INSTITUTO POLITÉCNICO DE BRAGANÇA

Course Unit	Computer Systems Security	Field of study	Computer Engineering
Master in	Informatics	School	School of Technology and Management
Academic Year	2023/2024	Year of study	1
Level	2-1	ECTS credits	6.0
Type	Semestral	Semester	1
Code	5060-710-1104-00-23		

Workload (hours)	162	Contact hours	T	-	TP	60	PL	-	TC	-	S	-	E	-	OT	-	O	-

T - Lectures; TP - Lectures and problem-solving; PL - Problem-solving, project or laboratory; TC - Fieldwork; S - Seminar; E - Placement; OT - Tutorial; O - Other

Name(s) of lecturer(s)	Rui Alexandre Coelho Alves, Tiago Miguel Ferreira Guimaraes Pedrosa

Learning outcomes and competences

At the end of the course unit the learner is expected to be able to:
1. Identify the importance of security in systems and computer networks
2. Identify the main vulnerabilities in systems and computer networks and possible solutions
3. Define security policies and use protection mechanisms and applications
4. Use secure development methodologies
5. Perform systems and network security assessment

Prerequisites

Before the course unit the learner is expected to be able to:
Basic knowledge on computer systems and networks.

Course contents

Fundamentals on systems and network security; introduction to criptography; vulnerabilities and attacks; security methods and applications; systems and network hardening; secure development; security assessment.

Course contents (extended version)

1. Fundamentals on systems and network security
   - Introduction
   - Authentication
   - Authorization
   - Accounting
   - Policies and security mechanisms
2. Introduction to cryptography
   - Cypher and key types
   - Data authentication
   - Public Key Management
   - Post-quantum cryptography
3. Vulnerabilities and attacks
4. Security methods and applications
   - Secure Protocols
   - Firewalls
   - Intrusion Detection Systems
   - Virtual Private Networks
   - Wireless Network Security
5. Systems and services hardening
6. Secure development
7. Security assessment
   - Process phases
   - Tools and applications for security assessment
   - Forensic Analysis

Recommended reading

1. W. Stallings, "Cryptography and network security: principles and pratice", Global Edition, 8th edition, Pearson, 2023
2. Robert Ciesla, "Encryption for Organizations and Individuals: Basics of Contemporary and Quantum Cryptography", Apress, 2020
3. M. Gregg, D. Kim, "Inside Network Security Assessment", Sams, 2006
4. A. Zúquete, "Segurança em Redes Informáticas - 4 ed", FCA, 2013
5. M. Correia e P. Sousa (2010), "Segurança no software", Lidel

Teaching and learning methods

The course unit will be taught using expository lessons and practical classes for resolution of exercises, demonstrations and execution of projects. The course documentation will be provided through the e-learning platform.

Assessment methods

1. Alternative 1 - (Regular, Student Worker) (Final)
   - Practical Work - 30% (Practical assignment on hardening solutions or generic security improving.)
   - Practical Work - 30% (Practical assignment on security auditing.)
   - Work Discussion - 20% (Resolution of proposed homework assignments.)
   - Intermediate Written Test - 20% (Written exams.)
2. Alternative 2 - (Regular, Student Worker) (Supplementary, Special)
   - Practical Work - 35% (Practical assignment on hardening solutions or generic security improving.)
   - Practical Work - 35% (Practical assignment on security auditing.)
   - Final Written Exam - 30% (Final written exam.)

Language of instruction

English

Electronic validation

Rui Alexandre Coelho Alves, Tiago Miguel Ferreira Guimaraes Pedrosa	José Luís Padrão Exposto	José Eduardo Moreira Fernandes	José Carlos Rufino Amaro
03-10-2023	03-10-2023	03-10-2023	07-10-2023

This document is valid only if stamped in all pages.