澳門理工大學
Universidade Politécnica de Macau
Macao Polytechnic University

**FACULTY OF APPLIED SCIENCES**

**MASTER OF SCIENCE IN BIG DATA AND INTERNET OF THINGS**

**LEARNING MODULE OUTLINE**

| | | | |
|---|---|---|---|
| Academic Year | 2023/2024 | Semester | 1 |
| Module Code | COMP6112 | | |
| Learning Module | Security and Authentication | | |
| Pre-requisite(s) | Nil | | |
| Medium of Instruction | English | | |
| Credits | 3 | Contact Hours | 45 hrs |
| Instructor | Dr. Amang Kim | Email | amang@mpu.edu.mo |
| Office | Rm# A320 | Office Phone | 8599.6455 |

**MODULE DESCRIPTION**

This module focuses on information systems security. Students will learn fundamentals of computer security, formal models of security, aspects of information systems security such as access control, hacks/attacks, systems and programs security, intrusion detection, cryptography, networks and distributed systems security, worms, and viruses, and other Internet secure applications. Students will develop the skills necessary to formulate and address the security needs of enterprise and personal environments.

**MODULE INTENDED LEARNING OUTCOMES (ILOS)**

On completion of this learning module, students will be able to:

| | |
|---|---|
| M1. | Design the information systems security practiced in computer operating systems, distributed systems, networks and representative applications. (AHEP4-M2) |
| M2. | Estimate familiarity with prevalent network and distributed system attacks, defences against them, and forensics to investigate the aftermath. (AHEP4-M3) |
| M3. | Explain the core cryptography, how it has evolved, and some key encryption techniques used today. (AHEP4-M7) |
| M4. | Interpret security policies (such as authentication, integrity and confidentiality) as well as protocols to implement such policies in the form of message exchanges. (AHEP4-M4, AHEP4-M5) |

These ILOs aims to enable students to attain the following Programme Intended Learning Outcomes (PILOs):

| **PILOs** | | **M1** | **M2** | **M3** | **M4** | **M5** | **M6** |
|---|---|---|---|---|---|---|---|
| P1. | Master the principles of system engineering and relevant enabling technologies for building of IoT solutions | ✓ | | | | | |
| P2. | Critically evaluate scientific methodologies and mathematical models for Big Data and its applications | ✓ | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| P3. | Master the advanced software and programming tools and techniques for IoT solutions and Big Data | | | | | | |
| P4. | Explain the processes involved in IoT solutions and Big Data analytics in a typical business setting | | | | | | |
| P5. | Explain different application domains and analyze their requirements for IoT and Big Data | | | | | | |
| P6. | Apply knowledge in advanced communication and multimedia technologies for the design and implementation of IoT solutions | | | | | | |
| P7. | Apply knowledge in applied statistics, machine learning, leading-edge technologies and programming techniques for Big Data | | | | | | |
| P8. | Design and carry out an advanced project following an ethical and professional methodology | | | | | | |
| P9. | To demonstrate advanced knowledge and R&D techniques in Big Data and IoT | | ✓ | | | | |
| P10. | To investigate and develop new, emerging ICT technology for Big Data and IoT | | | | ✓ | | |
| P11. | To develop a global vision on the critical development and new application of Big Data and IoT | | | ✓ | | | |
| P12. | To communicate technically and effectively in both speaking and writing | | ✓ | | | | |
| P13. | To have a positive attitude towards society and the environment. | | | | | | |
| P14. | To adhere to high moral standards and commit to excellence in life-long learning. | | | | | | |

**MODULE SCHEDULE, COVERAGE AND STUDY LOAD**

| Week | Content Coverage | Contact Hours |
|---|---|---|
| 1 | 1. Introduction | 3 |
| | 1.1. Threats, vulnerabilities, controls; risk; method, opportunity, motive; technical, administrative, physical controls; prevention, detection, deterrence | |
| | 1.2. Terminology, concepts | |
| 2-3 | 2. Identification and authentication | 6 |
| | 2.1. Identification goals | |
| | 2.2. Authentication requirements; human authentication, machine authentication, authentication technologies | |
| 4-5 | 3. Cryptography | 6 |
| | 3.1. Basic cryptography terms, symmetric and asymmetric ciphers | |
| | 3.2. Cryptographic protocols: digital signatures, key exchange, certificates, cryptographic hash functions | |
| 6-7 | 4. Security in programs | 6 |

