**COURSE SYLLABUS**

***Wireless and mobile devices security***

**1. Program identification details**

|  |  |
| --- | --- |
| 1.1 Higher education institution | „Ovidius” University of Constanta |
| 1.2 Faculty | Faculty Mathematics and Computer Science |
| 1.3 Department | Mathematics and Computer Science |
| 1.4 Field of studies | **Computer Science** |
| 1.5 Cycle of studies (degree) | Master |
| 1.6 Degree program/qualification | **Cyber Security and Machine Learning** |
| 1.7 Academic year | **2022-2023** |

**2. Course identification details**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2.1 Course title | | | Wireless and mobile devices security | | | | |
| 2.2 Course code | | | **FMI.CSML.I.2.14** | | | | |
| 2.3 Instructor | | | Deacu Daniela, Ph.D. | | | | |
| 2.4 Teaching assistant | | | Deacu Daniela, Ph.D. | | | | |
| 2.5 Year | **I** | 2.6 Semester | **2** | 2.7. Evaluation type | **C** | 2.8 Course type \*/\*\* | **DAP/**  **DO** |

*\* DF – fundamental course, DD – field course, DS – specialty course, DC – complementary course, DAP – advanced study course, DSI – synthesis course, DCA – advanced knowledge course.*

*\*\* DI – mandatory course; DO – optional course.*

**3. Estimated workload (hours per semester)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3.1 Number of teaching hours/week | | **2** | of which:  3.2 course | **1** | 3.3 applications*\*\*\** | **1** |
| 3.4 Total of teaching hours within the program/semester | | **28** | of which:  3.5 lecture | **14** | 3.6 applications | **14** |
| **3.7 Student workload for individual study** | | | | | | **72** |
| ***Distribution of workload*** | | | | | | [hours] |
| Individual study of texbooks, handbooks/reader, bibliography and notes | | | | | | 30 |
| Additional research (library, electronic resources, fieldwork) | | | | | | 14 |
| Homework (preparing seminar presentations, portfolios, critical essays, research papers, etc.) | | | | | | 14 |
| Individual consultations (optional) | | | | | | 8 |
| Evaluations / exams | | | | | | 6 |
| Other activities | | | | | | 0 |
| **3.8 Total hours per semester** | ***28 + 72 = 100*** | |  |  |  |  |
| **3.9 Number of credits** | **4** | |  |  |  |  |

*\*\*\* S - seminar; L - laboratory; P - project*

**4. Prerequisites (if any)**

|  |  |
| --- | --- |
| 4.1 Curriculum-related | Undergraduate studies |
| 4.2 Skills-related | Computer Networks |

**5. Requirements (if any)**

|  |  |
| --- | --- |
| 5.1. For running the course | Classroom available |
| 5.2. For running the seminar / laboratory /project  *\*The type is to be chosen according to the discipline* | Laboratory room available with computers |

**6. Acquired specific skills**

|  |  |
| --- | --- |
| Professional skills | Identify basic concepts and models for different types of mobile systems  Identifying, explaining and using security solutions for mobile systems |
| Cross-cutting skills | Execution of complex professional tasks, in conditions of autonomy and professional independence, involving the detection and solution of related problems in the use of wireless systems and mobile solutions.  Efficient use of information sources and communication resources as well as the development of teamwork, in the case of design, administration and use of different types of mobile systems. |

**7. Course goal and objectives**

|  |  |
| --- | --- |
| 7.1 The general objective of the course | Developing a deeper understanding of Wireless and mobile devices security.  Developing a deeper understanding of the most important mechanisms dedicated to protect data integrity and confidentiality, access control, authentication, quality and continuity of service. |
| 7.2 Specific objectives | Developing the ability to configure, optimize and maintain all the security mechanism implemented in a wireless/mobile network.  Developing the capacity to handle wireless and mobile devices security incidents.  Developing the capacity to research.  Improving the ability to extract, present and discuss results from recent papers on a certain topic. |

