Identification and Authentication

Academic Year: (2021 / 2022) **Review date: 10-06-2021**

Department assigned to the subject: Electronic Technology Department

Coordinating teacher: SANCHEZ REILLO, RAUL

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

No further requirements in addition to those needed to be admitted in the Master Course.

OBJECTIVES

CB6: Master the knowledge required to propose original designs or developments, often in a research process within the area of cyber security.
CB7: Ability to apply acquired knowledge to solve problems under novel or almost novel situations or within broader (multidisciplinar) contexts related with cyber security.
CB8: 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
CB9: 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 .
CB10: Students should have the learning skills required to continue studying in a autonomous or self-directed way.
CG2: Create, design, deploy and maintain a cyber defense global system in a given context
CG3: Create and refine concise and comprehensively documents, plans and projects in the scope of cyber security.
CG4: Know the relevant technique part of the legal regulation in cyber security and its implications in the design of systems and security tools.
CE4: Analyze systems to find attack evidences and to adopt the required measures to maintain the custody chain of the found evidences.
CE5: Apply the suited services, mechanisms and security protocols to a given case.
CE6: Design and evaluate security architectures of systems and networks.
CE7: Know and apply the cryptographic and steganographic mechanisms required to protect data stored in a system or data transiting a network.
CE8: 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

During this course the student will acquire the technical knowledge about identification and authentication processes. He/she will get familiar with the different identification and authentication schemes and devices, including the major biometric modalities and the identity management systems. Finally the main concepts related to privacy and legal environment will be given, related to identification and authentication.

Programme:

1. User authentication
1.1. Concepts and definitions
1.2. Authentication schemes. Multi-factor authentication
1.3. Robust authentication. Authentication by digital signature
1.4. Security analysis
1.5. Authentication architectures. Kerberos

2. Biometric Recognition
2.1. Definitions and working principles
2.2. Biometric systems
2.3. Security, privacy and practical aspects

3. Identity management
3.1. Life cycle of the digital identity
3.2. Identity management in distributed systems
3.3. Standards and federated systems

4. Ethical aspects and privacy legislation
4.1. Identification related standardization
4.2. LOPD

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES:
- Theretical lectures
- Theoretical-Practical lectures
- Office hours
- Work-sharing homework
- Individual homework

METHODOLOGY:
- Professor dissertations using computer and audiovisual means, explaining the main concepts involved and providing those relevant references to allow students to get more in depth in the subject.
- Critical reading of international references recommended by the professor.
- Jornal papers, reports and manuals for further discussion in class, to enhance and consolidate the knowledge acquired.
- Solving practical cases, presented by the professor to the students either individually or in groups
- Presentation and discussion in class, under the moderation of the professor, of subjects related to the course.
- Development of individual or group reports.

ASSESSMENT SYSTEM

The requested individual or group works, as well as the exam will be assessed using the following weighting scheme:
P1 (Cards): 10%
P2 (Biometrics): 20%
P3 (Identity Management): 20%

Exam: 50%, requiriing a minimum mark of 3 out of 10 to pass the course.

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

BASIC BIBLIOGRAPHY

- Anil K. Jain Biometrics : personal identification in networked society, Kluwer Academic, 2005
- Anil K. Jain, Raúl Sánchez Reíllo, et. al. Encyclopedia of Biometrics, Springer, 2015
- Finkenzeller, Klaus. RFID handbook : fundamentals and applications in contacless smart cards and identification, Wiles and Sons.
- Li, Stan Z. Encyclopedia of Biometrics, vols. 1 and 2, Springer, 2009
- Patrizio Campisi Security and Privacy in Biometrics, Springer, 2013
- Rankl, Wolfgang Smart card handbook, John & Wiley & Sons.
- Raúl Sánchez Reíllo, et. al. User-Centric Privacy and Security in Biometrics, IET, 2017
- Raúl Sánchez Reíllo, et. al. Iris and Periocular Biometric Recognition , IET, 2017
- Wayman, James. Biometric systems : technology, design, and performance evaluation., Springer.