with computer and audiovisual support, that develops the main concepts of the course and further bibliography is provided to extend student learning
Critical review of texts proposed by the course lecturers: News articles, reports, manuals and/or scientific papers, for either its discussion in class or to expand or consolidate the topics of the course
Solving practical examples, problems, etc. individually or in group, as proposed by the lecturer
Editing of reports individually or in group

ASSESSMENT SYSTEM

Continuous evaluation:
WLAN lab: 10%
MitM lab: 10%
TLS lab: 10%
Partial exam: 35%
Final exam (January): 35%

In the exams, it is necessary to obtain a minimum score of 3,5 over 10 points.

Non-continuous evaluation:
Final exam (June): 100%

% end-of-term-examination:	35
% of continuous assessment (assigments, laboratory, practicals…):	65

BASIC BIBLIOGRAPHY

- Charlie Kaufman, Radia Perlman, Mike Speciner Network Security: Private Communication in a Public World, Second Edition, 2002
- William Stallings Cryptography and Network Security: Principles and Practice, Prentice Hall, 2013

ADDITIONAL BIBLIOGRAPHY

- Jon Edney, William A. Arbaugh Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley Professional, 2003
- Sheila E. Frankel, Paul Hoffman, Angela Orebaugh, Richard Park Guide to SSL VPNs, NIST, 2008
- Stephen Thomas SSL & TLS essentials: securing the Web, John Wiley & Sons, 2000
- Yago Fernández Hansen, Antonio Angel Ramos Varón, Jean Paul García-Moran Maglaya RADIUS / AAA / 802.1x, RA-MA Editorial, 2008