Macao Polytechnic University

Faculty of Applied Sciences

Master of Science in Big Data and Internet of Things

Module Outline

Academic Year 2022/2023 Semester 1

Learning Module	Security and Authentication		**Class Code**	COMP6102	
Pre-requisite(s)	Nil				
Medium of Instruction	English			**Credit**	3
Lecture Hours	45 hrs	**Lab/Practice Hours**	0 hrs	**Total Hours**	45 hrs
Instructor	Dr. Amang Kim		**E-mail**	amangkim.mpi@gmail.com	
Office	Rm# A320		**Telephone**	8599-6455	

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.

Learning Outcomes

After completing the learning module, students will be able to:

1. Develop an understanding of information systems security practiced in computer operating systems, distributed systems, networks and representative applications. (SM1fl, EA1fl)
2. Gain familiarity with prevalent network and distributed system attacks, defenses against them, and forensics to investigate the aftermath. (EA3fl, ET3fl)
3. Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today. (SM1fl, EA1fl)
4. Develop an understanding of security policies (such as authentication, integrity and confidentiality) as well as protocols to implement such policies in the form of message exchanges. (ET1fl, ET2fl, ET5fl)

Content

1. Introduction (Ch. 1) 3.0 hours

1.1. Threats, vulnerabilities, controls; risk; method, opportunity, motive; technical, administrative, physical controls; prevention, detection, deterrence

1.2. Terminology, concepts

2. Identification and authentication (Ch. 2) 6.0 hours

2.1. Identification goals

2.2. Authentication requirements; human authentication, machine authentication, authentication technologies

3. Cryptography (Ch. 2 & Ch. 12) 6.0 hours

3.1. Basic cryptography terms, symmetric and asymmetric ciphers

3.2. Cryptographic protocols: digital signatures, key exchange, certificates, cryptographic hash functions

4. Security in programs (Ch. 3) 6.0 hours

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

5. Network security: Threats and controls (Ch.6 – Part I) 6.0 hours

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

6. Network security: Technologies (Ch.6 – Part II) 9.0 hours

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

7. Management of security (Ch. 10) **4.5 hours**

7.1. Security policies

7.2. Risk analysis

7.3. Physical threats and controls

8. Legal aspects of security (Ch. 11) **4.5 hours**

8.1. Legal protection for computer objects

8.2. Computer crimes

Teaching Method

Lectures, case method teaching and online support.

Attendance

Attendance requirements are governed by the "Academic Regulations Governing Master's Degree Programmes of Macao Polytechnic University".

Assessment

The learning module is graded on a 100 points scale, with 100 being the highest possible score and 50 being the passing score.

	Item	Description	AHEP3 LO	Percentage
1.	Popup Quiz	In-class assessments	SM1fl, ET1fl	6 %
2.	Assignments	Home-based exercises (x3)	SM1fl, EA1fl, EA3fl, ET2fl	54 %
3.	Test	Knowledge assessment (x2)	SM1fl, ET1fl, ET2fl, ET3fl, ET5fl	40 %
			Total Percentage:	**100%**

Teaching Material(s)

Textbook(s)

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

Reference

Reference book(s)

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