

Week 6 Tutorial: Access Control Models & AAA

Group Discussion and Analysis (60 minutes)

Groups discussion continues using the same scenarios and groups allocation as previous weeks.

Scenario topics:

1. An online holiday booking system.
2. A medium size school timetabling and attendance system
3. An estate agent web application
4. A restaurant self-service digital ordering system

Risk management work phase (1 hour)

Each group must:

- a) Identify Security Requirements
 - 1- Based on the identified risks from last week, determine the specific security requirements related to access control for your system.
 - 2- Consider different types of users (e.g., customers, employees, administrators) and their levels of access.
- b) Choose Suitable Access Control Models
 - 1- Evaluate different Access Control Models (e.g., Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC)).
 - 2- Determine the most appropriate model(s) for your system, considering factors like:
 - Sensitivity of data
 - User roles and permissions
 - Compliance requirements
 - Risk mitigation strategies identified last week
 - 3- Justify why the chosen model is best suited for your system.
- c) Implement AAA Principles

- 1- Authentication: Define how users will be authenticated (e.g., passwords, multi-factor authentication, biometrics).
- 2- Authorisation: Explain how access rights and permissions will be assigned based on the chosen model.
- 3- Accounting: Identify how user activities will be logged and monitored for security and compliance.

Presentation (10 minutes each)

Each group will briefly present their findings, explaining:

- Key security requirements based on last week's risk assessment.
- Chosen Access Control Model and justification.
- Implementation of AAA principles within their system.

Class Discussion (30 minutes)

The remaining of the session is focused on the assignment and how you should align this week activity with the assignment tasks.