토론 주제

자유 토론으로 진행되며, 토론할 주제가 없는 팀은 아래 내용을 참고하시길 바랍니다.

- 적극적으로 참여하기(말하는 것이 어색해도 끝까지 의견을 표현하기)
- 조장의 적극적인 중재 -> 조장이 토론 진행을 조율하고, 참여를 독려할 것
- 단답형 대답보다는 이유와 근거를 포함해서 말하기

토론 주제	세부 토론 주제
프로젝트 진행 속도 일정 조정 문제	• 우리 팀이 생각보다 진행이 빠른가? 느린가? • 일정이 지연되는 경우 주된 이유는 무엇인가? • 다른 팀은 어떻게 프로젝트를 효율적으로 관리하고 있나? • 일정 조정을 위해 우리가 놓치고 있는 요소는 무엇인가?
팀 협업 방식 역할 분배 방식 비교	• 우리 팀은 역할을 어떻게 분배하고 있는가? • 다른 팀은 효율적인 협업을 위해 어떤 툴을 사용하고 있는가? • 팀 내부에서 소통이 잘 안 되는 경우, 어떤 해결책이 있는가?
현재까지 가장 고민되는 기술적/연구적 난제 해결	• 우리 팀이 가장 해결하고 싶은 기술적인 문제(또는 연구적 난제)는 무엇인가? • 다른 팀은 비슷한 문제를 겪고 있거나, 해결 방법을 알고 있는가? • 이 문제를 해결하기 위한 다른 접근법이 있는가?
프로젝트 결과물 평가 방식 **&** 기대 효과 논의	• 프로젝트의 성공 기준을 어떻게 정할 것인가? • 결과물이 어떤 영향을 미칠 수 있는가? • 프로젝트가 종료된 후 어떻게 활용될 수 있을까?
예기치 못한 변수 **&** 리스크 관리 전략	• 프로젝트 진행 중 가장 예상하지 못했던 변수는 무엇인가? • 이 변수(리스크)로 인해 일정, 진행 방식, 협업 등에 어떤 영향이 있었는가? • 다른 팀은 어떤 변수들을 예상하고 대비하고 있는가? • 앞으로 발생할 수 있는 위험 요소를 줄이기 위해 어떤 전략을 세울 수 있을까?

종합설계**01** 토론 보고서

조 이름	15조
매칭된 조 이름	14조
날짜	2025.04.07
주제	프로젝트 진행 속도, 일정 조정 문제
논의 내용	상대 조는 GitHub API 등을 활용해 오픈 소스 코드를 수집하고, Tigress를 사용해 코드를 난독화한 뒤, 이를 LLM에 학습시켜 loop-switch와 같은 바이너리 구조의 존재 여부를 프롬프팅을 통해 판별하는 실험을 진행하고 있음. 전반적인 진행 상황은 무난한 편이며, 일정 지연은 주로 실험 결과가 유의미하지 않을 경우 반복 실험이 필요해지는 상황에서 발생하고 있음. 블로그를 통해 진행 상황을 정리하고 있으며 역할 분담도 이루어지고 있고, 주 1회 교수님과 Zoom 미팅을 통해 프로젝트를 점검하고 있음.
느낀점 및 도출된 인사이트	우리는 단순한 난독화 기법만으로는 LLM의 패턴 기반 분석을 완전히 막기 어렵다는 현실적인 한계를 체감하고, LLM을 고려한 고도화된 난독화 전략의 필요성을 인식하게 되었다. 특히, 제어 흐름 평탄화나 의미 없는 조건 삽입, 복잡한 switch-case 구조 등 LLM이 쉽게 판단할 수 없는 코드 구조를 설계하는 것이 중요하다고 느꼈고, 정적 난독화만으로는 부족하므로 동적 난독화나 실행 중 구조가 변하는 방식도 함께 고려해야 한다는 인사이트를 얻었다. 효과적인 난독화란 단순히 코드를 복잡하게 만드는 것이 아니라 분석자(LMM 또는 사람)의 분석 흐름 자체를 교란하는 방식으로 설계되어야 한다는 점도 확인할 수 있었다. 상대 팀이 진행 중인 LLM 기반 switch-case 탐지 실험은 우리 팀이 설정해야 할 난독화 효과 평가 기준 수립에 참고가 되며, 궁극적으로 우리는 공격자 모델을 상정한 방어적 사고를 기반으로 더 강력하고 정교한 난독화 전략을 설계해 나가야 한다는 교훈을 얻게 되었다.