Assessment Instruction

Competency: SEC-201: Data Privacy, Security, and Integrity

General Information

Competency Code: SEC-201

Competency Name: Data Privacy, Security, and Integrity

Semester: -

Instructor: Charnon Pattiyanon, Ph.D.

Competency Overview

Data is one of the most valuable assets in modern software systems, often containing sensitive or personal information that must be protected to uphold the reputation and trustworthiness of these systems. Ensuring data privacy, security, and integrity are essential principles in effective data protection.

In this competency, we explored three critical aspects of data protection. First, we will examine existing issues and the principles that should be prioritized. Then, we delve into specific techniques and methods used to safeguard data privacy, security, and integrity, equipping you with the skills to analyze and design modules that ensure robust data protection. Additionally, this competency introduced the concepts of data governance, including an overview of relevant laws and regulations for data privacy. By the end of this competency, you will have the knowledge and skills to handle data responsibly, ensuring security, integrity, and privacy in all aspects of data manipulation.

Assessing Skills

- **[SEC-201:00010] Analyze the sensitivity of data and information** – Successful students must be able to identify the sensitivity of data and information used in a software system.
- **[SEC-201:00020] Analyze the secure data and information processing** – Successful students must be able to design and evaluate secure data processing activities.
- **[SEC-201:00030] Evaluate data security in an information system** – Successful students must be able to implement data security techniques, such as encryption and secure key exchange, in a practical system.
- **[SEC-201:00040] Evaluate data integrity in an information system** – Successful students must be able to implement data integrity techniques, such as message authentication and digital signatures, in a practical system.

- **[SEC-201:00050] Evaluate data privacy preservation mechanisms in an information system** – Successful students must be able to apply data privacy preservation mechanisms, such as data anonymization and conditional privacy, in a practical system.
- **[SEC-201:00060] Analyze the compliance of data privacy laws and regulations** – Successful students must be able to understand, analyze, and suggest the compliance of a practical system to a data privacy laws and regulations.

Pre-cautions

- Please ensure that your answers to each part of the required outcomes are expressed in your own words and perspectives. **Plagiarism is strictly prohibited.** If there is evidence that content or ideas are significantly similar between two or more students without valid justification, the scores of all involved students will be deducted as a penalty for academic misconduct.
- Students are expected to demonstrate a deep understanding of the subject matter by applying **critical analysis and original insights**. Overreliance on AI-generated content without meaningful personal input will negatively affect the assessment score.
- Each response in your assessment should be written in a **"why" style**, where you provide justifications to explain the reasoning behind your answers. For example: *"I believe this privacy principle applies to the target system because ..."*. There is no single "correct" solution or criticism; instead, your analytical and reasoning skills will be evaluated based on the clarity and depth of your justifications.
- You are encouraged to ask questions to satisfy your curiosity about the assessment through email or the Canvas discussion page. However, please do not submit your assessment report for feedback. According to the submission policy, feedback will only be provided on formally submitted reports.

Submission Policy

- You are allowed to submit your work only once per semester. You may not submit your work and then request feedback from the instructor. However, it is at the instructor's discretion whether to provide feedback.
- All submissions must be completed **through the Canvas system only**, as your scores need to be stored and transferred to the university's system. Submissions made via any other channel will not be recognized as official, and you will not receive a score for your work.
- At the end of each semester, **CMKL University** sets a deadline for students to submit their assessments for all enrolled competencies. If you fail to submit your work by the stated deadline, you will not receive any score. In such cases, you must retake the competency in future semesters. While you may submit a request for consideration of a late submission, approval is subject to the instructor's discretion and the university's operational constraints.

Assessment Summary

Title: Implementing a secure information processing system in group

Overview:

This assessment requires you to form a team of **3 to 5 students** and implement a secure information system capable of storing and transmitting confidential or sensitive data between components or over the internet. Your system must incorporate **security, privacy, and integrity mechanisms** to ensure proper data protection. You are expected to demonstrate security awareness in both the implementation and the processes. In addition, you must submit a **design specification and analysis report** and deliver a **presentation of your work during the final week** of the competency.

Objective:

- Students must be able to analyze and design an information processing system that incorporates **security, privacy, and integrity measures** to ensure data and information protection.
- Students must be able to analyze, plan, and establish a **secure development process**.
- Students must be able to properly implement **security, privacy, and integrity measures**, including relevant techniques and tools.
- Students must be able to define and conduct **testing activities** that address security, privacy, and integrity concerns.

