CPE 393 – Fundamentals of Cybersecurity (2_2021)

Computer Engineering Department, King Mongkut's University of Technology Thonburi

Instructors: Assoc. Prof. Thumrongrat Amornraksa, Ph.D.
Pol. Lt. Prasitchai Boonserm, D.Eng.

Time/Location: Saturday 09.00-12.00 at Room CPE 1121 or Online with scheduled meetings via Zoom

Office hours: Aj. Thumrongrat Monday (08.30 - 13.00 pm.) or by appointment
Aj. Prasitchai Saturday (13.00-15.00 pm.) or by appointment

Contact Addresses: t_amornraksa@cpe.kmutt.ac.th
prasitchai.boonserm@gmail.com

Course Objectives: Introduction to cryptography. The architecture of computer systems and networks, and possible attacks. Authentication, authentication protocols, and key exchange protocols establish a secure service system. Design and analysis of security protocols. Computer and information security applications in software development, internet, and wireless network. Information security management system. Cyber risk analysis and controls. Hand-on experience on some network security tools.

Object Learning Outcomes

1. Identify key concepts and terminology in cybersecurity.
2. Identify the key components of securing networks, systems and applications, and data.
3. Apply cryptographic protocols to establish a secure service system, including database and program security.
4. Identify the key concepts of cyber risk management and selection of countermeasures.

Course Topics: Identify the Security Fundamentals, Cybersecurity and Risk Management, Asset Security, Security Architecture and Engineering, Business Continuity, Cryptography, Communication and Network Security, Identity and Access Management (IAM), Software Development Security, Security Assessment and Testing, Security Operations, Secured Software Delivery Pipeline.

Textbooks

1. A. Gordon, *Official (ISC)2 Guide to the CISSP® CBK®*, CRC Press, 4th Edition, 2015.
2. I. Meil, *CompTIA Security+:SY0-601 Certification Guide*, Packt Publishing, 2nd Edition,2020.

Reference

1. International Standard ISO/IEC 27001 Information Security Management System.
2. International Standard ISO/IEC 27002 Code of practice for information security controls.
3. The Six Pillars of DevSecOps: Automation, Available at https://cloudsecurityalliance.org/research/working-groups/devsecops/

Grading Policy: The final grade will be calculated according to the following weights:

Class Discussions	20 %	Homeworks	30 %
Midterm Examination	20 %	Final Examination	30 %

Note: The instructors reserve the right to change the grading policy, the course contents, and the class schedule as deemed appropriate.

Class Schedule (subject to change)

Week	Content
1 (Jan. 22)	Talk and Overview to the Course
2 (Jan. 29)	Identifying the Security Fundamentals
3 (Feb. 5)	Cybersecurity and Risk Management
4 (Feb. 12)	Asset Security + Homework 1 (Risk Analysis) + (HW 5%)
5 (Feb. 19)	No Class – Homework week
6 (Feb. 26)	Security Architecture and Engineering
7 (Mar. 5)	Business Continuity
8 (Mar. 12)	Security Discussion (Selected Topics) – Discussion Week – (Discussion 10%)
9 (Mar. 19)	Midterm Exam. (20%)
10 (Mar. 26)	Cryptography + Homework 2 (Crypthography) – (HW 5%) Capt. Korakoch Wilailux (Royal Thai Navy)
11 (Apr. 2)	Communication and Network Security 1 & 2 + Homework 3 – (HW 5%)
12 (Apr. 9)	No Class – Final Exam (1st-half 15%)
13 (Apr. 16)	Holiday Break (April 11-15) – Long weekend
14 (Apr. 23)	Identity and Access Management (IAM)
15 (Apr 30)	Software Development Security + Secured Software Delivery Pipeline
16 (May 7)	Security Assessment and Testing + Security Operations
17 (May 14)	Security Discussion (Selected Topics) – Discussion Week – (Discussion 10%)
18 (May 21)	Student Presentation/Demo (Topic: Secured Software Delivery Pipeline) – (HW 15%)
19 (May 23-27)	Final Exam (2nd-half 15%)