TQF 3 Course Specifications
Section 1 General Information

1. Course code and course title

Thai ICCS 418 ความมั่นคงในระบบคอมพิวเตอร์
English ICCS 418 Computer System Security

2. Number of credits 4 (4-0-8) (Lecture/Lab/Self-study)
3. Program and type of subject
   3.1 Program Bachelor of Science (Computer)
   3.2 Type of Subject Elective course
4. Course Coordinator and Course Lecturer
   4.1 Course Coordinator Kanat TANGWONGSAN
   4.2 Course Lecturers Asst. Prof. Dr. Wilawan RUKPAKAVONG
5. Trimester/ Year of Study
   5.1 Trimester All trimesters (excluding summer session) / for all students in all International College Undergraduate Programs
   5.2 Course Capacity Approximately 40 students
6. Pre-requisite -
7. Co-requisites -
8. Venue of Study Mahidol University, Salaya Campus
9. Date of Latest Revision Aug 28, 2020

Section 2 Goals and Objectives

1. Course Goals
   - To be able to identify security issues in various aspects of computing.
   - To be able to use this ability to design systems that are more protective of security.

2. Objectives of Course Development/Revision

2.1 Course Objectives

This course will teach the principles and practices of computer system security as applied to software and network layers. It covers the foundations and techniques of analyzing the security of systems and building secured systems.

2.2 Course-level Learning Outcomes: CLOs

By the end of the course, students will be able to (CLOs)

1. CLO 1 Describe fundamental of computer security concepts.
2. CLO 2 Explain access control mechanisms including their strengths and weaknesses.
3. CLO 3 Classify cryptography algorithms and explain the difference between them.
4. CLO 4 Classify software/operating systems and computer network vulnerabilities with security attack techniques.
5. CLO 5 Understanding the defense and analysis techniques for business continuity.

Section 3 Course Management

2. Course Description

กระแสการรักษาความปลอดภัย, ความมั่นคงปลอดภัยข้อมูลและการบริหารความเสี่ยง, การควบคุมการเข้าถึง, การออกแบบและสถาปัตยกรรมความมั่นคงปลอดภัย, โทรคมนาคมและการรักษาความปลอดภัยระบบเครือข่าย, วิทยาการเข้าถึงรหัสลับ, ความต่อเนื่องทางธุรกิจและการกู้คืนข้อมูล, การรักษาปลอดภัยของแอปพลิเคชั่น, การรักษาความปลอดภัยของระบบปฏิบัติการ, ฝึกปฏิบัติการไฟร์วอลล์, ดีเอ็มเอสและไอพีเอส

Security trends; information security and risk managements; access control, security architecture and design; physical and environmental security; telecommunications and network security; cryptography; business continuity and disaster recovery; legal/regulation compliance and investigations; application security; operation security; practical workshops of basic firewall appliance, DMZ and IPS.

2. Credit hours per trimester

Lecture (Hour(s))	Laboratory/field trip/internship (Hour(s))	Self-study (Hour(s))
48	0	96

3. Number of hours that the lecturer provides individual counseling and guidance.
1 hour/week

Section 4 Development of Students' Learning Outcome

2. Short summary on the knowledge or skills that the course intends to develop in students (CLOs)

By the end of the course, students will be able to:

1. CLO 1 Describe fundamental of computer security concepts.
2. CLO 2 Explain access control mechanisms including their strengths and weaknesses.
3. CLO 3 Classify cryptography algorithms and explain the difference between them.
4. CLO 4 Classify software/operating systems and computer network vulnerabilities with security attack techniques.
5. CLO 5 Understanding the defense and analysis techniques for business continuity.

2. Teaching methods for developing the knowledge or skills specified in item 1 and evaluation methods of the course learning outcomes

ICCH 418	Teaching methods	Evaluation Methods
CLO1	Reading assignment, interactive lecture, case studies, quiz, group activities, group discussion	Quiz, Homework, Examination
CLO2	Reading assignment, interactive lecture, case studies, quiz, group activities, group discussion	Quiz, Homework, Examination
CLO3	Reading assignment, interactive lecture, case studies, quiz, group activities, group discussion	Quiz, Homework, Examination
CLO4	Reading assignment, interactive lecture, case studies, quiz, group activities, group discussion	Quiz, Homework, Examination
CLO5	Reading assignment, interactive lecture, case studies, quiz, group activities, group discussion	Quiz, Homework, Examination

Section 5 Teaching and Evaluation Plans

1. Teaching plan

Week	Topic	Number of Hours		Teaching Activities/ Media	Lecturer
		Lecture Hours	Lab/Field Trip/Internship Hours		
1	Introduction to Computer Security	4	-	Reading assignment, interactive lecture, quiz, group activities, case studies, group discussion	Asst. Prof. Dr. Wilawan Rukpakavong
2-3	Access Control	8	-		
4-5	Cryptography	8	-		
6	Software vulnerabilities	4	-		
7	OS vulnerabilities and Malwares	4	-		
8	Network Security	4	-		
9	Internet Application Security and Privacy	4	-		
10	Database Security and Privacy	4	-		
11	Defense Techniques (Firewall, IDS)	4	-		
12	Digital Forensics	4	-		
	Total	48	-		

2. Plan for Assessing Course Learning Outcomes

2.1 Assessing and Evaluating Learning Achievement

a. Formative Assessment

- Worksheet
- Class discussion
- Group discussion

b. Summative Assessment

c. Projects

(1) Tools and Percentage Weight in Assessment and Evaluation

Learning Outcomes	Assessment Methods	Assessment Ratio (Percentage)	
CLO 1 Describe fundamental of computer security concepts.	Homework & Quiz	10	15
	Examination	5	
CLO 2 Explain access control mechanisms including their strengths and weaknesses.	Homework & Quiz & Project	10	15
	Examination	5	
CLO 3 Classify cryptography algorithms and explain the difference between them.	Homework & Quiz & Project	10	15
	Examination	5	
CLO 4 Classify software/operating systems and computer network vulnerabilities with security attack techniques.	Homework & Quiz & Project	20	35
	Examination	15	
CLO 5 Understanding the defense and analysis techniques for business continuity.	Homework & Quiz & Project	10	20
	Examination	10	
			100

