Systems security engineering

Academic Year: (2019 / 2020) **Review date: 23/04/2020 13:52:32**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: GONZALEZ-TABLAS FERRERES, ANA ISABEL

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Not appropriate

OBJECTIVES

Master the knowledge required to propose original designs or developments, often in a research process within the area of cyber security.

Ability to apply acquired knowledge to solve problems under novel or almost novel situations or within broader (multidisciplinar) contexts related with cyber security.

Ability to state critical opinions and judgements having incomplete or limited information in the field of cyber security. These judgements must take into account include considerations about social and ethical responsibilities

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.

Students should have the learning skills required to continue studying in a autonomous or self-directed way.

Create, design, deploy and maintain a cyber defense global system in a given context

Create and refine concise and comprehensively documents, plans and projects in the scope of cyber security.

Know the relevant technique part of the legal regulation in cyber security and its implications in the design of systems and security tools.

Analyze systems to find attack evidences and to adopt the required measures to maintain the custody chain of the found evidences.

Apply the suited services, mechanisms and security protocols to a given case.

Design and evaluate security architectures of systems and networks.

Know and apply the cryptographic and steganographic mechanisms required to protect data stored in a system or data transiting a network.

Analyze the risks of introducing personal devices in a corporate professional environment (Bring your own device). Know and apply the measures to control the risks.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Concepts of Secure Systems Engineering
1.1. Security properties
1.2. Security design principles
1.3. Risk management
1.4. Privacy and legislation
1.5. Software architectures

2. Secure software requirements
2.1. Policy decomposition
2.2. Identification and elicitation

3. Secure software design
3.1. Design processes
3.2. Design issues
3.3. Security of architectures
3.4. Technologies

4. Security of implementations
4.1. Security of programming languages
4.2. Vulnerabilities data bases
4.3. Defensive practices and measures
4.4. Source code. Versions.
4.5. Development environments
4.6. Code review and analysis
4.7. Code anti-manipulation techniques

5. Testing
5.1. Test strategy, test plans and test cases
5.2. Test types
5.3. Impact assessment and corrective actions
5.4. Test data life cycle management

6. Other issues

LEARNING ACTIVITIES AND METHODOLOGY

ACTIVITIES
Lectures
Laboratory practices
Tutoring sessions
Team work
Individual work

TEACHING METHODOLOGIES
Class lectures in which the main concepts of the subject are developed and the literature is provided to supplement student learning.
Resolution of laboratory practices and problems posed by the teacher individually or in group
Elaboration and oral presentation of technical works by the students

ASSESSMENT SYSTEM

% end-of-term-examination/test:	50
% of continuous assessment (assigments, laboratory, practicals…):	50

Individual or group assignments during the course (50%)
Final exam (50%)
Assessment in continuous and non-continuous modalities is similar.

BASIC BIBLIOGRAPHY

- Adam Shostack Threat modeling: Designing for security., John Wiley & Sons, 2014

- Mano Paul Official (ISC)2® Guide to the CSSLP® CBK®. Second edition., CRC Press, 2014