Security Engineering

Academic Year: (2019 / 2020) **Review date: 27-04-2020**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: ESTEVEZ TAPIADOR, JUAN MANUEL

Type: Compulsory ECTS Credits : 6.0

Year : Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Criptography and Information Security
Computer Networks
Operating Systems

OBJECTIVES

The main goal of this subject is to make students aware of the complexity of ensuring security principles in today IT systems and architectures. Only by understanding IT security from an engineering point view, as a multidisciplinary subject, we can design and develop secure IT systems needed in modern societies. The student will acquire the necessary skills to design and plan global security solutions. Students will also become familiar with the different security mechanisms, their life cycle and cost. Finally, students must know the main laws and regulations that govern this matter.

In order to achieve these goals, students must acquire specific knowledge, capacities and attitudes:
Regarding knowledge, at the end of the course the student will be able to:
- Understand the concept of security as a complex process covering different areas and disciplines, aware of the fact that a system is as secure as its weakest component.
- Know in depth the security evaluation norms and certification procedures.
- Understand the specific risks regarding distributed systems and in particular the Internet.
- Identify physical threats and the corresponding countermeasures.
- Identify the different components of a security plan.
- Get to know the life cycle of a security plan and the feedback-based paradigms used.
- To learn the legal regulation of information security on the national, European and international scales.

With regard to capacities, the students will acquire specific and generic capacities.
Regarding specific capacities, the student will be able to:
- Analyze security protocols and manage security risks, mainly concerning distributed systems. (PO: a,b)
- Evaluate the possibility to implement one or another security mechanism depending on the security risk assessment. (PO: b, c, e)
- Create a complete security plan managing all the appropriate security measures. (PO: a, c, e, f)

Regarding generic capacities and skills, the student will be given the opportunity:
- To work on a specific system, in a particular environment, to investigate vulnerabilities and possible threats. (PO: b, e)
- To study and identify the necessary information to solve a particular security problem. (PO: b, c, e)
- Apply multi-disciplinal knowledge (technical, organizational and legal) for the resolution of a particular problem. (PO: c, e, f)
Regarding attitudes, the student will be encouraged to:
- Adopt a critical view over traditional, ad-hoc security systems based on the accumulation of security equipment, without ever conducting a formal analysis for the development of a global solution. (PO: i, j, k)
- Develop the collaborative skills to be able to obtain, from security IT managers, the necessary information about a system to analyze and assess risk, and to communicate the proposed solutions. (PO: d, f, g)
- A positive attitude towards team working, to coordinate different points of view and opinions, in search of global secure systems. (PO: d, f)
- A positive attitude towards the laws that affect the implementation of systems and security products.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Introduction to Computer Security
1.1 What is Computer Security?
1.2 The CIA Triad
1.3 Vulnerabilities
1.4 Threats and Attackers
1.5 Harm
1.6 Controls

2. Authentication and Access Control
2.1 Passwords
2.2 Biometric Authentication
2.3 Authentication Tokens
2.4 Federated Identity Management
2.5 Access Control and Access Policies
2.6 Implementing Access Control
2.7 Other Access Control Paradigms

3. Software Security
3.1 Buffer Overflows
3.2 Incomplete Mediation
3.3 Undocumented Access Points
3.4 Race Conditions
3.5 Countermeasures

4. Malware
4.1 Malicious Code
4.2 Types of Malware
4.3 Payloads
4.4 Transmission and Propagation
4.5 Activation
4.6 Stealth

5. Web Security
5.1 Browser Attacks
5.2 Web Attacks Targetting Users
5.3 Obtaining User or Website Data
5.4 Email Attacks

6. Operating System Security
6.1 Historical Notes
6.2 OS Design to Protect Objects
6.3 OS Tools to Implement Security
6.4 Secure Design Principles

7. Network Attacks
7.1 Interception Attacks
7.2 Man-in-the-Middle Attacks
7.3 Denial of Service Attacks

8. Security Protocols: Transport Layer Security
8.1 History and Design Goals
8.2 Handshake Protocol
8.3 Record Protocol
8.4 TLS Interception
8.5 Certificate Pinning

9. Privacy
9.1 Privacy in the Web: Web Bugs and ATS
9.2 Onion Routing: TOR
9.3 The General Data Protection Regulation (GDPR)

LEARNING ACTIVITIES AND METHODOLOGY

The teaching methodology includes:
1. Lectures to present the knowledge base that students must acquire. Students will be provided with the lecture notes used in class along with additional documents and basic text references to help in the

study of the topics covered. (PO: a, b, c, e, f, h, j)
2. Practical lectures, where the students will have to solve exercises and quizzes. (PO: a, b, g, k)
3. Discussion of real cases to illustrate concepts and techniques introduced during the lectures. (PO: c, f, g, k)
4. Lab sessions in computer labs, where the students will learn techniques and develop skills in the use of cybersecurity tools, including binary analysis, distributed systems security and network security. (PO: a, b, d, k)

ASSESSMENT SYSTEM

The final mark will depend on the following criteria:
(a) Lab assignments: 50%. (PO: a, b, d, g, k). These lab exercises are compulsory and will be marked by grading the associated deliverables and, in some cases, oral presentation of the results.
(b) Final exam: 50%. (PO: a, c, e, f, g, k). Sitting the final exam is compulsory. The student mist get at least 50% of the maximum mark to pass the course.

There will be a special examination session where the student who has not followed or has failed the continuous assessment scheme described above (lab sessions) will be able to hand-in, if s/he so wishes, all the related coursework. In such a case, the final mark will be computed using the scheme described above. Alternatively, the student can choose to seat just a final exam. Inn this case, the final mark will be that of the final exam.

In all other circumstances not covered above, the procedure established by the University on the 31st of May, 2011 will be followed.

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

BASIC BIBLIOGRAPHY

- Anderson, Ross SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTRED SISTEMS (2nd edition), Wiley, 2008
- Pfleeger, Charles. Pfleeger, Shari L SECURITY IN COMPUTING (4ª edition), Prentice Hall, 2007

ADDITIONAL BIBLIOGRAPHY

- Vacca, John R. (Editor). COMPUTER AND INFORMATION SECURITY HANDBOOK., Elsevier (The Morgan Kaufmann Series in Computer Security)., 2009.

BASIC ELECTRONIC RESOURCES

- ENISA . Publications: http://www.enisa.europa.eu
- INCIBE . OSI/CERTSI: https//www.incibe.es
- NIST . Special Publications (NIST-SP): http://www.nist.gov/publication-portal.cfm