(2) Grading System

Grade	Achievement	Final Score (% Range)	GPA
A	Excellent	90-100	4.0
B+	Very good	85-89	3.5
B	Good	80-84	3.0
C+	Fairly good	75-79	2.5
C	Fair	70-74	2.0
D+	Poor	65-69	1.5
D	Very Poor	60-64	1.0
F	Fail	Less than 60	0.0

(3) Re-examination (If course lecturer allows to have re-examination)

N/A - (Not applicable with MUIC)

3. Student Appeals

N/A

Section 6 Teaching Materials and Resources

1. Textbooks and/or other documents/materials

● *Charles P. Pfleeger, Shari Lawrence Pfleeger, "**Security in Computing**", 5th Edition (Pearson), 2015.*
(ISBN: 9780134085043

2. Recommended textbooks and/or other documents/materials

- James Graham, Ryan Olson, Rick Howard, "Cyber Security Essentials", CRC press, 2010.
- Linda K. Lavender, "Principles of Cybersecurity", G-W Publisher, 2020.
- Selected readings from pertinent scientific journals and textbooks or video clips, as posted on the course's e-learning site

3. Other Resources (If any)
N/A

Section 7 Evaluation and Improvement of Course Management

1. Strategies for evaluating course effectiveness by students
   1.1 Student feedback of instructors, teaching methods and materials, and course content through MUIC student evaluation forms
2. Strategies for evaluating teaching methods
   2.1 Evaluation of effectiveness based on student evaluation scores and comments
   2.2 Evaluation through peer observations by co-instructor or other Division faculty
3. Improvement of teaching methods
   3.1 Adjustments based on student feedback, personal observations, comments from peer observations and discussions with supervisor and/or other Division faculty in one-on-one and/or group meetings as specified by MUIC guidelines
4. Verification process for evaluating students' standard achievement outcomes in the course
   4.1 Verification through student performance on assessments based on MUIC/Division standards
5. Review and plan for improving the effectiveness of the course
   5.1 Course instructors (and coordinator/supervisor) will meet to discuss results of student evaluations and student performance based on learning outcomes in order to identify point for improvement
   5.2 Strategy for improvement set according to MUIC/Division guidelines

Appendix
Alignment between Courses and General Education courses

Table 1 The relationship between course and Program Learning Outcomes (PLOs)

	Program Learning Outcomes (PLOs)					
	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
(ICCS418)		2.1, 2.2			5.2,5.3, 5.4	6.2

Note: Indicate the level of CLOs by letter I, R, P or M. Using the information as shown in the Curriculum Mapping of TQF2.

Table 2 The relationship between CLOs and Program LOs (Number in table = Sub LOs)

ICCS418	Learning Outcomes in the Computer Science Program (CS-PLOs)					
	1	2	3	4	5	6
CLO 1 Describe fundamental of computer security concepts.		2.1, 2.2				
CLO 2 Explain access control mechanisms including their strengths and weaknesses.		5.4, 6.2				
CLO 3 Classify cryptography algorithms and explain the difference between them.					5.4	
CLO 4 Classify software/operating systems and computer network vulnerabilities with security attack techniques.					5.2 5.3	
CLO 5 Understanding the defense and analysis techniques for business continuity.		2.1, 2.2				

Table 3 The description of Program LOs and Sub LOs of the course

LOs	Sub LOs
1. Demonstrate proficiency in scientific communication	1.1 Identify means and platforms of communication commonly used in computing disciplines 1.2 Communicate inchoate ideas to others for further development and refinement 1.3 Describe computing concepts to members of the community with accuracy and clarity.
2. Carry out work with scientific integrity and professionalism	2.1 Recognize the concepts of intellectual property, copyright licenses, and law pertaining to information technology 2.2 Provide ethical reasoning and awareness of issues surrounding bias, fabrication, falsification, plagiarism, outside interference, censorship, and information privacy. 2.3 Demonstrate good time management, self-regulation, autonomy, and professional code of conduct of the discipline.
3. Appraise scientific information critically	3.1 Apply quantitative reasoning using mathematical methods and scientific facts, taking into consideration multiple perspectives. 3.2 Provide a succinct description of the issue (i.e., a problem, a question, or a hypothesis), separating facts and assumptions 3.3 Differentiate source, validity, objectives, key arguments, and consequences of a piece information. 3.4 Create a response to the issue by synthesizing collected information critical to the assessment
4. Use a teamwork mindset in the context of computing.	
5. Execute common computing methodologies appropriate for a problem scenario	5.1 Carry out the process of converting a process/algorithm to a machine-executable program. 5.2 Use suitable techniques for correctness and cost analysis of computer programs 5.3 Deconstruct a computer system to reveal its structure, components, and process of construction 5.4 Select common computing techniques (e.g., standard algorithms, data structures, design patterns, programing style, and computing paradigms) appropriate for a given problem scenario.
6. Formulate computational solutions to novel situations grounded on the foundation of computer science	6.1 Model a given problem using suitable abstractions, including problem decomposition, in the context of computing 6.2 Compare the relative strengths and weaknesses among multiple designs or implementations 6.3 Assess the feasibility and efficacy of a computational solution based on its design and implementation 6.4 Devise computational solutions to novel situations using knowledge and experience in computer science