| | | |
|---|---|---|
| | 4.1. Malicious code: viruses, Trojan horses, worms | |
| | 4.2. Program flaws: buffer overflows, time-of-check to time-of-use flaws, incomplete mediation | |
| | 4.3. Testing techniques | |
| | 4.4. Trusted operating systems: independent evaluation | |
| 8-9 | 5. Network security: Threats and controls | 6 |
| | 5.1. Network technology (depth depends on students' background) | |
| | 5.2. Network threats: eavesdropping, spoofing, modification, denial of service attacks | |
| | 5.3. Architectural controls | |
| | 5.4. Cryptographic controls | |
| | 5.5. Administrative and physical controls | |
| 10-12 | 6. Network security: Technologies | 9 |
| | 6.1. Firewalls | |
| | 6.2. Intrusion detection systems | |
| | 6.3. Monitoring systems | |
| | 6.4. Virtual private networking | |
| | 6.5. Remote authentication systems | |
| | 6.6. Blockchain Governance Game | |
| 13-14 | 7. Management of security | 4.5 |
| | 7.1. Security policies | |
| | 7.2. Risk analysis | |
| | 7.3. Physical threats and controls | |
| 14-15 | 8. Legal aspects of security | 4.5 |
| | 8.1. Legal protection for computer objects | |
| | 8.2. Computer crimes | |

**TEACHING AND LEARNING ACTIVITIES**

In this learning module, students will work towards attaining the ILOs through the following teaching and learning activities:

| Teaching and Learning Activities | M1 | M2 | M3 | M4 | M5 | M6 |
|---|---|---|---|---|---|---|
| T1. Class teaching (lecture) | ✓ | | ✓ | ✓ | | |
| T2. Literature review | | ✓ | | ✓ | | |
| T3. Tests | | ✓ | ✓ | | | |

**ATTENDANCE**

Attendance requirements are governed by the Academic Regulations Governing Master's Degree Programmes of the Macao Polytechnic University. Students who do not meet the attendance requirements for the learning module shall be awarded an 'F' grade.

**ASSESSMENT**

In this learning module, students are required to complete the following assessment activities:

| Assessment Activities | Weighting (%) | AHEP4 LOs | ILOs to be Assessed |
|---|---|---|---|
| A1. Popup Quiz | 6% | AHEP4-M2, | P1, P2, |
| A2. Take home assignments (x3) | 54% | AHEP4-M3, AHEP4-M4, | P11, P12, |
| A3. Tests (x2) | 40% | AHEP4-M5, AHEP4-M7 | P1, P2, P9, P10 |

The assessment will be conducted following the University's Assessment Strategy (see www.mpu.edu.mo/teaching_learning/en/assessment_strategy.php). Passing this learning module indicates that students will have attained the ILOs of this learning module and thus acquired its credits.

Students with an overall score of less than 35 in the coursework will fail the module even if the overall score for the module is 50 or above.

Students with a score of less than 35 in the final examination will fail the module even if the overall score for the module is 50 or above.

**REQUIRED READINGS**

1. Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies (2015), Security in Computing, 5th Edition. Prentice Hall. 978-0134085043

**REFERENCES**

1. William Stallings, Lawrie Brown (2017). Computer Security: Principles and Practice, 4th Ed. Pearson. 978-0134794105
2. Evan Gilman, Doug Barth (2017). Zero Trust Networks: Building Secure Systems in Untrusted Networks (1st Edition). O'Reilly Media. 978-1491962190

**STUDENT FEEDBACK**

At the end of every semester, students are invited to provide feedback on the learning module and the teaching arrangement through questionnaires. Your feedback is valuable for instructors to enhance the module and its delivery for future students. The instructor and programme coordinators will consider all feedback and respond with actions formally in the annual programme review.

**ACADEMIC INTEGRITY**

The Macao Polytechnic University requires students to have full commitment to academic integrity when engaging in research and academic activities. Violations of academic integrity, which include but are not limited to plagiarism, collusion, fabrication or falsification, repeated use of assignments and cheating in examinations, are considered as serious academic offenses and may lead to disciplinary actions. Students should read the relevant regulations and guidelines in the Student Handbook which is distributed upon the admission into the University, a copy of which can also be found at www.mpu.edu.mo/student_handbook/.