AI-정보보안 튜토리얼

일시: 2025년 6월 13일(금) 09:00~11:45

장소: 메종글래드 제주 2층 아메티스트홀

프로그램

시 간	발표주제	발표자
09:00~10:15	MCP(Model Context Protocol) 소개	정현준(국립군산대학교 교수)
10:15~10:30	Coffee break	
10:30~11:45	소프트웨어 취약점 탐지 자동화 방법론 소개 및 최신 연구 동향	최재승(서강대학교 교수)

강연소개

MCP(Model Context Protocol) 소개

정현준 (국립군산대학교 교수)

- 국립군산대학교 조교수 (2021~현재)
- 광주과학기술원(GIST) 블록체인인터넷경제연구센터 연구 (2017~2020)
- 고려대학교 박사 (2017)

본 튜토리얼에서는 AI시스템이 외부 데이터와 효과적으로 연동되는 기술인 MCP(Model Context Protocol)를 소개한다. MCP는 AI 모델이 다양한 데이터 소스와 연결되어 실시간으로 정보를 주고받을 수 있도록 설계된 프로토콜로, 이를 활용하면 AI가 더욱 정확하고 개인화된 답변을 제공할 수 있다. 튜토리얼은 MCP에 대해서 기본적인 개념을 설명한 뒤 MCP서버를 구현하여 기본적인 사용법에 대하여 배워본다. 본 튜토리얼은 인공지능 및 LLM 분야의 특별한 선수 지식을 요구하지 않으며, 인공지능 및 LLM에 관심있는 모든 참가자를 대상으로 상정한다.

소프트웨어 취약점 탐지 자동화 방법론 소개 및 최신 연구 동향

최재승 (서강대학교 교수)

- 서강대학교 컴퓨터공학과 조교수 (2022-현재)
- 사이버보안연구센터 선임연구원 (2022)
- 한국과학기술원(KAIST) 전산학 박사 (2017-2022)
- 서울대학교 컴퓨터공학과 학석사 (2011-2017)

본 튜토리얼에서는 소프트웨어 취약점을 자동으로 탐지하는 연구 분야를 소개하고, 최근 인공지능의 발전이 이 분야의 연구에 어떻게 활용될 수 있는지 최신 연구 동향을 논의한다. 튜토리얼의 초반부에서는 소프트웨어 취약점에 대한 기본적인 개념을 설명한 뒤, 취약점의 자동 탐지를 위한 방법론을 정적 분석과 동적 분석으로 나누어 소개한다. 이후, 퍼즈 테스팅 (퍼징) 기술을 중심으로 하여 세부적인 연구 주제 및 사례를 설명한다. 끝으로, 최근 큰 주목을 받고 있는 LLM을 소프트웨어 테스팅 및 분석에 접목하여 활용하는 최근 연구 동향을 간략히 살펴본다. 본 튜토리얼은 정보보안 분야의 특별한 선수 지식을 요구하지 않으며, 소프트웨어 보안 취약점에 대해 관심이 있는 모든 참가자를 수강 대상으로 상정한다.