# Lecture 0

## Course Overview

**Dr. Charnon Pattiyanon**
Assistant Director of IT, Instructor
Department of Artificial Intelligence and Computer Engineering
**CMKL University**

# Welcome to
# 18-631: Introduction to Information Security

# Let me introduce myself first 🤗

This is my LinkedIn and Personal Website.

- My name is **Charnon Pattiyanon, Ph.D.** and my students called me *Ajarn Top* or *Ajarn Charnon*.
- If you would like to contact me, feel free to email me at charnon@cmkl.ac.th or schedule a meeting at my office (**706, 7th floor**).
- I currently serve as the Assistant Director of IT and an Instructor in **Cybersecurity** at CMKL University.
- I started my academic journey with *a Bachelor of Engineering (B.Eng.)* in Computer Engineering (International Program) at **KMUTT**.
- I began my career as a web developer at a software house in Thailand.

# Let me introduce myself first 🤗


This is my LinkedIn and Personal Website.

- After working for a few years, I realized that I was capable of more than just day-to-day development work. I decided to pursue *a Master of Science (M.Sc.)* in Software Engineering at **Chulalongkorn University**.
- After graduating, I joined G-ABLE Co., Ltd. in the Security Solutions Department, where I realized that working as **a white-hat security engineer** was the right path for me.
- I chose to challenge myself by pursuing *a doctor of Philosophy (Ph.D.)* in Information Science at Japan Advanced Institute of Science and Technology or **JAIST** in Ishikawa, Japan, where I conducted extensive research in the fields of information security and privacy.

# How about you?

- What is your name and how can I call you during the lecture?
- Where did you come from?
- What are your past educations and work experiences?
- What is information security in your opinion?
- What are your expectations of this course?
- Have you ever experienced any issues about information security?

# Course Description

- This course introduces you with the technical and policy foundation of information security.
- The **main objective** of this course is to enable students to reason about information systems from a security engineering perspective, considering technical, economic and policy factors.
- **Contents of this course cover:**
  - *Basic and Advanced Cryptography; Access Control; Common Software Vulnerabilities; Network Fundamentals and Security; Web Security; Security Economics; Security Management/Assurance;*
- **Prerequisites:**
  - A basic working knowledge of computers, networks, C and UNIX programming.
  - An elementary mathematics background
  - Students lacking technical background (e.g., students without any prior exposure to programming) are expected to catch up through self-study.

# Course Objectives and Goals

- The educational objectives intended to be fulfilled upon successful of this course are:
  - Students should acquire technical skills in ***building*** secure information systems.
  - Students should acquire technical skills in ***analyzing*** security of information systems.
  - Students should acquire analytical and creative skills in ***identifying security problems*** within the context and ***finding solutions*** by:
    - ***Designing*** a system, component, or process to meet desired security requirements.
    - Identifying, formulating, and solving security issues in modern computer and information systems.
    - Understanding the impact of engineering solutions in a global, economic, environmental, and societal context.
  - Students should acquire professional skills in functioning within a larger work environment.
  - Students should be aware of the need for, and an ability to engage in a life-long learning.

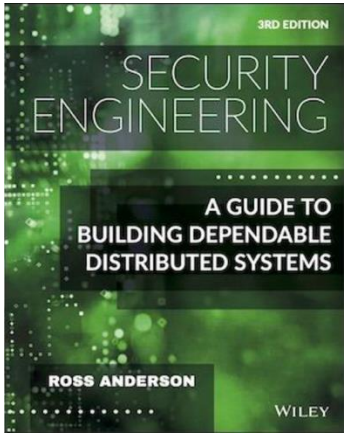
# Course General Information

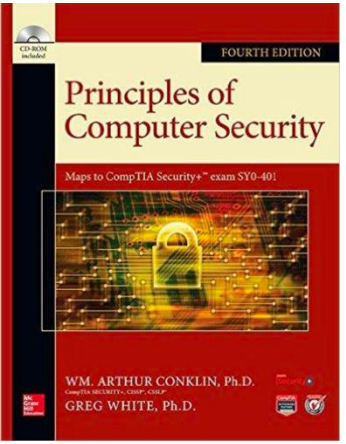
- **Lecture Time:** Every Tuesday and Wednesday, 10:00 – 11:30
- **Office Hours:** By appointment only.
- **Instructor Information:**
  - Dr. Charnon Pattiyanon (Room 706), charnon@cmkl.ac.th
  - Dr. Raveekiat Singhaphandu (Room 706), raveekiat@cmkl.ac.th

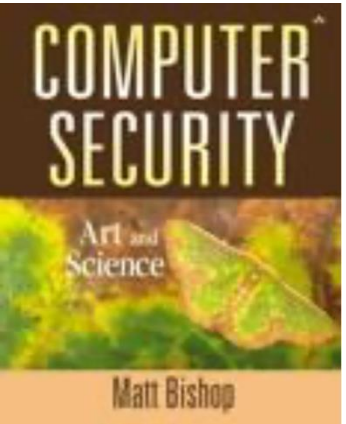
- **Learning Platform and Materials:** Canvas
- **Communication Channel:** Email, Discussion Page on Canvas
- **Grading Criteria:**
  - Midterm Exam (**25%**),
  - Final Exam (**40%**),
  - Quizzes and Assignments (**35%**).