Deliverables:

- A list of team member list
- A brief description of the implementing information processing system.
- A set of presentation materials
- A final report for the group assessment project

Detailed Assessment Instruction

1. Form a team of **3 to 5 students** enrolled in this competency. If you wish to form a team with more or fewer members, please consult the instructor.
2. Identify the **roles and responsibilities** of each team member. These role assignments will guide task delegation during the presentation. At least **3 out of the 4 roles** below must be included:
    - **Security Team Leader:** Responsible for overseeing the secure software development project. The student in this role must be able to explain secure development activities and how the team plans the development process.
    - **Security Analyst and Designer:** Responsible for analyzing system requirements from business needs and designing the system architecture and structure. The student in this role must be able to explain design decisions and how protection mechanisms are integrated into the system.
    - **Security Engineer and Developer:** Responsible for implementing the target system and deploying security, privacy, and integrity protection mechanisms. The student in this role must be able to explain code implementation, use of libraries, and methods for ensuring correct implementation.
    - **Security Auditor and Tester:** Responsible for auditing and testing the developed system. The student in this role must be able to explain how test cases are prepared for security, privacy, and integrity requirements, and how testing activities are conducted.
3. **Deliverable:** Submit your **team member list along with roles and responsibilities** in the Canvas assignment.
4. Select **a target information-processing system** for your project and implement security, privacy, and integrity protection mechanisms. The chosen system must satisfy the following qualifications:
    - The system may be either an existing application (which you can replicate as a command-line program) or a new system you intend to implement; examples include chat applications, file-sharing systems, or registration systems.
    - The system must store, manipulate, display, and transmit data to deliver functionality to users.
    - The system should include multiple components and support data communication among components to demonstrate protection mechanisms during transmission.
    - For simplicity, the system must be implementable at minimum as a command-line program.
5. **Deliverable:** Submit the **name and description** of the chosen system, including details about its functionality and how it processes data.

6. Design the chosen information-processing system with explicit consideration for data security, privacy, and integrity. Work collaboratively to produce a complete system design, leveraging your software design and development skills to implement a full secure software development process. **Deliverable: a design specification** document that provides the system's functional, structural, and behavioral designs with integrated data protection. The design specification must follow the provided template and be included in the final project report.
7. Develop the chosen system to provide its core functionality. At a minimum, you must implement a **command-line interface program** that clearly demonstrates its features. Fancy features or graphical user interfaces are optional. The implementation must incorporate security, privacy, and integrity protection mechanisms (either those discussed in the lecture or others) and must be sufficient to inspire user trust in the system. You may use existing libraries or frameworks to simplify the implementation of security, privacy, and integrity protections.
8. Write an **analysis report** on security, privacy, and integrity. The team must evaluate the current state of data protection in the chosen system's implementation and identify opportunities for improvement. **Deliverable: An analysis report describing the system's data security, privacy, and integrity protections**, following the provided template. This report must be included in the final project submission.
9. Prepare a **10-minute presentation** for the final class of the competency. The presentation should include details of the chosen system's implementation and will be organized as follows:
    - Each student must introduce themselves and state their roles and responsibilities at the beginning.
    - The team must present their work within the 10-minute limit. Proper time management is required, and exceeding the limit unreasonably may result in a score deduction.
    - A 5–10 minute Q&A session with peers and the instructor will follow. Teams may receive additional points for active participation in asking questions.

    Deliverable: A presentation slide deck following the given template, submitted on Canvas at least one day before the presentation.
10. Deliver the presentation during the final class session of the competency on the designated date and time.
11. **Consolidate documents and finalize the project report.** After the presentation, gather comments and feedback, and revise your report accordingly. The final project report must include both the **design specification** and the **analysis report**, following the provided template.
12. Submit the **final assessment project report** on Canvas before the last day of assessment.

Important Dates for the Assessment Project

- **Submission Deadline for Team Member List and Roles:** September XX, 2025, 11:59PM
- **Submission Deadline for System Title and Description:** September XX, 2025, 11:59PM
- **Submission Deadline for A Presentation Slide Deck:** November XX, 2025, 11:59PM
- **Assessment Project Presentation Date:** November XX, 2025, 2:00PM – 4:00PM
- **Submission Deadline for Assessment Project Final Report:** November XX, 2025, 11:59PM

Presentation Rubric

The presentation will be equivalent to 30% of your final score or 200 points out of 600 points (from 6 assessing skills). Some parts will be graded as a group performance, while others will be graded individually. The following rubric will be used for grading the presentation.

- (10 Points) **Time Management:** Full points will be awarded to the group that could effectively manage their presentation time, staying within the 10-minute limit.
- (10 Points) **Individual Effort:** Each student will receive full points if they participate equally in the presentation alongside their team members.
- (30 Points) **Smoothness of the Presentation:** Full points will be awarded to the group that could show evidence of well preparation and rehearsal, ensuring a seamless presentation.
- (50 Points) **Completeness of the Content:** Full points will be awarded if the presentation content is complete, justifiable, and comprehensive.
- (100 Points) **Effectiveness in Answering Questions:** Full points will be awarded for each student who can effectively answer audience questions, based on their assigned role. Students must demonstrate a clear understanding of data privacy, security, and integrity mechanisms.