**8. Contents**

|  |  |  |
| --- | --- | --- |
| **8.1 Lecture** | **Teaching methods** | **Number of hours** |
| 1. Introduction to wireless standards and technologies. | Dialog  Active and interactivemethods | 1 |
| 2. Threats, vulnerabilities and risks in Wireless/Mobile Communications. | 1 |
| 3. Security measures. | 1 |
| 4. Mobile Ad-Hoc Network Security. | Problematization  Interaction, problematization, argumentation  Synthesizing / essentializing information  Independent and cooperative learning | 1 |
| 5. Cellular Network Security. | 1 |
| 6. Wireless Local Area Network Security. | 1 |
| 7.Wireless Personal Area Network Security. Bluetooth security assessment and monitoring. Legacy Pairing. Secure Simple Pairing. | 2 |
| 8. Security assesments of IoT devices. | 2 |
| 9. Radio Frequency Identification (RFID) Security. | 2 |
| 10. Mobile device security. Andoid and iOS Security. | 2 |
| **Bibliography:**   1. W. Osterhage. Wireless Network Security (second edition). CRC Press, Taylor & Francis Group, 2018 2. N. Boudriga. Security of Mobile Communications. CRC Press, Taylor & Francis Group, 2009 3. Chaouchi, M. Laurent-Maknavicius. Wireless and Mobile Networks Security. Wiley, 2009 4. David Tse, Pramod Viswanath, Fundamentals of Wireless Communication, Cambridge University Press, 2005. 5. VijayGarg, Wireless Communications and Networking, Morgan Kaufmann, 2007. 6. W. Stallings, Wireless Communications & Network, 2nd Edition, 2004.4.Dharma Prakash Agrawal, Qing-An Zeng, Introduction To Wireless And Mobile Systems, 2005. 7. Yan Zhang, Wireless Quality of Service -Techniques, Standards, and Applications, 2008. 8. Andrea Goldsmith, Wireless Communications, 2006. 9. Matthew Gast, 802.11 Wireless Network s: The Definitive Guide, Second Edition, 2005. | | |

|  |  |  |
| --- | --- | --- |
| **8.2 Applications\* (seminar / laboratory / project)**  *\*The type is to be chosen according to the discipline* | **Teaching methods** | **Number of hours** |
| 1. Threats and Vulnerabilites in an industrial context. | Dialog  Problematization  Active and interactive methods  Interaction, problematization, argumentation  Synthesizing / essentializing information  Independent and cooperative learning | 1 |
| 2. Security measures. Security Setings for a Wireless Acces Point. SSID hiding, MAC filtering, Wi-Fi Protected Access | 1 |
| 3. Modes of unauthorized access. Denial of Services Attacks, Man-in-the-middle Attacks, SSID Identification, MAC spoofing, Network injection. Evil Twin Acces Point. | 1 |
| 4. Practical attacks against WEP, WPA, WPA2 | 1 |
| 5. Attacks on mobile technologies. | 1 |
| 6. Bluetooth Attacks . | 1 |
| 7. RFID Security Assessment. | 2 |
| 8. Security assessments of IoT protocols and implementations. | 2 |
| 9.Andoid devices, security and privecy concerns. | 2 |
| 10.iOS devices, security and privacy concerns. Jailbreak. | 2 |
| **Bibliography:**   1. W. Osterhage. Wireless Network Security (second edition). CRC Press, Taylor & Francis Group, 2018 2. N. Boudriga. Security of Mobile Communications. CRC Press, Taylor & Francis Group, 2009 3. Chaouchi, M. Laurent-Maknavicius. Wireless and Mobile Networks Security. Wiley, 2009 4. David Tse, Pramod Viswanath, Fundamentals of Wireless Communication, Cambridge University Press, 2005. 5. VijayGarg, Wireless Communications and Networking, Morgan Kaufmann, 2007. 6. W. Stallings, Wireless Communications & Network, 2nd Edition, 2004.4.Dharma Prakash Agrawal, Qing-An Zeng, Introduction To Wireless And Mobile Systems, 2005. 7. Yan Zhang, Wireless Quality of Service -Techniques, Standards, and Applications, 2008. 8. Andrea Goldsmith, Wireless Communications, 2006. 9. Matthew Gast, 802.11 Wireless Network s: The Definitive Guide, Second Edition, 2005. | | |

**9. Correlation between the content of the course and the needs/expectations of the epistemic community, professional associations and/or significant employers relevant for the program**

|  |
| --- |
| The notions introduced in this course will develop students' ability to analyze and lead to a better and deeper understanding of the issues of wireless security and mobile devices.  The course offers access to current, theoretical information, but with practical applicability and aims to develop research and innovation skills, preparing candidates who can become members of the research departments of companies in the field. |

**10. Evaluation**

|  |  |  |  |
| --- | --- | --- | --- |
| Type of activity | 10.1 Evaluation criteria | 10.2 Evaluation methods | 10.3 Percentage of final grade |
| 10.4 Course | Active participation in teaching activities | Written exam  Course and Laboratory Project | 30%  50% |
| 10.5 Applications\*  Laboratory  *\*The type is to be chosen according to the discipline* | Active participation, problematization | Laboratory activity and homework completion | 20% |
|  | | | |
| 10.6 Minimum standard of achievement for the acquisition of the ECTS credits | | | |
| Realization and presentation of a project on a specialized topic in the area of security of mobile and wireless systems, in the context of the course program. | | | |

|  |  |  |
| --- | --- | --- |
| Date of completion  20.09.2022 | Course Instructor,    Deacu Daniela, Ph.D. | Teaching Assistant,    Deacu Daniela, Ph.D. |

Date of approval in the Department Head of Department

27.09.2022 Assoc. Prof., Puchianu Crenguta Ph.D.

Dean,

Assoc. Prof. Nicola Aurelian, Ph.D.