# Learning Topics and Class Schedule

| Week | Tue | Wed | Topics | By |
|---|---|---|---|---|
| 1 | 8/26 | 8/27 | Introduction, Threat Models, Basic Security Properties | Dr. Charnon |
| 2 | 9/2 | 9/3 | Cryptography: History, Private Key Algorithms | Dr. Charnon |
| 3 | 9/9 | 9/10 | Cryptography: Public Key Algorithms, Unkeyed Algorithm, Hashes | Dr. Charnon |
| 4 | 9/16 | 9/17 | Cryptography: PKI, Basic Policy Overview | Dr. Charnon |
| 5 | 9/23 | 9/24 | Access Control: OS, Multilevel and Multilateral Security | Dr. Charnon |
| 6 | 9/30 | 10/1 | Basic Software Vulnerabilities | Dr. Charnon |
| 7 | 10/7 | | **Midterm Exam** | |
| | 10/8 | | Software Vulnerability Defenses, Software/Hardware Issues (TCG/Rowhammer) | Dr. Charnon |
| 8 | 10/14 | 10/16 | **Fall Break** | |
| 9 | 10/21 | Holiday | Buffer Overflows | Dr. Raveekiat |
| 10 | 10/28 | 10/30 | Network Fundamentals: Security Protocols, SSL/TLS | Dr. Raveekiat |
| 11 | 11/4 | 11/6 | Network Security: TCP Vulnerabilities, DDoS Attacks | Dr. Raveekiat |
| 12 | 11/11 | 11/13 | Web Security, Anonymity | Dr. Raveekiat |
| 13 | 11/18 | 11/20 | Security Economics / Psychological Aspects, Online Crime | Dr. Raveekiat |
| 14 | 11/25 | 11/27 | Usable Security, Management and Assurance | Dr. Raveekiat |
| 15 | 12/2 | | **Final Exam** | |

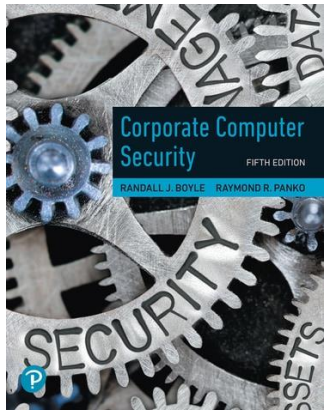


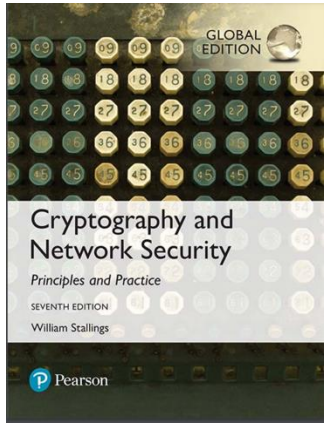



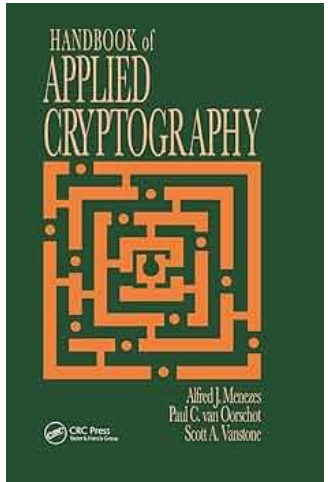




# Textbooks and Course Resources

- **Recommended Readings/Textbooks:**
  - Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley.
  - Wm. Arthur Conklin et al. Principles of Computer Security. [Practical]
  - Matt Bishop. Computer Security: Art & Science. [Formal Methods]
  - Randy J. Boyle and Raymond R. Panko. Corporate Computer Security.
  - William Stallings. Cryptography and Network Security: Principles and Practice.
  - Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. The Handbook of Applied Cryptography.
- **Online Materials:**
  - Open Web Application Security Project (OWASP) https://owasp.org
  - CISSP Free by Skillset.com on YouTube https://www.youtube.com/channel/UC_SAXriJ73uF2l8d55G6mEA



# Security-Related Events and Online Materials

- **Conferences and Seminars:**
  - ***Black Hat Briefings*** – Very well-known for security experts.
  - ***DEF CON*** – The largest hacking and security conference.
  - ***IEEE Symposium on Security and Privacy (ISSP)*** – A must for academia.

- **Online Materials:**
  - Capture the Flag : https://ctftime.org
  - Bug Bounty and and Disclosure Programs: https://www.bugcrowd.com/bug-bounty-list/
    - Common Vulnerability Exposure: https://cve.mitre.org/
    - Google Reward: https://www.google.com/about/appsecurity/reward-program/
    - Microsoft Bounty: https://www.microsoft.com/en-us/msrc/bounty/

# Academic Integrity

- "In any manner of **presentation**, it is *the responsibility of each student to produce her/his own original academic work*."
- "In all academic work to be graded, **the citation of all sources is required**. When collaboration or assistance is permitted by the course instructor(s) [...], **the acknowledgement of any collaboration or assistance is likewise required**. This citation and acknowledgement must be incorporated into the work submitted and not separately or at a later point in time."
- "**Cheating** occurs when a student avails her/himself of an unfair or disallowed advantage [...]"
- "**Plagiarism** is defined as the use of work or concepts contributed by other individuals without proper attribution or citation. Unique ideas or materials taken from another source for either written or oral use must be fully acknowledged in academic work to be graded."

# End of the Lecture

Please don’t hesitate to raise your hand and ask questions if you're curious about anything!