Seminar Feedback Report (Week09)

2021312738 소프트웨어학과 김서환

9주차 세미나의 내용은 성균관대학교 오상학 연구원의 발표는 AI 코딩 도우미 도구의 보안 문제에 대해 다루었다. 첫 번째로, 최근 많이 사용되는 AI 코딩 도우미들이 오픈소스 데이터를 학습하는 과정에서 신뢰할 수 없는 코드를 포함할 수 있으며, 이러한 취약점이 실제 개발자에게 보안 위협을 줄 수 있다는 점을 설명해주셨다. 두 번째로는 코드 오염과 모델 오염이라는 두 가지 주요 공격 방식이 소개해주셨으며, 특히 코드 생성 도구를 사용하는 개발자들이 취약한 코드를 수용할 가능성이 높다는 실험 결과를 통해 실제 공격 가능성이 확인되었다. 마지막으로, 전통적인 보안 교육만으로는 이러한 위협에 대응하기 어려우며, AI 모델 기반 도구에 특화된 보안 교육이 필요하다는 점을 강조하셨다. 이번 발표는 AI 도구의 발전과 함께 보안 관점에서의 새로운 도전 과제를 인식하게 해주는 중요한 내용이었다고 생각이 들었다.
그 다음, 이재혁 연구원의 발표는 소프트웨어 테스트 분야에서의 상징적 실행(symbolic execution) 기법에 대한 연구를 중심으로 진행되었다. 상징적 실행은 자동 테스트 케이스 생성을 위한 유망한 기법으로, 프로그램의 입력을 기호 변수로 대체해 다양한 실행 경로를 분석하는 방식이다. 그러나 이 과정에서 제약 해결(SMT 솔버 호출) 비용이 매우 크다는 한계가 있으며, 이를 극복하기 위한 기법으로 시딩(seeding) 전략이 소개해주셨다. 이 연구에서는 최적의 시드 테스트 케이스를 선택하기 위한 TopSeed 알고리즘을 제안하고, 이를 통해 테스트 성능이 최대 35.5%까지 향상되었고, 랜덤 설정에서도 성능이 25.4% 개선되었다고 설명해주셨다. 하지만, 이재혁 연구원께서 최적의 시드를 선택하는 것이 여전히 도전 과제로 남아있다고 말씀해주시면서 발표를 마쳤다. 이 발표는 소프트웨어 테스트 자동화의 효율성을 높이기 위한 새로운 접근 방법과 실험 기반 성과를 잘 보여주는 사례라고 생각이 들어 인상 깊었다.