| | | | | | |
|---|---|---|---|---|---|
| Course Title | Information Security | | | | |
| Course Code | DIS504 | | | | |
| Course Type | Elective | | | | |
| Level | Postgraduate | | | | |
| Year / Semester | 1st Year / 2nd Semester | | | | |
| ECTS | 7.5 | Lectures / week | 1 | Laboratories / week | - |
| Course Purpose and Objectives | The objectives of the course are:<br>• Provide the fundamentals of Information security.<br>• Present the information threats and attacks and ways to protect the information from such attacks.<br>• Look at specific technical areas of information security such as authentication, access control, denial of service, intrusion detection and prevention systems and, finally cryptographic algorithms.<br>• Concern with management aspects of information security and more specifically on management practices related to risk management.<br>• Discuss the legal and ethical issues that are commonly found in today's organizations.<br>• Introduce computer forensics and how we can find evidence. | | | | |
| Learning Outcomes | After completing the course the students are expected to:<br>O[1] Explain the challenges and scope of information security;<br>O[2] Identify the common threats faced today;<br>O[3] Describe the access control mechanism used for user authentication and authorization;<br>O[4] Understand the importance of cryptographic algorithms used in information security;<br>O[5] Explain the use of such security tools as firewalls and intrusion prevention systems;<br>O[6] Recognize the importance of physical security and discuss ways to improve physical security of an enterprise; | | | | |

| | | | |
|---|---|---|---|
| | O[7] Ensure infrastructure and network security;<br>O[8] Examine and resolve legal and ethical issues;<br>O[9] Enhance critical thinking and analysis skills through the use of case studies, research papers and small group exercises.<br>O[10] Strengthen research, writing and presentation skills. | | |
| Prerequisites | None | Required | None |
| Course Content | 1st week: Introduction to Information Security<br>2nd week: Attacks and Threats<br>3rd week: Denial of Service Attacks<br>4th week: Intrusion Detection and Prevention Systems<br>5th week: Basic Cryptography<br>6th week: Access Control Fundamentals<br>7th week: User Authentication<br>8th week: Physical Security<br>9th week: Risk Management<br>10th week: Network Security<br>11th week: Legal and Ethical Issues in Information Security<br>12th week: Introduction to Forensics<br>13th week: Conclusions / Rehearsal | | |
| Teaching Methodology | Mix of interactive lectures, active learning techniques and activities. More precisely:<br>• Interactive Lectures<br>• Notes and PowerPoint Presentations in digital format through the electronic platform<br>• Basic textbook(s) and additional bibliography<br>• Assignments<br>• Interactive Activities<br>• Discussions in Forums through the electronic platform of real word case studies<br>• Web links<br>• Critical reflection on research article<br>• Peer review on group working and discussion in forum | | |

<table>
<tr><td></td><td>

- Educational videos on real world case studies and critical discussion in forum

</td></tr>
<tr><td>Bibliography</td><td>

Compulsory Bibliography

- W. Stallings, L. Brown, Computer Security Principles and Practice, 4th edition, 2018, Pearson
- Wenliang Du, Computer & Internet Security: A Hands-on Approach
- Michael E. Whitman, Principles of Information Security, 6th edition, 2018

Additional Bibliography

- Yang, J.; Chen, Y.-L.; Por, L.Y.; Ku, C.S. A Systematic Literature Review of Information Security in Chatbots. Appl. Sci. 2023, 13, 6355. https://doi.org/10.3390/app13116355
- Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping study. Arabian Journal for Science and Engineering, 45(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2
-

</td></tr>
<tr><td>Assessment</td><td>

5% Quizzes<br>
20% Projects/Assignments<br>
10% Peer Assessment<br>
5% Oral Presentation<br>
60% Final exams

*Assessment methods and mapping with Learning Outcomes*

<table>
<tr><th></th><th>Percentage</th><th>O1</th><th>O 2</th><th>O3</th><th>O4</th><th>O5</th><th>O6</th><th>O7</th><th>O8</th><th>O9</th><th>O10</th></tr>
<tr><td>Quizzes</td><td>5%</td><td>√</td><td>√</td><td></td><td></td><td>√</td><td></td><td></td><td>√</td><td></td><td></td></tr>
<tr><td>Projects / Assignments</td><td>20%</td><td></td><td></td><td>√</td><td>√</td><td></td><td>√</td><td>√</td><td></td><td></td><td>√</td></tr>
<tr><td>Peer Assessment</td><td>10%</td><td></td><td></td><td>√</td><td>√</td><td></td><td>√</td><td>√</td><td></td><td>√</td><td>√</td></tr>
<tr><td>*Oral Presentation</td><td>5%</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>√</td><td>√</td></tr>
<tr><td>Final exam</td><td>60%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td><td></td><td>√</td><td></td><td></td></tr>
</table>

</td></tr>
</table>

| | |
|---|---|
| | *Oral presentation of a state of the art research paper or a case study in the field of "Information Security". List of papers or case studies to be announced during Week 4. |
| Language | English |