SEC-301: Security Challenges in Modern AI Systems

Lecture 0 – Competency Overview

Instructed By:

Dr. Charnon Pattiyanon

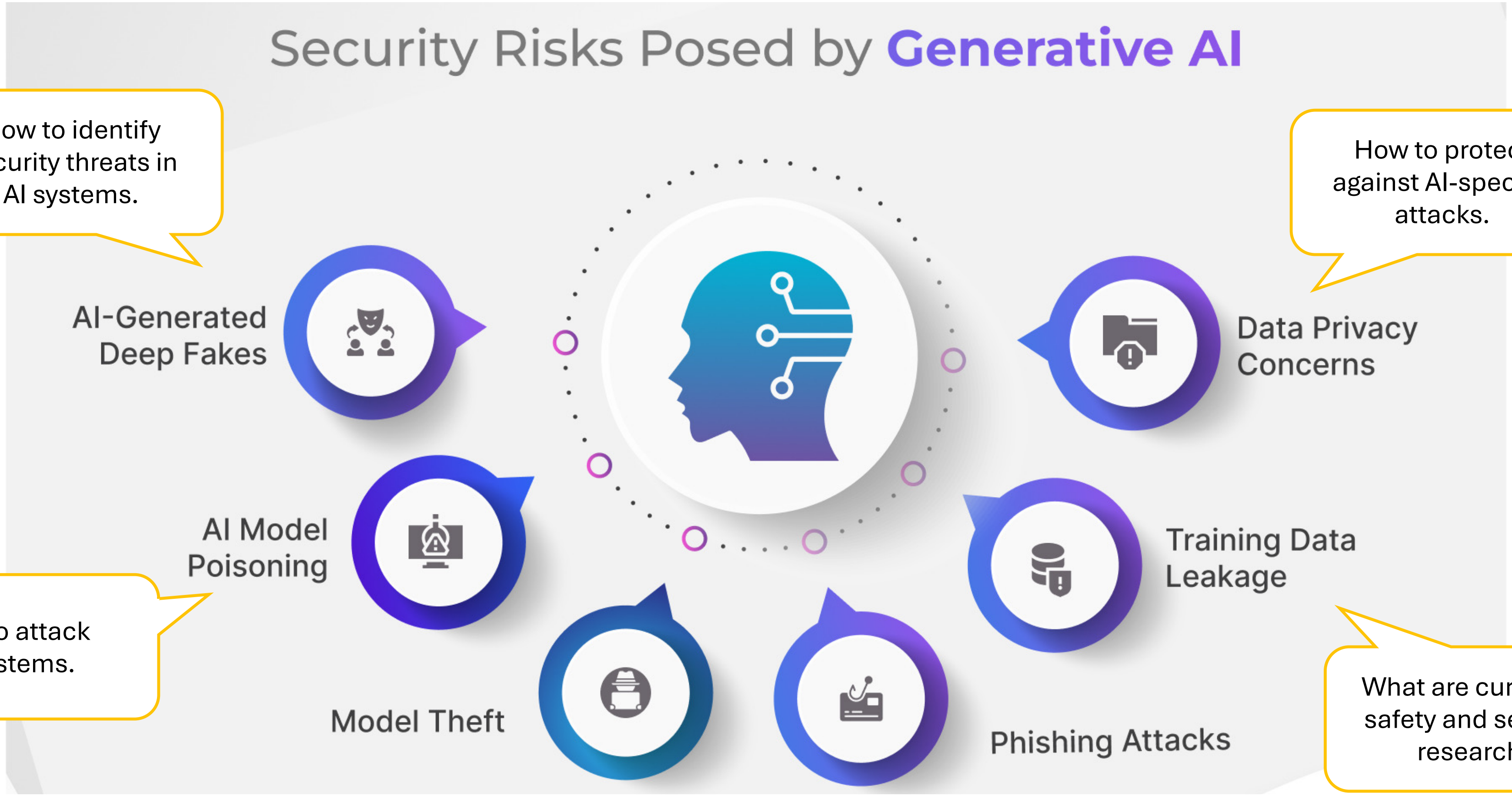
Assistant Director of IT and Instructor
CMKL University

Artificial Intelligence and Computer
Engineering (AICE) Program

General Information

- **Competency Period:** January 19, 2026 to February 9, 2026 (**4 Weeks**)
- **Classroom Location:** CMKL 601
- **Lecture Time:** Every Monday, 10:00 – 11:00
- **Lab/Practical Session Time:** No Lab
- **Office Hours:** Every Monday, 11:00 – 12:00
- **Communication Channel:**
  - Class Material / Lecture Slides: https://cmkl.instructure.com/courses/906/modules
  - Discussion / Q&A: https://cmkl.instructure.com/courses/906/discussion_topics
  - Assessment Submission: https://cmkl.instructure.com/courses/906/assignments

Competency Description



How to identify security threats in AI systems.

How to protect against AI-specific attacks.

How to attack AI systems.

What are current AI safety and security research?

Skills and Assessment

- There are four skills to be assesed in this competency:
  - **[SEC-301:00010]** – Analyze AI security Risks.
  - **[SEC-301:00020]** – Analyze AI security threats using analysis techniques.
  - **[SEC-301:00030]** – Analyze AI-specific attack scenarios.
  - **[SEC-301:00040]** – Understand AI Safety in academic.

- **Assessment:**
  - Work in a pair to tackle security challenges in a modern AI system.
  - Implement a security-protection technique for an AI model's training process.
  - Write a report to communicate the design of the protection for the selected AI system.

Competency Schedule

Date	Classroom	Lecture
January 19, 2026	601	• Lecture 0: Competency Overview • Lecture 1: AI Security Risks • **Assessment Announcement**
January 26, 2026	601	• Lecture 2: Basic Security Threat Analysis Techniques • **Homework 1: Identify Security Threats in the Selected AI System. [No Submission]**
February 2, 2026	**No Lecture / No Class**	
February 9, 2026	601	• Lecture 3: AI Security Risk Prevention Techniques (Part I)
(Make-up Class)	TBA	• Lecture 3: AI Security Risk Prevention Techniques (Part II) • Lecture 4: AI Security and Safety Research
May 1, 2026	**Assessment Report Submission Deadline**	

70% Attendance is required for all students (3 out of 4 classes) .

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."
- The use of AI tools are **not prohibited** in the competency; however, it is required for students to input their original idea in the deliverables.

End of the Lecture

Please do not hesitate to ask any questions to free your curiosity,

If you have any further questions after the class, please contact me via email (charnon@cmkl.ac.th).